HITACHI
Inspire the Next

Hitachi Compute Blade 2000
User's Guide

Hitachi Data Systems

MK-99BDS2K001-16

© 2011 - 2015 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://portal.hds.com.

Notice: Hitachi, Ltd., products and services can be ordered only under the terms and conditions of the applicable Hitachi Data Systems Corporation agreements. The use of Hitachi, Ltd., products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, zSeries, z/VM, z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

Important Notes

This product includes codes licensed from RSA Data Security.

Reliability of the System Equipment

The system equipment you purchased is designed for general office work. Avoid using it for applications requiring high reliability that may seriously affect human life or property. We shall not assume any responsibility for any accidents resulting from such use of the product.

Examples of inappropriate applications of system equipment intended for general office work are:

- Control of a chemical plant, control of medical devices, and control of emergency communications, all of which require high reliability.

You need a different system for such high reliability applications. Please consult our sales department for the appropriate system.

Regulatory Compliance Notices

❑ Federal Communications Commission (FCC) Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at personal expense. The user is cautioned that changes or modifications not expressly approved by the manufacturer could void the user's right to operate the equipment.

❑ EN55022 Compliance

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

❑ 電波障害自主規制 (Japan)

この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

❑ Class A Emission Statement (Korea)

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

❑ Canadian Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

❑ Product recycling and disposal (EU and Norway) (Waste Electrical and Electronic Equipment Directive 2002/96/EC [WEEE])

The following mark on Products indicates that these Products are to be collected separately and to be recycled or discarded according to applicable local and national regulations. For further information regarding return, collection, recycle or disposal, please contact your sales company where you purchased the Products.



The above mark is not printed on the following Products but these Products are also subject to electrical and electronic equipment (EEE). These un-marked Products are, as well as marked Products, to be collected separately and to be recycled or discarded according to applicable local and national regulations. For further information, please contact your sales company where you purchased the Products.

No.	Products code	Products name
1	GVX-EC2********, GV-EC2******X1-Y	CPU
2	GVX-MJ2********, GV-MJ2****** X1-Y	Memory
3	GVX-UH2********, GV-UH2******X1-Y	HDD KIT
4	GVX-CA2********, GV-CA2****** X1-Y	RAID Card

No.	Products code	Products name
5	GVX-C*2********, GV-C*2******X*-Y	Mezzanine Card
6	GVX-CN2XFP*****, GV-CN2XFP* X*-Y	XFP module
7	GVX-BE2********, GV-BE2*****X*-Y	Dummy Module

Note: The above regulation/marking applies only to countries within the European Union (EU) and Norway.

❑ Export control

To export this product, check the export control-related regulations and follow the necessary procedures. If you have any questions, contact our sales representative.

Note that the same handling is required for peripheral equipment and pre-installed software shipped with this product.

❑ Chinese RoHS

有毒有害物质和元素的名称及含量

零件名称	有毒有害物质和元素					
	铅（Pb）	汞（Hg）	镉（Cd）	六价铬（Cr（VI））	多溴联苯（PBB）	多溴二苯醚（PBDE）
伺服器底座	×	○	○	○	○	○
刀鋒型伺服器	×	○	○	○	○	○
管理模块	×	○	○	○	○	○
局域网交换机模块	×	○	○	○	○	○
光纤交换机模块	×	○	○	○	○	○
网络路径模块	×	○	○	○	○	○
PCI Express 交换机模块	×	○	○	○	○	○
I/O 插槽拡充机件	×	○	○	○	○	○
I/O 模块	×	○	○	○	○	○
电源模块	×	○	○	○	○	○
分电盘	×	○	×	○	○	○

○：表示该零件的所有均质材料中的有毒有害物质的含量在 SJ/T 11363-2006 标准规定的限量範围内。

×：表示该零件的某一均质材料中的有毒有害物质的含量超出 SJ/T 11363-2006 标准规定的限量範围。

Notes on Deleting Data when Disposing of or Transferring the System Equipment

Personal computers and system equipment are used for various purposes at the office and home. Important data of customers are recorded in the hard disks in these computers and system equipment.

You must erase these important data contents when transferring or disposing of the system equipment.

However, it is not easy to erase data written on the hard disk.

When you “erase data”, you generally do one or more of the following:

- Discard data in the “Recycle Bin”.
- “Delete” data.
- Erase data using the “Empty Recycle Bin” command.
- Perform initialization (formatting) of the hard disk using software utilities.
- Recover the factory defaults using a recovery CD.

The above operations only change the file management information of data recorded on the hard disk; actually the data is just blocked from view.

That is, although the data appears to have been erased, it was just made unavailable under an operating system such as Windows. The actual data remains on the hard disk and may be read using special data recovery software. Consequently, important data on the hard disk of the system equipment can be read and used for unexpected applications by malicious people.

To avoid unauthorized access to important data on the hard disk when disposing of or transferring the system equipment, it is extremely important for you to erase all data recorded on the hard disk at your own risk. When you erase the data, we recommend that you purchase and use a dedicated software or service, or corrupt the data on the hard disk physically or magnetically using a hammer or strong magnet to make it unreadable.

Transferring the system equipment without deleting software on the hard disk (operating system, applications, etc.) may be against software licensing agreements. Check your software licensing agreements carefully.

.

Introduction

Thank you for purchasing Hitachi system equipment. This manual describes procedures for the use of the system equipment such as installation, connection, and handling.

The BladeSymphony server name has been changed to Hitachi Compute Blade. If you are using BladeSymphony based server products, substitute references to Hitachi Compute Blade with BladeSymphony.

The Hitachi Virtualization Manager (HVM) name has been changed to Hitachi logical partitioning manager (LPAR manager, or LP). If you are using HVM based logical partitioning feature, substitute references to Hitachi logical partitioning manager (LPAR manager, or LP) with HVM.

Notation

❑ Symbols

Meanings of symbols used in this manual are as follows:

⚠ **Danger**	This indicates information about how to avoid physical injury to yourself and others.
⚠ **WARNING**	This indicates the presence of a potential risk that might cause death or severe injury.
⚠ **CAUTION**	This indicates the presence of a potential risk that might cause relatively mild or moderate injury.
NOTICE	This indicates the presence of a potential risk that might cause damage to the equipment and/or damage to surrounding properties.
	This indicates notes not directly related to injury or severe damage to the equipment.
	This indicates advice on how to make the best use of the equipment.

Abbreviations for Operating Systems (OS)

In this manual, the following abbreviations are used for OS name:

- Microsoft® Windows Server® 2012 R2 Standard
  (Hereinafter, referred to as Windows Server 2012 R2 Standard)
- Microsoft® Windows Server® 2012 R2 Datacenter
  (Hereinafter, referred to as Windows Server 2012 R2 Datacenter)
- Microsoft® Windows Server® 2012 Standard
  (Hereinafter, referred to as Windows Server 2012 Standard)
- Microsoft® Windows Server® 2012 Datacenter
  (Hereinafter, referred to as Windows Server 2012 Datacenter)
- Microsoft® Windows Server® 2008 R2 Standard
  (Hereinafter, referred to as Windows Server 2008 R2 Standard)
- Microsoft® Windows Server® 2008 R2 Enterprise
  (Hereinafter, referred to as Windows Server 2008 R2 Enterprise)
- Microsoft® Windows Server® 2008 R2 Datacenter
  (Hereinafter, referred to as Windows Server 2008 R2 Datacenter)
- Microsoft® Windows Server® 2008 Standard
  (Hereinafter, referred to as Windows Server 2008 Standard)
- Microsoft® Windows Server® 2008 Enterprise
  (Hereinafter, referred to as Windows Server 2008 Enterprise)
- Microsoft® Windows Server® 2008 Datacenter
  (Hereinafter, referred to as Windows Server 2008 Datacenter)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Standard without Hyper-V)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Enterprise without Hyper-V)
- Microsoft® Windows Server® 2008 Datacenter without Hyper-V™
  (Hereinafter, referred to as Windows Server 2008 Datacenter without Hyper-V)
- Microsoft® Windows Server® 2008 Standard 32-bit
  (Hereinafter, referred to as Windows Server 2008 Standard 32-bit)
- Microsoft® Windows Server® 2008 Enterprise 32-bit
  (Hereinafter, referred to as Windows Server 2008 Enterprise 32-bit)
- Microsoft® Windows Server® 2008 Datacenter 32-bit
  (Hereinafter, referred to as Windows Server 2008 Datacenter 32-bit)
- Microsoft® Windows Server® 2008 Standard without Hyper-V™ 32-bit
  (Hereinafter, referred to as Windows Server 2008 Standard without Hyper-V 32-bit)
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V™ 32-bit
  (Hereinafter, referred to as Windows Server 2008 Enterprise without Hyper-V 32-bit)
- Microsoft® Windows Server® 2008 Datacenter without Hyper-V™ 32-bit
  (Hereinafter, referred to as Windows Server 2008 Datacenter without Hyper-V 32-bit)
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Standard x64 Edition)
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Enterprise x64 Edition)
- Microsoft® Windows Server® 2003 R2, Standard Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Standard Edition)
- Microsoft® Windows Server® 2003 R2, Enterprise Edition
  (Hereinafter, referred to as Windows Server 2003 R2, Enterprise Edition)

- Microsoft® Windows Server® 2003, Standard x64 Edition
  (Hereinafter, referred to as Windows Server 2003, Standard x64 Edition)
- Microsoft® Windows Server® 2003, Enterprise x64 Edition
  (Hereinafter, referred to as Windows Server 2003, Enterprise x64 Edition)
- Microsoft® Windows Server® 2003, Standard Edition
  (Hereinafter, referred to as Windows Server 2003, Standard Edition)
- Microsoft® Windows Server® 2003, Enterprise Edition
  (Hereinafter, referred to as Windows Server 2003, Enterprise Edition)
- Microsoft® Windows® 2000 Server Operating System
  (Hereinafter, referred to as Windows 2000 Server)
- Microsoft® Windows® 2000 Advanced Server Operating System
  (Hereinafter, referred to as Windows 2000 Advanced Server)

OS names used in this manual stand for official OS names in “Included OS” in the table below:

OS name in this manual	Included OS
Windows Server 2012 R2	Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter
Windows Server 2012	Windows Server 2012 Standard Windows Server 2012 Datacenter
Windows Server 2008 R2	Windows Server 2008 R2 Standard Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Datacenter
Windows Server 2008	Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter Windows Server 2008 Standard without Hyper-V Windows Server 2008 Enterprise without Hyper-V Windows Server 2008 Datacenter without Hyper-V Windows Server 2008 Standard 32-bit Windows Server 2008 Enterprise 32-bit Windows Server 2008 Datacenter 32-bit Windows Server 2008 Standard without Hyper-V 32-bit Windows Server 2008 Enterprise without Hyper-V 32-bit Windows Server 2008 Datacenter without Hyper-V 32-bit
Windows Server 2008 64-bit	Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter Windows Server 2008 Standard without Hyper-V Windows Server 2008 Enterprise without Hyper-V Windows Server 2008 Datacenter without Hyper-V
Windows Server 2008 32-bit	Windows Server 2008 Standard 32-bit Windows Server 2008 Enterprise 32-bit Windows Server 2008 Datacenter 32-bit Windows Server 2008 Standard without Hyper-V 32-bit Windows Server 2008 Enterprise without Hyper-V 32-bit Windows Server 2008 Datacenter without Hyper-V 32-bit
Windows Server 2003 R2	Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition

OS name in this manual	Included OS
	Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition
Windows Server 2003 R2 (x64)	Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition
Windows Server 2003 R2 (32-bit)	Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition
Windows Server 2003	Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition
Windows Server 2003 (x64)	Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edit
Windows Server 2003 (32-bit)	Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition
Windows 2000	Windows 2000 Server Windows 2000 Advanced Server

SP is short for Service Pack.

Utility program

For the proper use of Compute Blade server blades, it is highly recommended to install all utilities provided with the product. If utilities are not properly installed, the system may not operate correctly and have trouble detecting or analyzing failures. Please be sure to install the utilities.

Installation manuals and utilities are shipped with devices and/or option cards.

Please refer to “Remote Console Application User’s Guide” for the installation of the remote console utility.

❑ Compute Blade utility program list

Utility name	Function	Applicable OS
Blade Server Manager	Notifies faults; manages power supplies and resources.	Windows
Blade Server manager Plus	Manages N+1 cold standby and rack	Windows
Deployment Manager	Provides OS package; backups system disks.	Windows
CM2/Network Element Configuration	Manages network devices.	Windows
ServerConductor/ Agent	Manages resources, operation, and faults of the system equipment.	Windows、
ServerConductor/ Advanced Agent	Controls power supplies in cooperation with ServerConductor/Agent.	Windows, Linux
MegaRAID Storage Manager	Watch, management, maintenance, and array construction of a disk array controller and physical, logical drive connected to the disk array controller	Windows, Linux
Hfcddutil	Sets various parameters and the persistent binding function into a target adapter.	Linux
HFCtools	Collects error logs for a target adapter.	Windows
One Command Manager	Sets various parameters of adapters, and collects logs.	Windows, Linux
Remote Console application	Functions of power operation, remote video, keyboard, mouse, remote FD, remote CD/DVD are available.	Windows

Information on Support and Service

Missing Parts on Delivery

The product is checked by local support personnel when it is delivered.

In some cases, no checkout work is performed or no local support personnel visit you when the product is delivered. If you find any missing part or if you have any questions on the delivered product in such cases, contact your reseller.

When You Need Help

1 **Refer to the manual.**
Refer to Chapter 13 “When You Need Help” in this manual. Also refer to other printed manuals provided with the product.

2 **Contact us by phone.**

Contact the reseller where you have purchased the product.

Contents

Important Notes ... iii
Reliability of the System Equipment ... iii
Regulatory Compliance Notices ... iii
Notes on Deleting Data when Disposing of or Transferring the System Equipment ... v
Introduction ... vii
Notation ... vii
Utility program ... xi
Information on Support and Service ... xii
Missing Parts on Delivery ... xii
When You Need Help ... xii
Precautions for Safe Use ... xxiv
How to Use the Manuals ... xlviii
Manual Organization ... xlviii
Contents of the Manuals ... xlix
How to Use the Electronic Manual ... l

1. Before Use ... 1

Installation Environment ... 2
Restrictions ... 4
Environment for using System Equipment and Peripheral Equipment ... 4
Handling the System Equipment and Peripheral Equipment ... 5
Electrical Outlets ... 7
Avoiding Problems ... 8
Backing Up Data Back ... 8
Function of RAID ... 8
Preventing Computer Viruses ... 8
Backing Up System Equipment Settings ... 9

2. How to Use the System Equipment ... 11

System Equipment ... 12
Names and Functions ... 12
I/O Slot Expansion Unit ... 35
Names and Functions ... 35

3. Connecting the System Equipment and Powering On ... 43

Install the System ... 44
Connect the System ... 45
Connect the Remote Console ... 45
Remote Console Application (Reclient) ... 46
Remote Console Application (Java Application) ... 46
Connect the USB Cable to the Server Blade ... 62
Connect the Power Cables ... 63
Connect the I/O Slot Expansion Unit ... 68
Connect the Power Cables ... 68

Turn the Power On or Off ... 70
Turn on the Power ... 70
Turn off the Power ... 71

4. Adding Optional Components 73

Mount Internal Optional Components 74

5. Server Blade Setup 75

Standard Server Blade Settings (X55A1/X55A2/X55R3/X55S3/X55R4 Models) 76
Initial Settings with Server Blade Web Console 76
Server Blade Web Console Function 90
[Server Operation] Tab 94
[Server Settings] Tab 103
[Maintenance] Tab 120
[Logs] Tab 123
Standard Server Blade Setup Menu (X55A1/X55A2 Models) 127
EFI Setup Screen 127
Main Menu 128
Advanced Menu 130
Chipset Menu 133
iSCSI Menu 135
Boot Menu 136
Security Menu 139
Save & Exit Menu 140
Standard Server Blade Setup Menu (X55R3/X55S3/X55R4 Models) 141
EFI Setup Screen 141
Main Menu 142
Advanced Menu 144
Chipset Menu 150
Boot Menu 152
Security Menu 156
Save & Exit Menu 157
Remote CD/DVD Boot Procedure 158
Remote Console Application (Reclient) 158
Remote Console Application (Java application) 161
Hardware Memory Dump 167
How to Set Hardware Memory Dump 168
How to Start Hardware Memory Dump 172
Where Hardware Memory Dump is Stored 174
MegaRAID WebBIOS 175
SAS RAID Controller 176
MegaRAID SAS 1078 177
MegaRAID SAS 2108 243
MegaRAID SAS 2208 327
High-performance Server Blade Settings (X57A1/X57A2 Models) 402
Initial Settings with Server Blade Web Console 402
Server Blade Web Console Function 404
[Server Operation] Tab 404
[Server Settings] Tab 414
[Maintenance] Tab 414
[Log] Tab 414
High-performance Server Blade Setup Menu (X57A1/X57A2 Models) 415
EFI Setup Screen 415
Main Menu 416
Advanced Menu 418
Chipset Menu 420
iSCSI Menu 422

Boot Menu....423
Security Menu....426
Save & Exit Menu....427

6. Management Module Settings....429

External Interface for the Management Module....430
Cable Connection for the System Console....432
Connect with LAN Cable....432
Connect with Serial Cable....433
Initial Settings of Management Module....434
Initial Settings of the Management Module via System Web Console....434
Initial Settings of the Management Module via System Console....439
Backing up and Restoring the Settings....441
Backing up the Management Module Settings....441
Restoring the Management Module Settings....443
Backing up the Fibre Channel Card Settings....445
Backing up the LPAR manager Settings....447
Restoring the LPAR manager Settings to the Management Module....448
Restoring the LPAR manager Settings to the Server Blade....450
Account....452
Account Overview....452
Privilege and Role....454
Privilege, Role, and Account....454
System Console Command Reference....455
Command List....455
Basic Operation....457
Chassis Management....462
Partition Management....528
Network Management....543
External Server Connection Manager....569
Managing Security....609
Managing Switch Modules....639
Backing Up and Restoring Settings....643
Association between Commands and Permissions....655
System Web Console....658
Functionality of the System Web Console....658
Login and Logout....661
Operation Screen....661
Status Display....663
Physical Partition Management....665
Server Blade Management....670
I/O Adapter Management....674
Switch Module Management....686
Management Module Management....689
Cooling Fan Module Management....683
Power Supply Module Management....685
Server Chassis Management....687
Session Management....707
Physical Partition Settings....708
User Account Settings....713
Configuration of Network....715
Service Settings....723
Server Chassis Settings....729

Power Settings 730
Time Setting 733
Language Setting 735
Console Settings 736
Backing up and Restoring the Settings 737
SC/BSM Settings 740
HCSM Settings 742
SNMP Settings 744
E-mail Notification 747
HA Monitor Settings 750
LDAP Settings 751
Firmware Management 754
Log Management 757
Detail Display of MARLOG 770
Error Pages 772
SVP (Service Processor Log) Message 774
HCSM (Hitachi Compute Systems Manager) Alert Message 779

7. Configuring the LAN Switch Module 799

Notes on Use 800
Connection to Setup Terminal 802
LAN Interface Connection 802
Serial Interface Connection 804
Command Input Mode Overview 805
Operation Command Mode (For the General User) 805
Operation Command Mode (For the System Administrator) 805
Configuration Command Mode 806
Initial Installation Operation Overview 807
Login 807
Setting the System Administrator’s Password 808
Adding a User ID and Deleting “operator” 808
Backup and Restore of Module Information 810
Connection with the Server Blades 813
Uplink Failover Overview 814
LAN Switch Module Web Console 816
LAN Switch Module Web Console Functions 816
Connection to a LAN Switch Module 818
Operation 819
Display Version 820
Time 821
NTP Server 822
Spanning tree 824
VLAN 825
Link Aggregation 827
Ethernet Port 830
Uplink Failover 835
IPv4 Static Route 836
Log Output 837
Operation Terminal Connection 838
SAVE 839
Copy Configuration File 840

8. Configuring the 10 Gb DCB Switch Module 841

Notes on Use 842
Connection to Setup Terminal 842
Initial Installation Operation Overview....844
Login 845
Setting the Administrator's Password 845
Backup and Restore of Module Information 846
Backing up Configuration....846
Restoring Configuration 846
Connection with the Server Blades....847

9. Configuring the LAN Pass Through Module 849

1 Gb LAN Pass Through Module....850
Notes on Use 850
Connection with Server Blades....851
10 Gb LAN Pass Through Module....854
Notes on Use 854
Connection with Server Blades....855

10. Configuring the Fibre Channel Switch Module 857

Notes on Use 858
Connection to Setup Terminal 859
LAN Interface Connection....859
Serial Interface Connection....861
Initial Installation Operation Overview....862
Connection with Server Blades....863
Backup and Restore of Module Information 867

11. I/O Slot Expansion Unit....869

External Interface for the I/O Slot Expansion Unit 870
Cable connection to the I/O Slot Expansion Unit....872
Connection with LAN Cable....872
Connection with Serial Cable....873
Initial Settings of the I/O Slot Expansion Unit 874
Initial Settings via System Console....874
Backup and Restore the Settings 876
Backup the I/O Slot Expansion Unit Settings....876
Restore the I/O Slot Expansion Unit Settings 877
Account 879
Account Overview 879
Privilege and Role....881
Privilege, Role, and Account....881
System Console Command Reference....882
Command List....882
Basic Operation....884
Chassis Management 888
Network Management....929
External Server Connection Manager....937
Managing Security 969
Backing Up and Restoring Settings 985
Correspondence between Commands and Permissions 987
Alert Log Message 989

12. Logical partitioning manager.....995
LPAR manager Overview 996
LPAR manager Product Specifications.....996
Architecture Overview.....1011
Logical Partitioning.....1012
LPAR manager Introduction.....1037
Console Used in LPAR manager.....1038
Preparation for LPAR manager Boot 1039
Operation Flow.....1041
LPAR manager Boot 1042
EFI Setting 1042
LP Mode setting 1045
LPAR manager firmware bank number selection 1047
Booting LPAR manager 1048
LPAR manager Initial Settings.....1049
Basic Operation of LPAR manager.....1057
Add LPAR and Change LPAR Name 1057
Assign Scheduling Mode and Processors to LPARs.....1061
Change Processor Group Assignment 1065
Change Memory Size Assignment.....1067
Set Auto Activate to LPAR.....1071
Change OS Types on LPARs 1073
Assign PCI Devices to LPARs 1074
Assign USB Devices to LPARs.....1080
Assign Remote Consoles to LPARs 1083
Assign VNICs (Virtual NICs) to LPARs.....1084
Assign Shared FCs to LPARs.....1086
Save Configuration Changed on LPAR manager Screen 1088
Guest OS Operation.....1090
Boot the Guest OS.....1090
Guest OS Display Setting 1139
Shutdown Guest OS and Deactivate LPAR.....1142
Backup of LPAR manager 1145
Backup Files for LPAR manager.....1145
LPAR manager Screen Operations 1147
LPAR manager Screen Display 1147
Move between Guest and LPAR manager Screens 1150
LPAR manager Key Operations.....1152
Summary of LPAR manager Screens.....1156
Quit LPAR manager 1289
Shutting down the LPAR manager system 1289
LPAR manager Functions.....1292
Virtual NIC Functions 1292
Shared FC Functions 1316
Timer Functions 1327
LPAR manager Operating Mode.....1333
Virtual COM Console Function 1337
Logical VGA Snapshot.....1343
Cooperation with ServerConductor.....1343
Guest Memory Dump Function 1344
LPAR manager Dump Collection Command 1348
HVM Management Command 1350
Command for obtaining an overview of system operation.....1351

HCSM....1361
HVM Navigator....1362
Monitoring....1362
Configuration Viewer....1362
LPAR Migration....1362
LP Model Updating....1363
LPAR manager Version Upgrade....1363
Migration between Basic Environment and LPAR manager Environment....1364
LPAR manager Security....1366
Certificates in LPAR manager....1366
Management Interface Security....1369
Cautions....1371
Emulex 10 Gb NIC-1 Gb Switch Module....1371
Emulex 10 Gb NIC-10 Gb Switch Module....1371
Setting FC Switch....1372
Using Shared FC....1372
Connection Type for Shared FC Port....1372
Notes on SMP Configuration....1374
Restriction on X55R3/X55S3 with 2-core CPU....1377
Restriction on TPM (Trusted Platform Module)....1377
Notes on adding NIC....1377
Restriction on Emulex 10 Gb NIC....1378
System Requirements for LPAR manager and LPAR....1379
Setting LPAR manager System....1379
Maximum Resolution....1379
Setting Guest OS Display....1380
Serial Setting with Guest Screen in Use....1380
Using Linux....1380
Using Windows....1380
NETM/Remote Control....1381
Notes on ServerConductor/Blade Server Manager....1381
Notes on ServerConductor/Deployment Manager....1383
SC/Advanced Agent....1383
Power Capping....1384
Processor Capping....1384
Assigning Processors when SMT Enabled....1384
Degeneration/Isolation of Processors, Memories, and PCI Devices....1386
Degeneration of Processor Cores....1386
Using USB Device....1387
Memory Size Assigned to LPAR....1388
LPAR Memory Fragmentation....1389
Hardware Memory Dump....1392
Memory Space with Hardware Memory Dump Enabled....1393
Maximum Number of NIC Ports Assigned to an LPAR on Linux....1394
Maximum Number of NIC Ports Assigned to an LPAR on Windows....1394
Notes on using SR-IOV....1403
View of Shared NIC/Virtual NIC using the ethtool Command....1408
Remote Console....1408
Detecting Shared NIC Linkdown....1408
Breakdown of Inter-LPAR Communications....1409
Impact on LPAR manager by I/O Slot Expansion Unit Modes....1411
Timeout for Saving Configuration....1412
Settings for WWN and MAC address....1412
N+M Cold Standby....1413

Time Setting in Switchover and Recovery with N+M Cold Standby 1413
Time Difference at N+M Cold Standby 1415
N+M Cold Standby with Virtual NIC System Number Expansion 1415
UPS (Uninterruptible Power Supply) 1415
Powering Off LPAR manager 1416
Boot Option Settings 1416
Shared FC Port Status 1417
Notes on LPAR manager Shutdown 1417
Flash Memory Failure 1417
Performance Slowdown in Management Path 1418
Note on Oracle IPMI 1418
LPAR manager Setting Item 1419
LPAR manager System Setting 1419
LPAR manager Partition Setting 1421
HBA EFI Driver Setting 1423
LPAR manager Setting Change and Affected Area 1426
Port Numbers Used by LPAR manager 1428
System Configuration 1429
Example of System Configuration (Network) 1429
Example of System Configuration (Connected to Storage via FC Switch) 1431
Example of System Configuration (Directly Connected to Storage) 1433
Example of System Configuration (Hardware Configuration) 1435
Connection to 1 Gbps LAN Switch Module 1436
Connection to 1/10 Gbps LAN Switch Module 1437
Connection between 8 Gbps FC Switch Modules and 2-port FC Mezzanine Cards 1438
Connection between 8 Gbps FC Switch Modules and 4-port FC Mezzanine Cards 1439
LPAR manager Boot Messages 1440
LPAR manager On-Screen Messages 1452
LPAR manager System Logs Screen Messages 1453
HCSM (Hitachi Compute Systems Manager) Alert Message 1480
Software License 1482
Information on Software License 1482

13. System Operation and Management 1485

Server Blade Operation 1486
Symmetric MultiProcessing (SMP) between Server Blades 1486
OS Console (Serial Console Redirection) 1488
Notes on the Wake On LAN (WOL) Functionality 1494
Operation of I/O Slot Expansion Unit 1496
Overview of I/O Slot Expansion Unit 1496
Operation Mode of I/O Slot Expansion Unit 1497
Network Settings 1499
List of Module Management Interfaces 1499
Management Network 1500
Internal Network 1501
Setting the Connection Method 1502
Setting the IP Address 1503
Port Selection for Management Interface Connection 1504
Management Interface Connection Using Tag-VLAN 1506
Network Configuration at Management Module Failover 1508
Link Fault Tolerance (LFT) 1509

Setting Management Server Information
for ServerConductor/Blade Server Manager 1511
HCSM (Hitachi Compute Systems Manager) 1513
Notes on Connection between HCSM and a Management Module 1513
Management by HCSM 1513
Relation with ServerConductor/BladeServer Manager 1514
WWN in the Compute Blade 2000 1515
MAC Address in the Compute Blade 2000 1517
Smart Configure 1518
Overview of Smart Configure 1518
Method of Smart Configure 1519
Smart Configure Execution Triggers 1520
Operation of Partitions during Smart Configure 1521
Time Required for Smart Configure 1521
N+M Cold Standby 1522
N+M Cold Standby Overview 1522
Mechanism of the N+M Cold Standby 1524
Prerequisites for the N+M Cold Standby 1530
Smart Configure in N+M Cold Standby 1533
Procedure for Implementing the N+M Cold Standby 1534
Setting Change after Configuring the N+M Cold Standby 1539
Changing CNA after Configuring the N+M Cold Standby 1539
UPS Connection for the N+M Cold Standby 1540
RTC Time Synchronization at N+M Cold Standby Failover 1541
Digital Certificates for the System Web Console 1543
Overview of Digital Certificates for the System Web Console 1543
Procedures to Use Digital Certificates for the System Web Console 1555
E-mail Notification 1555
E-mail Notification Overview 1555
E-mail Notification Setup 1558
SNMP Function 1562
SNMP Function Overview 1562
How to Use the SNMP Function 1564
MIB Reference 1568
SNMP Function for I/O Slot Expansion Unit 1693
SNMP Function Overview for I/O Slot Expansion Unit 1693
How to Use the SNMP Function for I/O Slot Expansion Unit 1695
MIB Reference for I/O Slot Expansion Unit 1698
LDAP Server Linkage 1727
Overview of the LDAP Server Linkage 1727
Supported LDAP Server 1728
Environmental Setting for Active Directory 1728
Setting Management Modules and Server Blades 1739
Setting Group Authentication 1741
Power Efficiency 1742
Power Monitoring 1742
Power Capping 1744
DBS (Demand Base Switching) 1746
Optimized Power Supply Module Control 1747
Control of Maximum Power Consumption 1747
Dictionary Updating 1748
Updating Dictionary 1749
Operation Log 1752

Operation Log Overview 1752
Operation Log Messages 1756
Syslog Transfer 1766
Overview 1766
Audit events to transfer 1767
Log format 1767
Using Syslog transfer 1767
Notes on Windows 1769
Memory Dump in No System Response 1769
Complete Memory Dump 1770
Useful Settings for Red Hat Enterprise Linux 1771
Using Parameters to Stop the System at Hardware Failure 1771
System Time Delay with Red Hat Enterprise Linux 5 (x86) 1773
System Problems by Error in Detecting Frequency of APIC Timer at OS Boot 1775
Hardware Memory Dump 1777
Hot-Plug Module with PCIe Error Isolation Mode Enabled 1778
TCP Checksum Offload 1779
Additional Setting for Kdump Configuration with 1-TB Main Memory 1780
CPU Planned Degradation with 4-blade SMP (X57A1/X57A2 models) 1780
Useful Settings for VMware 1781
Using Parameters to Stop the System at Hardware Failure 1781
PCI Error Handling Mode 1784
PCI Error Handling Mode Available for OS/Virtual Environment 1785
Devices Supporting PCIe Error Isolation Mode 1787
SMASH for Server Blades 1790
SMASH Overview 1790
SMASH Features 1790
Connection to SMASH-CLP 1791
Connection to SMASH using WS-MAN 1795
IPMI Commands List 1800
Security of Management Interfaces 1802
Network Communication by the System Equipment 1802
Security Strength 1803
Relationship between Security Strength and Functions 1804
User Setting for Security Strength 1806
Functions Depending on the Security Strength 1807

14. When You Need Help 1811

Troubleshooting 1812
Server Blade Problems 1812
Fan Module Problems 1815
Management Module Problems 1816
Power Supply Module Problems 1817
How to Display the Screen of Server Blade 1818
To Remotely Display the Screen 1818
Memory Dump Collection 1819
Memory Dump for Windows 1819
Memory Dump for Linux 1821
Memory Dump for VMware 1822
Error at Server Blade Startup 1825
When Error Messages Appear 1825

15. Maintenance and Replacement Parts 1827

Items Requiring Routine Maintenance 1828
Cleaning 1829
System Equipment 1829
I/O Slot Expansion Unit 1830
Service Life Limited Parts 1831
Notes on Maintenance 1832

Appendix: Specifications

Glossary

Precautions for Safe Use

Items of precautions for safe use are indicated with safety alert symbols and headings, “WARNING”, “CAUTION”, and “*NOTICE*” as shown below.

	This is a safety alert symbol. It calls attention to a potential safety hazard to humans. In order to avoid possible injury or death, follow the message provided after this symbol.
 **DANGER**	This indicates information about how to avoid physical injury to yourself and others.
 **WARNING**	This symbol indicates the presence of a potential risk that might cause death or severe injury.
 **CAUTION**	This symbol indicates the presence of a potential risk that might cause relatively mild or moderate injury.

NOTICE	This symbol indicates the presence of a potential risk that might cause severe damage to the equipment and/or damage to surrounding properties.



[Example 1: hazard identification]
The equilateral triangle filled in with yellow △ indicates a precaution. A safety alert symbol inside the triangle △ indicates the type of hazard, such as “an electric shock hazard”.



[Example 2: prohibition]
The red circle with a red diagonal bar ⦸ indicates an action that you must not take. The red diagonal bar ⦸ is placed over a figure that depicts the “must-not” item involved, such as a screwdriver to disassemble a device. The red circle with a red diagonal bar without a symbol indicates the general prohibition.



[Example 3: mandatory action]
The circle filled in with blue ● indicates an action to take. A white figure inside the circle ● shows the action to take, such as unplugging the power cable from the outlet. The same circle with an exclamation mark ❗ indicates generally should-take actions.

Common precautions concerning safety

Please carefully read through these safety instructions to follow:

- When operating the equipment, follow the instructions and procedures provided in the manual.
- Be sure to follow notes, cautionary statements and advice indicated on the equipment or in the manual.
- Referring to manuals attached to other products which you install in or connect to the equipment, follow the instructions described in those manuals.
-

Failure to follow those instructions can cause injury, fire or damage to property including the equipment.

Operations and actions to perform

Do not perform operations or actions other than those described in the manual.
Should you find any problem with the equipment, turn off the power, unplug the power cable from the electrical outlet, and then contact your reseller or call for maintenance personnel.

Pay attention

The equipment and the manual carry notes, cautionary statements and advice that have been fully examined and reviewed. However, unforeseeable situations may occur. When operating the equipment, always stay alert as well as follow instructions.

Precautions for Safe Use

General Safety Precautions

Always follow these instructions shown below when handling the equipment.





Handling of power cables

Always use the power cables shipped with the equipment, and follow the instructions below: Failure to follow the correct handling practices lead to damaging the power cables to expose the copper wires and to overheat due to short-circuiting or partial disconnection, which may cause electric shock or fire.

- Do not place any object on the power cables.
- Do not pull the power cables.
- Do not apply pressure on the power cables.
- Do not fold the power cables.
- Do not twist the power cables.
- Do not work upon the power cables.
- Do not use the power cables near heat-generating appliances.
- Do not heat the power cables.
- Do not bundle the power cables.
- Do not fasten the power cables with staples.
- Do not use nicked power cables.
- Do not subject the power cables to ultraviolet or strong visible light continuously.
- Keep the power cables from contact with alkali, acid, fat and oil, or humidity.
- Do not use the power cables in a high-temperature environment.
- Do not use the power cables above their specified rating.
- Do not use the power cables for other devices.
- Be sure to hold the plug section when inserting or removing the power cable.
- Do not touch the power plug with moistened hands.

Do not place any objects around the electrical outlets in order to allow users to quickly unplug the power cables.




Poor contact and tracking

Comply with the following instructions when handling the power plug. Otherwise, tracking or poor contact may cause overheating and a fire.

- Make sure that the power plug is fully and securely inserted into the electrical outlet.
- Before inserting the power plug, confirm that there is no dust or a water droplet on the plug. If any dust or water droplet is found, wipe it off with a dry cloth and then insert it.
- Check that the outlet can firmly hold the plug.
- Qualified technical personnel should work on the electrical outlet.

Precautions for Safe Use




Handling of batteries

Since maintenance personnel should change batteries, do not change them yourself. Follow the instructions described below. Inappropriate handling can result in injury because the battery can overheat, burst, and catch fire.

- Do not put the battery on charge.
- Do not short out the battery.
- Do not disassemble the battery.
- Do not heat the battery.
- Do not deform the battery.
- Do not incinerate the battery.
- Do not moisten the battery.





Abnormal heat, smoke, abnormal noise, or abnormal smell

Should you find anything abnormal occurring, turn off the power and unplug all the power cables of the equipment (maximum of 4) from the electrical outlets. Using the power cables after such occurrences can lead to an electric shock or fire.

Do not place any objects around the electrical outlets to allow users to quickly unplug the power cables.





Do not repair, remodel or disassemble

Do not attempt to repair, remodel or disassemble the equipment on your own, except for performing expansion work in accordance with the instructions in this manual. Work performed by unqualified persons can lead to an electric shock, fire, or burns. Especially it is hazardous if you touch areas inside the high-voltage power unit.





Removal of the cover or bracket

Do not remove the cover or bracket. It can result in an electric shock, burns or equipment failure.

Precautions for Safe Use




Requirements for power outlets

- Use a grounding 2-pole plug-in power outlet. Outlets of any other types would cause an electric shock or fire.
- In order to prevent an electric shock, connect the outlet's grounding electrode to a grounding terminal installed by a qualified electrician. Without connection to the grounding terminal, an electric shock can occur in the event of a failure in power supply modules.





Plugging and unplugging

- When inserting the power plug into the electrical outlet or removing it, be sure to hold the plug section. Do not pull the cable; it can partially break the wire, overheat the broken part and lead to a fire.
- Be sure to handle the power plug with a dry hand when inserting or removing it into/from the outlet. Handling it with a moistened hand can cause an electric shock.



Cover for the power supply module

When a power supply module is in operation, the cover and handle get hot. Be careful when replacing a failed module. You can get burned.



High temperature at the 10GBASE-R transceiver

The 10GBASE-R transceiver in the 10Gbps LAN switch module gets hot in operation. To remove the transceiver, therefore, allow at least approximately 5 minutes after the power supply for the 10Gbps LAN switch module is turned off from the management module. Failure to do so can cause you to get burned.




Laser beam

- On this product, a Class 1 laser product is installed. Do not look directly at the laser beam. Do not look at the laser beam using an optical instrument.
- Under the laser module cover, a laser beam is being emitted. Do not remove the cover of an unused board.



Plastic bags for packaging

To avoid danger of suffocation, do not leave plastic bags, such as air bubble cushioning for packaging, within reach of children.



Requirements for the product

Install the product on a fixed rack. Do not lean against the product or stand on it.
Do not install the product in a place with weak floors and walls.
Do not subject the product to excessive vibration. That can drop and fall the product, leading to failure.

Precautions for Safe Use



Do not place objects on the equipment

Do not place a vase, potted plant or any other container with water in it, or small metal items like pins and clips, on the equipment. Operating the equipment with conductive objects inside, such as metal and water, could lead to an electric shock, smoke, or a fire.



Use for purposes other than the original purpose

Do not use the equipment for any purpose other than its original purpose, such as for a step or bookends. If you do, the equipment may fall or malfunction, which causes injury or failure.



Installing the equipment in a rack

- To install or remove the system equipment in or from the rack cabinet, always get help from at least one other person or use tools. If the system equipment has to be installed on 31U and above of the rack cabinet or it is already installed there, call for maintenance personnel instead of attempting to install or remove it. Defective installation may cause the system equipment to fall, resulting in injury or equipment failure.
- To perform any operation with the equipment pulled out from the rack cabinet, be sure to install a stabilizer into the rack cabinet. Applying excessive force could cause the rack cabinet to fall, resulting in injury or equipment failure. If a stabilizer is not installed, call for maintenance personnel.



Locking the rail into place

Be sure to pull out the equipment until it locks into place. If not, the equipment may move unexpectedly, which causes you to get injured such as your finger caught in the gap.



Adding and replacing parts

The cover and internal parts are hot immediately after the power is turned off. You must wait for about 30 minutes before adding or removing internal parts unless otherwise specified in this manual. If not, the hot equipment causes you to get burned.



Contact with metal edges

When moving the equipment or adding parts, take care not to hurt yourself on the metal or plastic edges. You can wear cotton gloves to protect your hands.



Eye fatigue

Provide luminance of 300 to 1000 lux for viewing the display. Take a break of 10 to 15 minutes every hour. Viewing the display for many hours could cause eyestrain.

Precautions for Safe Use

Signal cables

- Route cables not to trip over them. Tripping over cables could cause injury or failure of devices connected to the equipment, and also could cause loss of valuable data.
- Do not place heavy items on the cables. Avoid routing cables close to a thermal appliance. If you do, it could cause damage to cable sheaths, resulting in failure of the connected devices.

Disposal of the equipment

- For disposal by a business operator
  Check the industrial waste disposal regulations in your country and follow the necessary procedures.
- For disposal by an individual
  Consult your reseller or follow the relevant regulations in your region.

Precautions for Safe Use

Precautions against Damage to Equipment



Insertion of foreign objects into the equipment

Do not allow clips, pins or any other metal items or flammable items to enter the equipment through a vent or by any other means. Continuing to operate the equipment with foreign objects could cause failure.



Spraying smoke or fine mist

Turn off the power to the system equipment and completely wrap the entire system equipment with a plastic sheet before spraying smoke or fine mist from a can such as an insecticide. The smoke or fine mist, which enters inside of the equipment, can cause failure.



Impact from falling

Do not fall the equipment or hit it against another object. It can cause internal deformation and deterioration. Operating the equipment under such defective conditions can cause failure.



Vent

A vent is used for preventing rise in temperature inside the equipment. Do not block the vent by placing or leaning an object. If you do, the temperature rises, which can cause failure. Check and clean ventilation holes periodically to keep the dust from gathering on them.



Power supply module

Since the power supply module has a high-voltage area in it, do not open the cover. If you do, it can result in an electric shock or equipment failure.



Contact with connection terminals

- Do not touch connection terminals, such as a connector, with your hand or any metal item. Do not insert any objects such as wire into them. Do not place the equipment in a place with metal pieces. If you do, a short circuit can be developed, causing equipment failure.
- When you have to touch the card, be careful not to hurt yourself. You can wear cotton gloves. Without caution, it can cause injury.



Not designed to operate outdoors

Do not operate the equipment outdoors. If you do, it could cause a failure.

Precautions for Safe Use

Installation environment

Meet the installation environment requirements for the system equipment shown in Chapter 1. If you use the equipment in the environment with temperatures higher than the permissible temperature, increase in internal temperature can cause a failure in equipment.

Moving between two locations with a temperature differential

When you move the equipment from one location to another, a significant temperature gap between the two locations may cause condensation on the surface or inside the equipment. Operating the equipment with condensation inside can cause a failure in equipment. Leave the equipment at the new location for several hours until the equipment temperature conforms to that of the new environment before you start using it. When you move the equipment from an environment with temperature 5°C to that with 25°C, for example, leave it for about two hours.

Adding and connecting to peripheral devices

Before adding or connecting peripheral devices to the equipment, remove all power plugs from the outlets and disconnect all cables from the equipment unless otherwise instructed. Use only peripheral devices which are explicitly listed as supported in the manual, and always follow the instructions in the manual. Using devices other than those mentioned above would cause a failure in peripheral devices and equipment due to the difference in connection specifications.

Consumables

Use only specified consumables. Using consumables other than those specified would not only reduce reliability of the product but also cause a failure, electric shock, or fire.

Radio interference

When you install the equipment next to another electronic device, the radio waves may interfere with each other. In particular, a television set or a radio in the vicinity may make a noise. If this happens, do the following:

- Place the equipment as far away as possible from the TV or radio.
- Change the antenna orientation of the TV or radio.
- Plug these cables into separate electrical outlets.

Precautions for Safe Use

Anti-earthquake measures

Strong vibration such as that generated by an earthquake could cause the equipment to move, fall, and be thrown out of the window, which results in serious accidents. In order to prevent disastrous outcomes, consult a maintenance company or an expert business for developing counter-seismic measures to implement them accordingly.

Handling hard disks

A hard disk is a precision instrument. Handle it carefully when you use it. Inappropriate handling could result in hard disk failure.

- When carrying the system equipment or hard disk, handle it carefully not to vibrate or hit it. Before handling a hard disk, remove static electricity or wear cotton gloves.
- Before moving the system equipment, turn off the power, remove the power plug from the electrical outlet, and wait for at least 30 seconds.

Rat control

Rats can cause the following damage to a computer system:

- Breakage of cable sheaths
- Corrosion, contact failure, or soiled parts inside the equipment

In order to prevent the above damage, consult an expert business for developing rat control measures and implement them accordingly.

Faulty disk

- If you attempt to replace faulty disks using an incorrect procedure or faulty alternative disk, data on the disk can be corrupted. Before replacing the disk, back up the data.
- Replacing a hard disk without failure would corrupt the data on it. Do not remove any hard disk other than the faulty disk.

Precautions for Safe Use

Warning Signs in the Manual

⚠ WARNING

Handling of heavy loads

- Since the equipment is heavy, be careful when you move it. Handling of this equipment without extra care can hurt your arms or back.
- To relocate or lift heavy loads such as this product, use tools or perform the task with the help of at least another person. If not, handling of heavy loads could lead to injury or equipment failure.

  Refer to [Chapter 3: Install the system].

Multiple connections to a single outlet not allowed

Do not connect multiple power cables to a single electrical outlet. Overheating the power cables or outlet would cause a fire and trip the circuit breaker, which affects other devices on the same circuit.

Refer to [Chapter 3: Connect the Power Cables; Connect the I/O Slot Expansion Unit].

Not designed to operate in a humid or dusty environment

Do not use the equipment near a place where water is used such as a bath tab, washing stand, sink, washing machine, or swimming pool; in a humid basement, or in a dusty place. Such conditions can lower electric insulation, which can cause an electric shock or fire.

Refer to [Chapter 1: Installation Environment].

Cleaning

- Turn off the power and pull out the power cable before cleaning the system equipment. If not, the cleaning could cause an electric shock or equipment failure.
- Turn off the power and pull out the power cable before cleaning the I/O slot expansion unit as well. If not, the cleaning could cause an electric shock or equipment failure.

  Refer to [Chapter 14: Cleaning].

Precautions for Safe Use

⚠ CAUTION

Handling of the system equipment

Adding or replacing optional components inside the system equipment must be performed by maintenance personnel. Do not attempt to remove the cover of the equipment. Do not attempt to install or remove optional components. Since parts implemented in the system equipment are high-density, operation or maintenance by inexperienced persons leads to injury or equipment failure. When you need to add or replace optional components, contact your reseller or call for maintenance personnel.

Refer to [Chapter 4: Mount Internal Optional Components].

Using at an unstable place

Do not place the equipment in an unstable place such as an inclined ground and narrow place. The equipment can fall and cause injury.

Refer to [Chapter 1: Installation Environment].

Precautions for Safe Use

NOTICE

Backing up data

Always create backup copies of important data on a hard disk to auxiliary storage. If the hard disk fails, all data stored on the disk will be lost.

Refer to [Chapter 1: Handling the System Equipment and Peripheral Equipment].

Disk array

- You must not change a disk array during system operations. If you do, all data will be lost from those disks due to change in the disk array.

  Refer to [Chapter 5: Building Disk Arrays].

- When enabling the write cache of the disk array, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

  Refer to [Chapter 5: Virtual Drives; Building Disk Arrays for RAID 0, 1, 5, and 6; Building Disk Arrays for RAID 10; Changing the Write Policy for Disk Arrays].

- When a disk array is deleted, all data in those hard disks including the disk array information will be lost. Backup your required data before deleting a disk array.

  Refer to [Chapter 5: Deleting Disk Arrays].

- When a disk array is initialized, all data in those hard disks including the disk array information will be lost. Backup your required data before initializing a disk array.

  Refer to [Chapter 5: Initializing Disk Arrays].

- If you select [New Configuration], all data in those hard disks including the disk array information will be lost. Backup your required data before selecting “New Configuration”.

  Refer to [Chapter 5: Building Disk Arrays for RAID 0, 1, 5, and 6; Building Disk Arrays for RAID 10].

Precautions for Safe Use

NOTICE

Controller properties submenu 2

This setting item is not supported. Do not use this setting.

Refer to [Chapter 5: MegaRAID WebBIOS].

Schedule Consistency Check setting submenu

This setting item is not supported. Do not use this setting.

Refer to [Chapter 5: MegaRAID WebBIOS].

Power operation

Follow the prescribed procedure for power operation. Powering on or off not according to the prescribed procedure can cause equipment failure.

Refer to [Chapter 3: Turn the Power On or Off].

Connecting a cable to the management module

If a device with the same IP address as that for the BMC on the management module or server blade exists on the network, a failure will occur on the system equipment when you connect the management module to a network.

Complete a network configuration before connecting a cable to the management module.

Refer to [Chapter 6: Cable connection for the system Console].

Precautions for Safe Use

NOTICE

N + M cold standby function

- When the N+M cold standby function is enabled, the power LED on the front panel lights solid orange, Smart Configure is automatically executed, and then the status LED (CND) on the server blade lights solid green. Confirm that the power LED of the front panel lights solid orange to show Smart Configure is completed before pressing the power button of the server blade for a second or more.
  For a system with N+M cold standby configured, you cannot update LPAR manager firmware versions on all server blades at a time. Then, discrepancies between firmware versions of server blades are allowed only when the LPAR manager firmware version on a standby server blade is later than that on the active server blade.

  Refer to [Chapter 3: Turn the Power On or Off].
- Do not operate the server blade during Smart Configure. If you do, Smart Configure may fail.

  Refer to [Chapter 13: Overview of Smart Configure].
- Make sure to apply the same LPAR manager firmware version with the active partition to the standby partition. If you apply different LPAR manager firmware versions to the active and standby partition, N+M failover may fail.

  Refer to [Chapter 13: Mechanism of the N+M Cold Standby].
- Do not set the EFI Shell to the highest booting priority in the EFI Setup menu. If the EFI Shell is on the top of the boot option, the OS will not successfully boot after N+M switching and failback.

  Refer to [Chapter 13: Procedure for Implementing the N+M cold Standby (1)].
- With a standard server blade, executing the Smart Configure changes the SAN boot priority to the lowest automatically.

  Refer to [Chapter 13: Procedure for Implementing the N+M cold Standby (4)].
- If you change the LPAR configuration (processors, memory, or device assignment), make sure to implement [F9]: “Save Configuration” on the LP Menu screen. For details, see “Save Configuration Changed on LP Screen”.

  Refer to [Chapter 13: Procedure for Implementing the N+M cold Standby (4)].
- When a switching alert is issued by the BSM command, the active partition is forcibly powered off.

  Refer to [Chapter 13: Procedure for Implementing the N+M cold Standby (5)].

Precautions for Safe Use

NOTICE

Uplink failover

- This function cannot be set with spanning tree, GSRP, or VRRP.

  Refer to [Chapter 7: Uplink Failover Overview].

- When setting this function to the port of a link aggregation, set this to the channel group to which the port belongs.

  Refer to [Chapter 7: Uplink Failover Overview].

- Set this function only when the target external port and the link aggregation channel group have linked up.

  Refer to [Chapter 7: Uplink Failover Overview].

First Aid for Electric Shock

First aid is the help you can provide before you can get professional medical help. For serious conditions, it is vitally important to take the victim to a doctor as soon as possible. Have someone call an ambulance at once while you apply first aid.

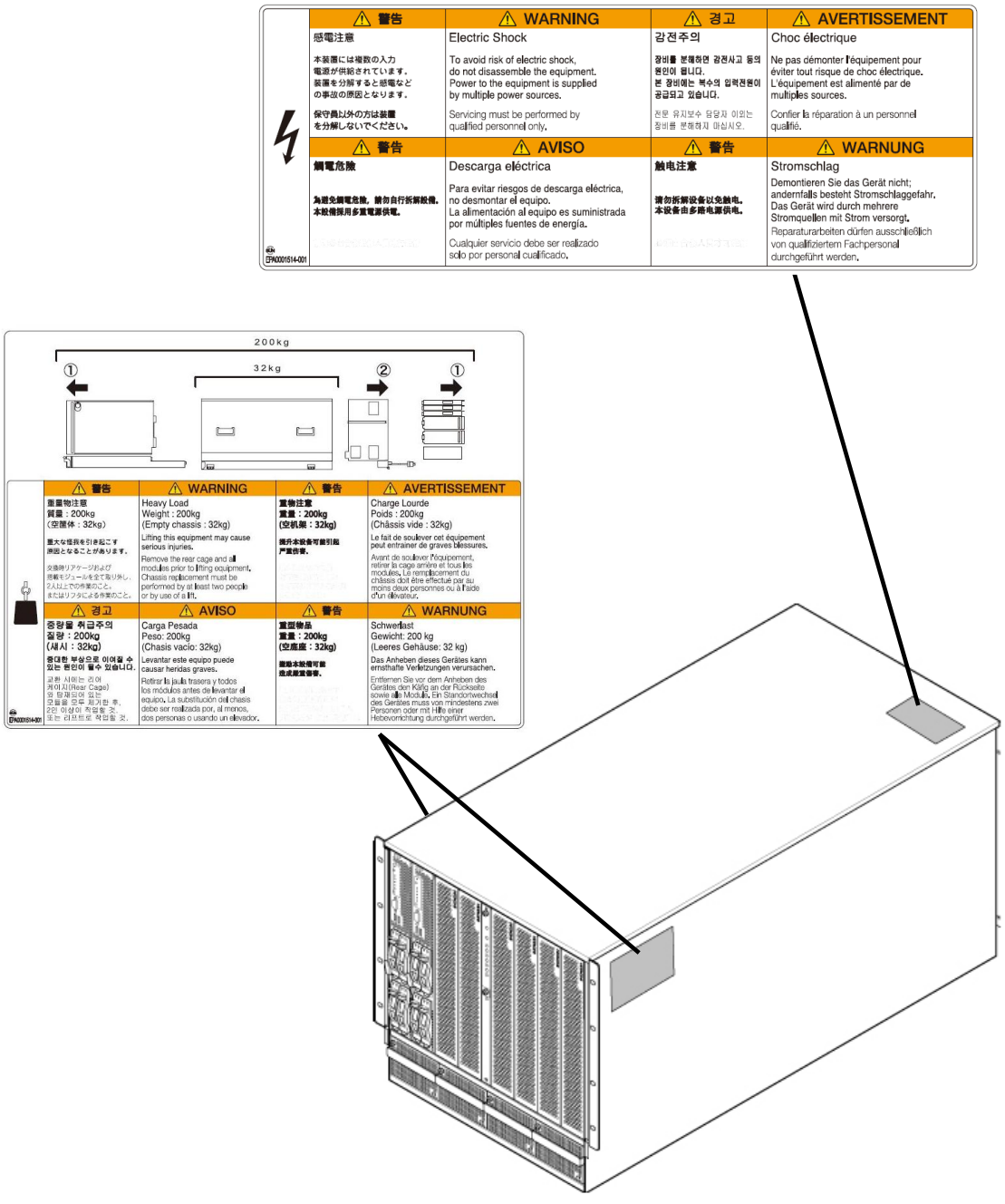
Break the victim's contact with the source of electricity in the quickest safe way possible. Turn off the main switch of the power distribution panel immediately and ground the circuits. Remove the victim from contact with the current, using a dry wooden pole, a dry rope or dry clothing. Do not touch the victim before contact with the current is broken.

Warning labels

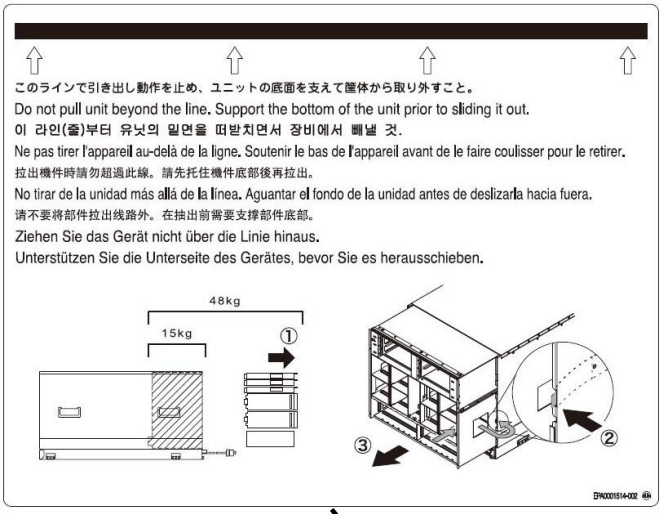
Warning labels can be found at the following locations on the system equipment.

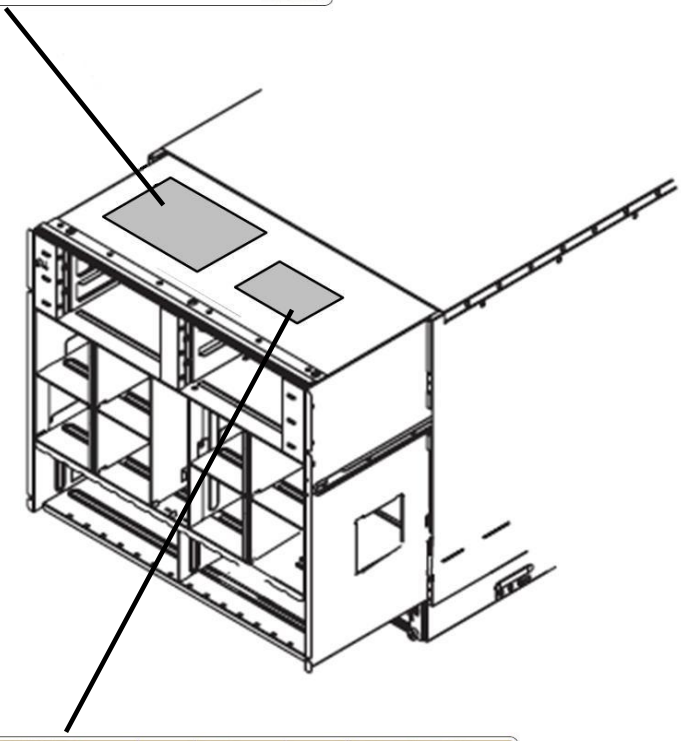
❑ Chassis

[Front View of A1/A2 Chassis]



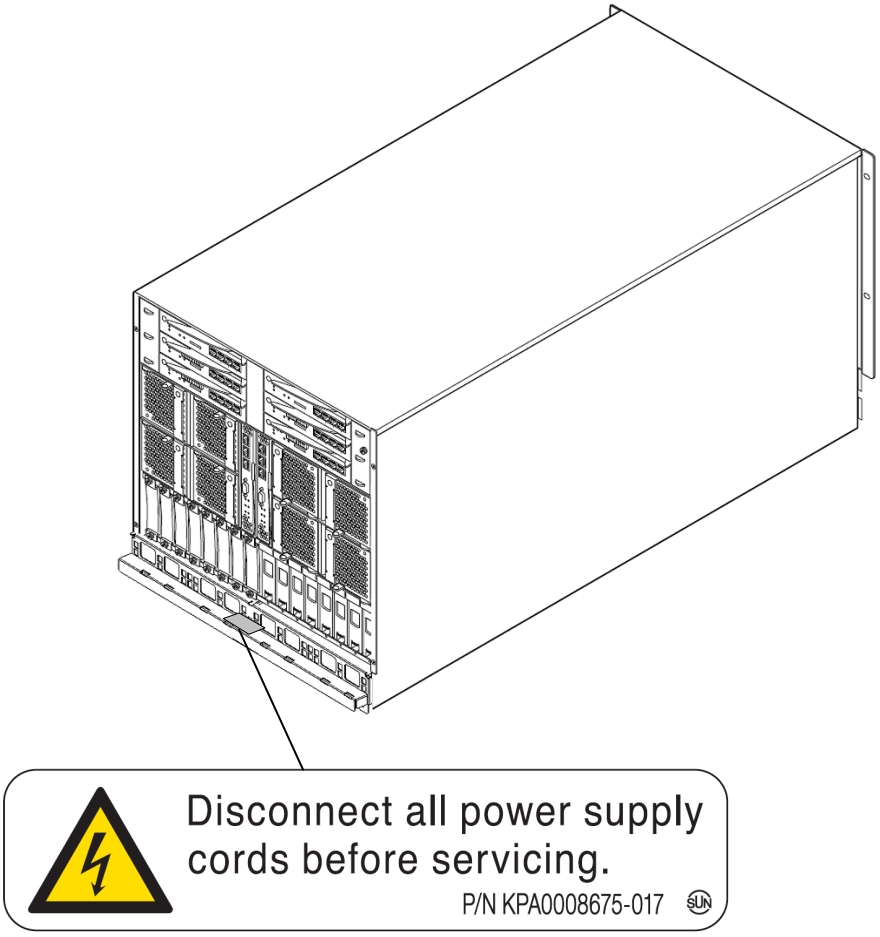
[Rear View of A1/A2 Chassis]



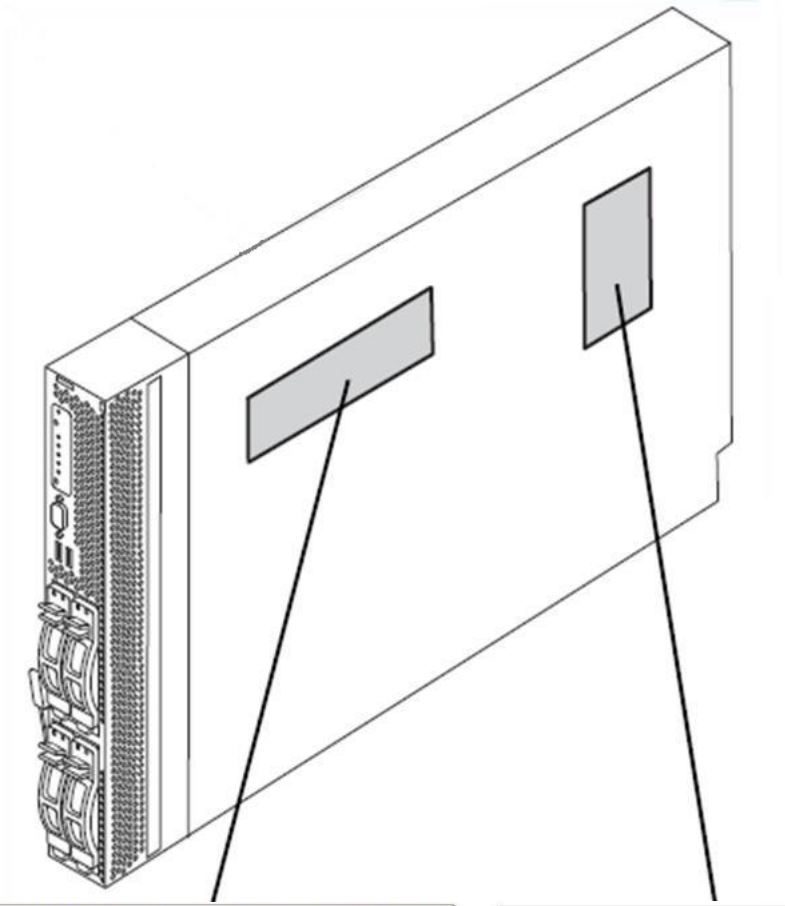




[Rear View of A2 Chassis]



❑ Server Blade



	⚠ 注意	⚠ CAUTION	⚠ 주의	⚠ ATTENTION
>60℃	高温注意 火傷の危険有り。 3分以上待ってから カバーを開けること。	CAUTION - High Temperature CAUTION hot, risk of serious burn injuries. Wait 3 or more minutes prior to opening cover.	고온 주의 화상을 입을 위험이 있습니다. 3분 이상 기다린 후 덮개를 여십시오.	ATTENTION - Prudence à haute température ATTENTION - Risque de brûlures graves. Attendre au moins 3 minutes avant d'ouvrir le couvercle.
	⚠ 小心	⚠ PRECAUCIÓN	⚠ 注意	⚠ ACHTUNG
	小心 - 高温 小心，高温可能导致严重灼伤	PRECAUCIÓN - Alta Temperatura PRECAUCIÓN, caliente, riesgo de graves lesiones por quemadura. Esperar 3 o más minutos antes de abrir la tapa.	注意-高温 注意-灼伤危险。	ACHTUNG - Hohe Temperaturen ACHTUNG heiß, Gefahr von schwerwiegenden Verbrennungen. Warten Sie mindestens drei Minuten, bevor Sie das Gehäuse öffnen.

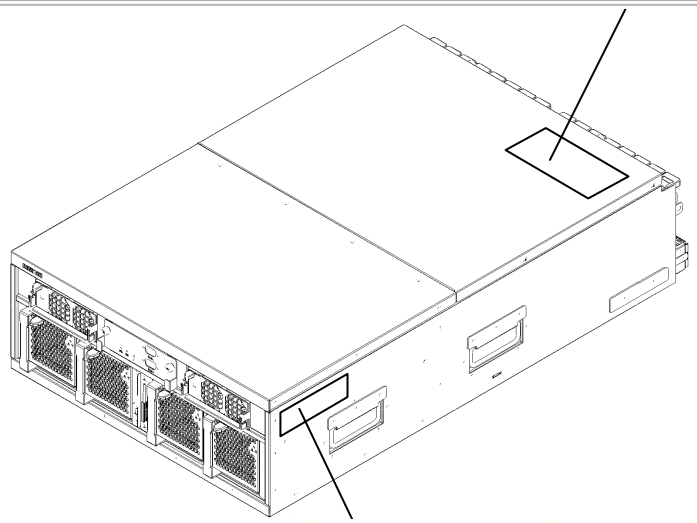
EPA0001614-101



❑ I/O Slot Expansion Unit

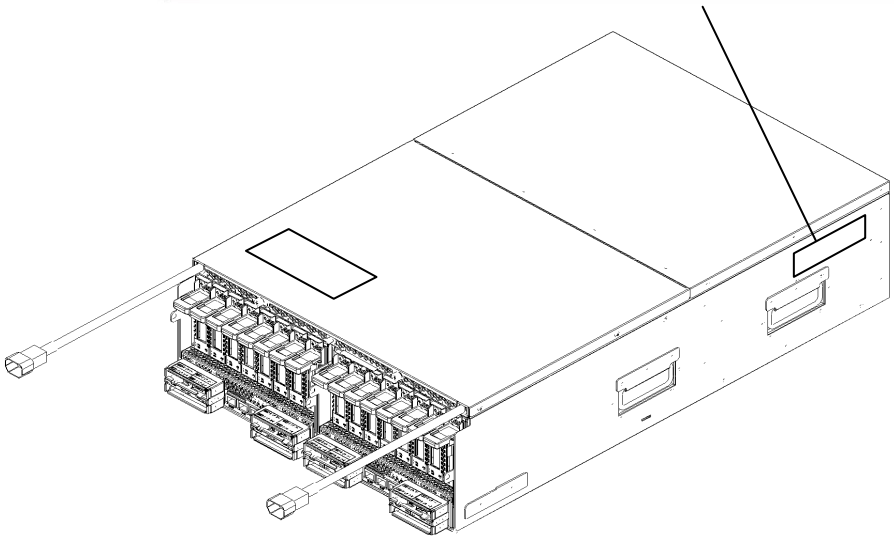
⚠ 警告	⚠ WARNING	⚠ 경고	⚠ AVERTISSEMENT
感電注意 本装置には複数の入力電源が供給されています。 装置を分解すると感電などの事故の原因となります。 保守員以外の方は装置を分解しないでください。	Electric Shock To avoid risk of electric shock, do not disassemble the equipment. Power to the equipment is supplied by multiple power sources. Servicing must be performed by qualified personnel only.	감전주의 장비를 분해하면 감전사고 등의 원인이 됩니다. 본 장비에는 복수의 입력전원이 공급되고 있습니다. 전문 유지보수 담당자 이외는 장비를 분해하지 마십시오.	Choc électrique Ne pas démonter l'équipement pour éviter tout risque de choc électrique. L'équipement est alimenté par de multiples sources. Confier la réparation à un personnel qualifié.
⚠ 警告	**⚠ AVISO**	**⚠ 警告**	**⚠ WARNUNG**
觸電危險 為避免觸電危險，請勿自行拆解設備。 本設備採用多重電源供電。	Descarga eléctrica Para evitar riesgos de descarga eléctrica, no desmontar el equipo. La alimentación al equipo es suministrada por múltiples fuentes de energía. Cualquier servicio debe ser realizado solo por personal cualificado.	触电注意 请勿拆解设备以免触电。 本设备由多路电源供电。	Stromschlag Demontieren Sie das Gerät nicht; andernfalls besteht Stromschlaggefahr. Das Gerät wird durch mehrere Stromquellen mit Strom versorgt. Reparaturarbeiten dürfen ausschließlich von qualifiziertem Fachpersonal durchgeführt werden.

EPA0001514-001



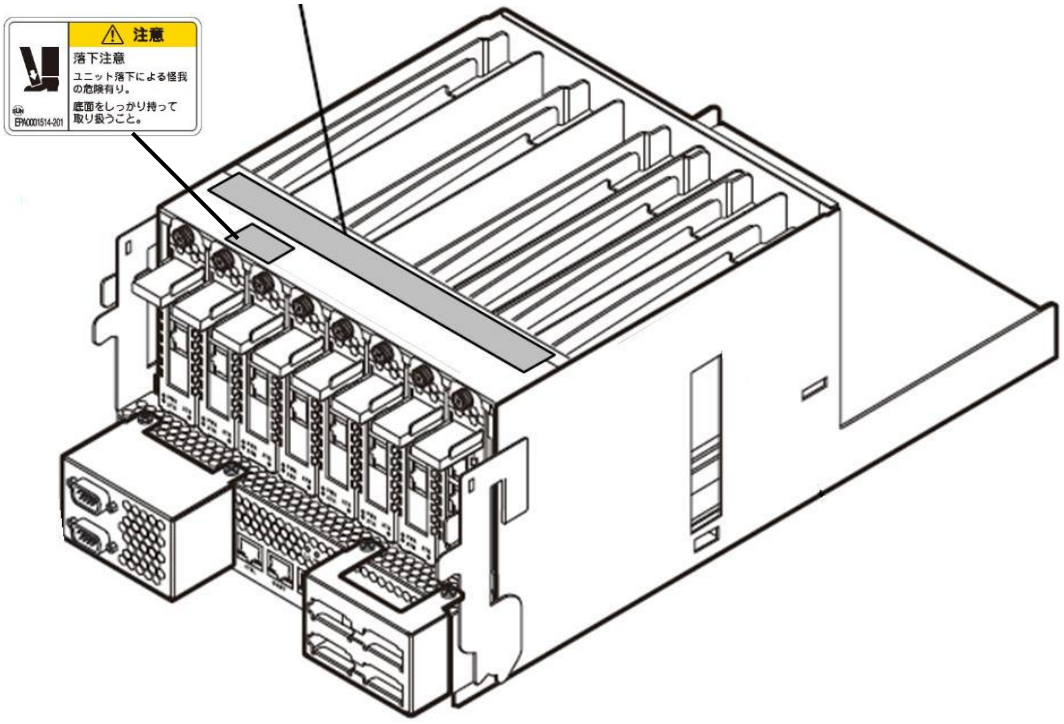
⚠ 注意	⚠ CAUTION	⚠ 주의	⚠ ATTENTION
重量物注意 質量：48kg 腕や腰を痛める原因となることがあります。 交換時搭載モジュールを全て取り外し、2人以上で作業のこと。 またはリフタによる作業のこと。	Heavy Load Weight : 48kg Lifting this equipment may cause personal injuries. Remove all modules prior to lifting equipment. Chassis replacement should be performed by at least two people or by use of a lift.	중량물 취급주의 질량 : 48kg 팔과 허리를 다칠 수 있습니다. 교환시 탑재된 모듈을 모두 빼낸후, 2사람 이상이 함께 작업할 것. 또는 리프터로 작업할 것.	Charge Lourde Poids: 48kg Soulever cet équipement peut entraîner des blessures. Avant de soulever l'équipement, retirer la cage arrière et tous les modules. Le remplacement du châssis doit être effectué par au moins deux personnes ou à l'aide d'un élévateur.
⚠ 小心	**⚠ PRECAUCIÓN**	**⚠ 注意**	**⚠ ACHTUNG**
重型物品 重量：48kg 搬動本設備可能造成人員傷害。	Carga Pesada Peso: 48kg Levantar este equipo puede causar heridas personales. Retirar todos los módulos antes de levantar el equipo. La substitución del chasis debe ser realizada por, al menos, dos personas o usar un elevador.	重物注意 重量：48kg 提升本设备可能引起人员伤害。	Schwerlast Gewicht: 48 kg Das Anheben dieses Gerätes kann Verletzungen verursachen. Entfernen Sie vor dem Anheben des Gerätes sämtliche Module. Ein Standortwechsel des Gerätes muss von mindestens zwei Personen oder mit Hilfe einer Hebevorrichtung durchgeführt werden.

EPA0001514-401

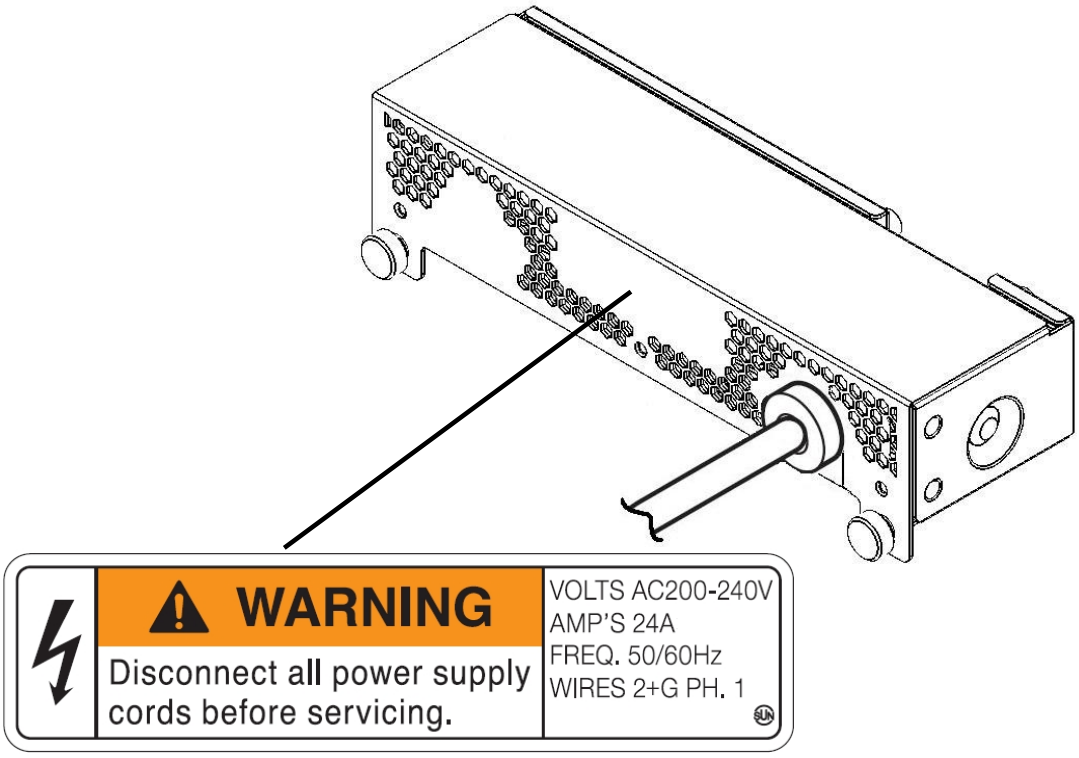


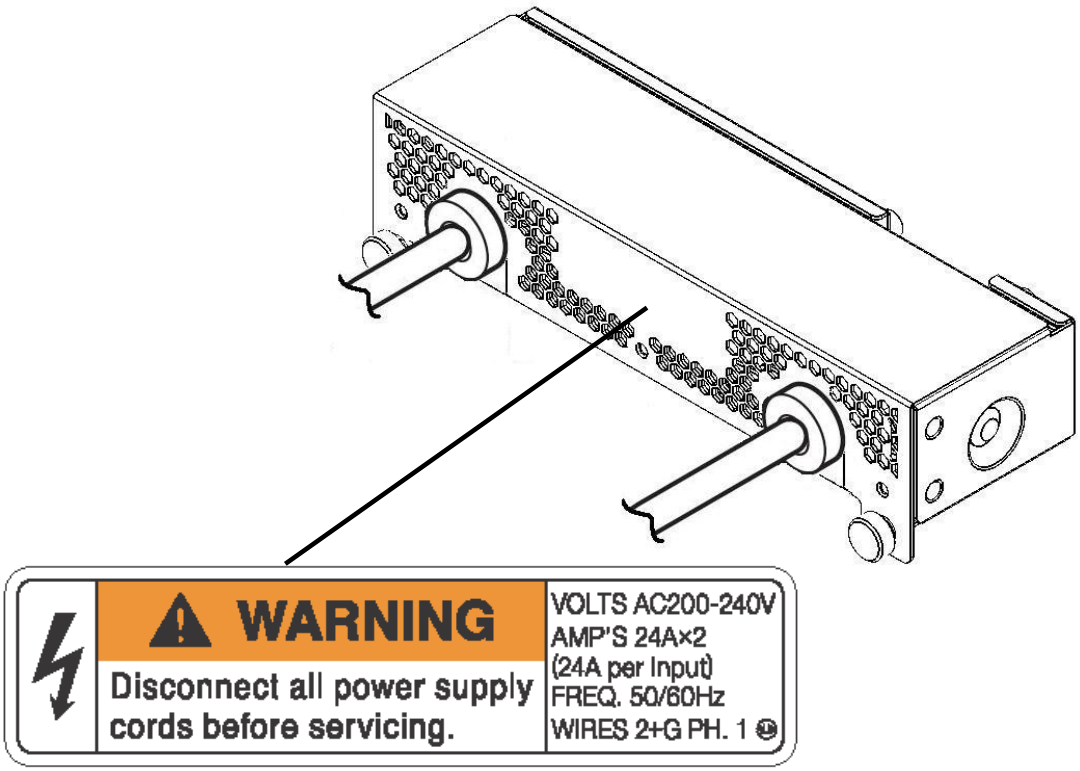
❑ I/O Module

⚠ CAUTION	⚠ 주의	⚠ ATTENTION	⚠ 小心	⚠ PRECAUCIÓN	⚠ 注意	⚠ ACHTUNG
Drop potential There is a risk of injury if the unit is dropped. Support the bottom of the unit prior to sliding it out.	낙하주의 유닛의 낙하로 인해 다칠 위험이 있습니다. 밑면을 확실하게 잡고 작업할 것.	Danger lié à une chute La chute de l'appareil peut entraîner un risque de blessures. Soutenir le bas de l'appareil avant de le faire coulisser pour le retirer.	注意物品掉落 若機件掉落可能使人受傷。	Cuidado con la caída Existe un riesgo de daño si se cae la unidad. Aguantar el fondo de la unidad antes de deslizarla hacia fuera.	掉落注意 部件掉落会有人员损伤危险。	Gefahr bei Herunterfallen des Gerätes Wenn das Gerät fallen gelassen wird, besteht Verletzungsgefahr. Unterstützen Sie die Unterseite des Gerätes, bevor Sie es herausschieben.



❑ AC Power Input Module





How to Use the Manuals

This section describes the manuals provided with the system equipment.

Manual Organization

The User's Guide and Software Guide are available as electronic manuals.

Depending on the configuration of the system equipment, additional manuals may be provided. Read these manuals if necessary.

Contents of Manuals

The contents of the User's Guide are described in the following table

Item	Contents
Precautions for Safe Use	Precautions concerning the safety of users of the system equipment.
How to Use the Manuals	How to use the manuals included with the system equipment.
1 Before Use	Overview of the system equipment and precautions on handling.
2 How to Use the System Equipment	Parts of the system equipment, optional components, and basic usage.
3 Connecting the System Equipment and Powering On	How to install the system equipment and connect peripheral equipment to it; and how to turn on and off the power.
4 Adding Optional Components	Provides information on how to mount option devices onto the system equipment.
5 Server Blade Setup	How to set up the Server Blade.
6 Management Module Settings	How to configure the settings of the management module.
7 Configuring the LAN Switch Module	Describes processes for configuring the LAN switch module.
8 Configuring the 10 Gb DCB Switch Module	Describes processes for configuring the 10 GB DCB switch module.
9 Configuring the LAN Pass Through Module	Describes processes for configuring the LAN pass through module.
10 Configuring the Fibre Channel Switch Module	Describes processes for configuring the fibre channel switch module.
11 I/O Slot Expansion Unit	Describes settings for the I/O slot expansion unit.
12 Logical partitioning manager	Describes Compute Blade logical partitioning manager.
13 System Operation and Management	Provides information helpful to operate and manage the system equipment.
14 When You Need Help	Covers measures to be taken when the system does not normally operate.
15 Maintenance and Replacement Parts	Describes a method for cleaning the system equipment. Also provides information on consumables.
Appendix: Specifications	Provides technological information on the system equipment, and other information.
Glossary	Defines the terms used in the document.

How to Use the Electronic Manual

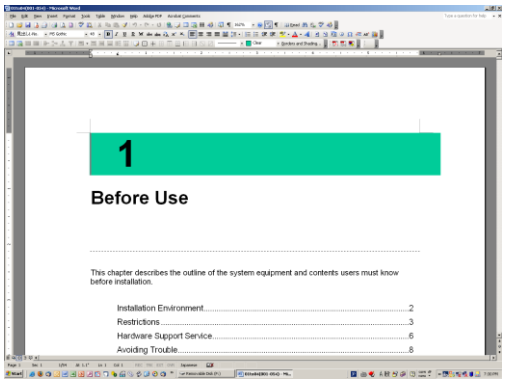
This section describes how to read the electronic manual.

❑ What to do before using the electronic manual

Adobe Reader must be installed on your system to read the electronic manuals. If you do not have Adobe Reader, download it from the Adobe website:
http://www.adobe.com

❑ Open/close the electronic manual

Double-click on the User's Guide or Software Guide. The electronic manual appears.



To close the electronic manual, click the [×] button at the top right corner of the window.

(This page is intentionally left blank.)

1

Before use

This chapter contains an overview of the system equipment and information users must know before installation.

Installation environment 2
Restrictions 4
Avoiding problems.....8

Installation environment

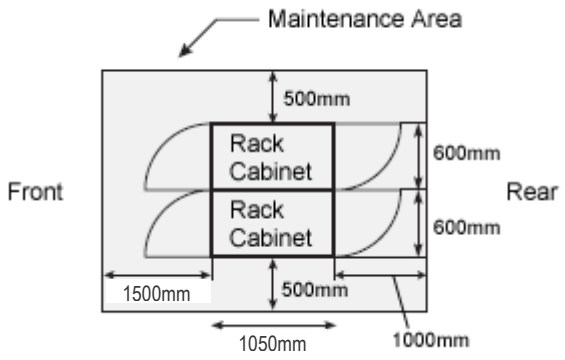
WARNING

Do not use the equipment near a place where water is used such as a bath tub, washing stand, sink, washing machine, or swimming pool; in a humid basement, or in a dusty place. Such conditions can lower electric insulation, which can cause an electric shock or fire.

CAUTION

Do not place the equipment in an unstable place such as an inclined ground and narrow place. The equipment can fall and cause injury.

The following table lists the installation environment requirements for the system equipment.

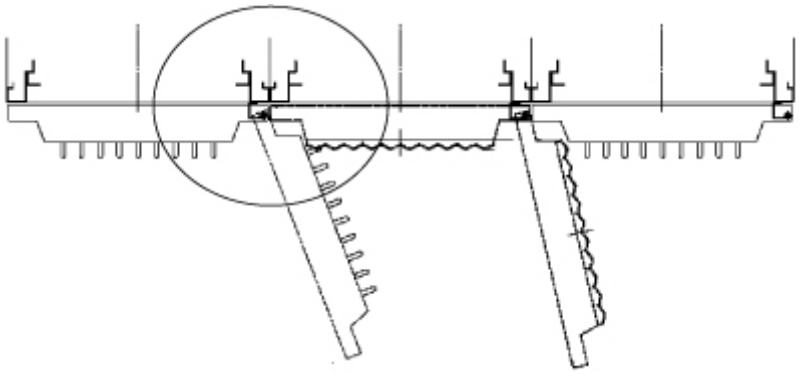
Item	Tolerance
Temperature	5 to 35°C [In non-operating status: 10 to 43°C]
Relative humidity	20 to 80% [In non-operating status: 8 to 90%] (no dew condensation)
Vibration	Max. 2.50 m/s^2 [In non-operating status: 9.80 m/s^2]
Dust	Same level as business offices in general
Installation space	

Do not install the system equipment in the following environment:

- Indirect sunlight
- In a location subject to excessive or abrupt temperature or humidity change
- Near any equipment generating electrical noise, such as a motor
- Near any equipment generating a ferromagnetic field
- In a dirty and dusty location
- On an inclined surface
- In a location subject to heavy vibration
- Where the air contains a large amount of corrosive gases (sulfur dioxide, hydrogen sulfide, chlorine gas, ammonia, and so on.) or salt content
- Where ventilation is blocked, such as on a shelf or in a box in a hermetically-sealed environment

Tip

When multiple racks are connected and installed, be careful when opening a rack door so that you do not hit the adjacent rack door.



Restrictions

This section describes the environmental restrictions and usage of the system equipment and its peripheral equipment.

Environment for using system equipment and peripheral equipment

- Be sure to house the system equipment in a rack cabinet from Hitachi, and place it on a level surface. Do not use the system equipment without a rack.

⚠ DANGER

Do not remove or install the system equipment in or from the rack cabinet. Always get help from at least one other person or use tools. If the system equipment has to be installed on 31U and above of the rack cabinet or it is already installed there, call for maintenance personnel instead of attempting to install or remove it. Defective installation may cause the system equipment to fall, resulting in injury or equipment failure.

- In a cold environment, wait 20 to 30 minutes after power-on before operating the equipment.
- In a hot environment, use an air-conditioner and wait until the room temperature becomes stable before operating the equipment.
- Do not use the equipment in a place subject to direct sunlight or heat generated by a heater or similar equipment.
- Do not use the equipment in an extremely dusty environment.
- Do not use the equipment in an extremely hot or cold environment, or an environment where the temperature widely fluctuates.
  Do not use the equipment in an extremely humid environment.
- Air that contains corrosive gases or salt content chemically corrodes the surface of the system equipment and the components of its peripheral equipment. The corrosion increases the contact resistance of electronic components and impairs the structural strength of movable parts, eventually reducing the reliability of the system equipment and its peripheral equipment to a large extent. Therefore, a place free from corrosive gases (particularly sulfur dioxide, hydrogen sulfide, chlorine gas, and ammonia gas, among others) must be selected for installation.
- A lightning strike occurring near the place where the system equipment is being used or poor power quality may cause the display to power off due to a temporary blackout or voltage reduction.
  If this happens, turn off the power to the system equipment, and turn it on again.

Handling the system equipment and peripheral equipment

NOTICE

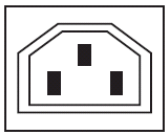
Always create backup copies of important data on the hard disk into auxiliary storage. If the hard disk fails, all data stored on it will be lost.

- Operation of the system equipment is not guaranteed if you use commercial hardware including Universal Serial Bus (USB) devices or software (including Windows purchased from other companies).
- We are not responsible for corruption of data or applications due to the hardware being physically damaged.
- Corruption of data or applications due to the hardware being physically damaged shall not be compensated.
- If you turn off the power switch, remove the power cable, or remove a server blade while booting or using the system, the system may not boot next time.
- The system equipment consists of precision electronic components. Do not bump, vibrate, or hit it.
- Bringing a strong magnetic source such as a magnet or loudspeaker near the system equipment causes failure of the system equipment and its peripheral equipment.
- Using a cathode ray tube (CRT) display near a magnetic source or high-tension line may cause color turbulence or distorted images. When you use it, keep away magnetic sources as much as possible.
- When you arrange the CRT displays back to back or side by side, keep a slight distance between them.
- If the mouse malfunctions, we recommend that the system equipment and its peripheral equipment should be powered through the same power strip with a noise filter.
- Remove any dirt and foreign particles from inside the mouse and internal roller. Foreign matter in the mouse prevents the smooth operation of the mouse.
- After turning off the power to the system equipment, wait at least 10 seconds before turning on the power again. Otherwise, the system equipment may not boot.
- If you need to use a pesticide spray, cover the system equipment completely with a plastic sheet before spraying.
- If you use the system equipment in a carpeted room or use a wrap during the operation, static electricity may be generated depending on the material to adversely affect the system equipment and its peripheral equipment. Use a static-free carpet or wrap.
- Be sure to protect the system equipment using packaging materials when transporting it. Keep the system equipment right side up at all times. Transportation without proper packaging or in the wrong orientation might cause equipment failure.
- The cover of the system equipment must not be removed by anyone other than the maintenance personnel.
- Be careful not to hit the system equipment or its peripheral equipment against any objects when moving things around.

- Do not block the vents on the front and rear of the system equipment. Blocking the ventilation causes failure. Keep the vents away from dust by periodically checking and cleaning them.
- The system equipment and server blades require regular maintenance. Perform maintenance according to Chapter 13 "Maintenance and Replacement Parts".
- Do not execute a keyboard reset (**Ctrl + Alt + Delete**) during system boot. It results in a system error.
- When you use a commercial console unit, turn on power to the system equipment and server blades without connecting the external power supply of the console unit. After turning on the power to the system equipment and server blades, connect the external power supply of the console unit.
- The system uses a network segment (the network address default: 192.168.253.0/24). If external network equipment uses the same address as this system equipment, change the address of this system, referring to “Configure Network Information” in Chapter 6. The same network address can be used in the multiple systems.

Electrical outlets

The following table shows the required specifications for electrical outlets and power plugs. Make sure to use the plug and outlet that comply with the specifications.

Item Number	Power supply Specifi-cations	Major products concerned	Type and capacity	Electrical plug and outlet*	
				Plug	Outlet
1	200-240V	• Outlet for the blade server A1 chassis • 200-240VAC outlet box	Grounding, 2-slot hook-up type outlet 30 A - 250 V	 (NEMA L6-30P)	 (NEMA L6-30R)
2	240 V	• Outlet for the blade server A1 chassis • 200-240VAC outlet box	32 A - 250 V	 (IEC309 Plug)	 (IEC309 Socket)
3	AC200V ± 20V 50Hz/60 Hz ± 1Hz	• Outlet for the I/O slot expansion unit • Outlet for the blade server A2 chassis	Grounding, 2-slot plug and socket outlet system 15A - 250V	 （IEC60320-C14）	 （IEC60320-C13）

For power supply outlets, use products qualified under local regulations.

Avoiding problems

Backing up data

The hard disk is very effective at storing large amounts of data. However, all your important data or programs may become unavailable due to disk failures or erroneous operations, such as accidental formatting. Be sure to create backup copies of hard disk contents into auxiliary storage such as Network Attached Storage (NAS) regularly using the copy command or a backup program. Hitachi Data Systems shall not be liable for any unavailability of data or programs arising from failure or erroneous operations.

Function of RAID

- The Redundant Arrays of Independent Disks (RAID) function is installed on this system equipment. The security of data protection can be improved by using the RAID function. When using this system equipment, Hitachi recommends the RAID function be used.
- Be sure to back up the content of the hard disks to an auxiliary source, such as a Linear Tape-Open (LTO) library device or NAS, regularly using the copy command and the backup program.

Preventing computer viruses

When a program or data suddenly becomes corrupted, such as an unexpected operation occurs or an unexpected screen appears, the system equipment may be infected with a computer virus. A computer virus is a malicious program which intrudes into the system equipment to make the equipment perform an uncontrollable operation or to corrupt data or programs. In many cases, the computer is infected through downloading an unidentified program via the Internet or using a floppy disk of unknown origin. Avoid these actions as much as possible or take preventive measures by using a virus-scanning program.

Backing up system equipment settings

System equipment stores various system settings and user settings. To avoid losing your settings in case of a failure, Hitachi Data Systems recommends that you back up the settings to the auxiliary storage, such as Network Attached Storage (NAS) and so on) using the backup command when you change the settings.

Concerning back up, perform the following:

- Back up the SVP configuration on the management module

  Back up the settings according to “Backing up the Management Module Settings” in Chapter 6”.

- Back up the setup data of the host bus adapter (HBA) basic input/output system (BIOS).

  Back up the settings according to the procedure in the *Hitachi Gigabit Fibre Channel Board User's Guide (Utility Software Edition)*.

- Back up the BIOS settings of the server blade

  Write down the changed BIOS settings.

- Back up the settings of the local area network (LAN) switch module

  Back up the settings according to the procedure in the manual that came with the LAN switch.

- Back up the RAID settings

  Write down the changed settings.

- Back up the settings of the Fibre-channel switch module

  Back up the settings according to the procedure in the user’s guide in the CD *Hitachi Compute Blade 2000 Fibre Channel Switch Accessory CD (EN)* that came with the Fibre-channel switch module.

2

How to use the system equipment

This chapter describes the parts of the system equipment.

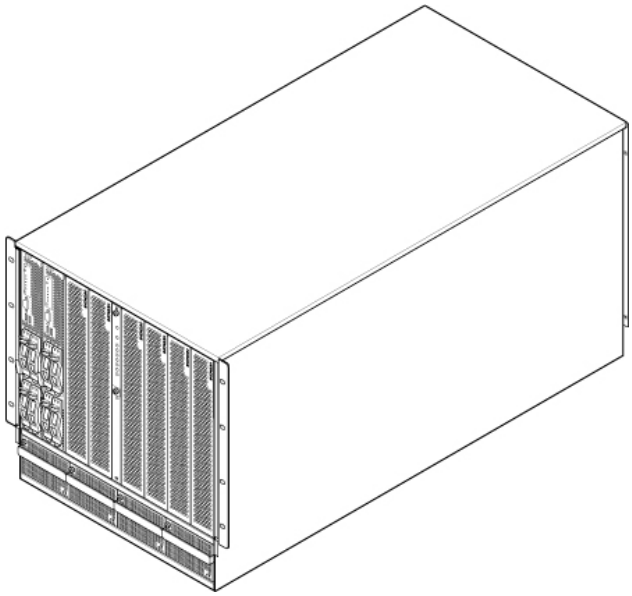
System equipment 12
I/O slot expansion unit.....35

System equipment

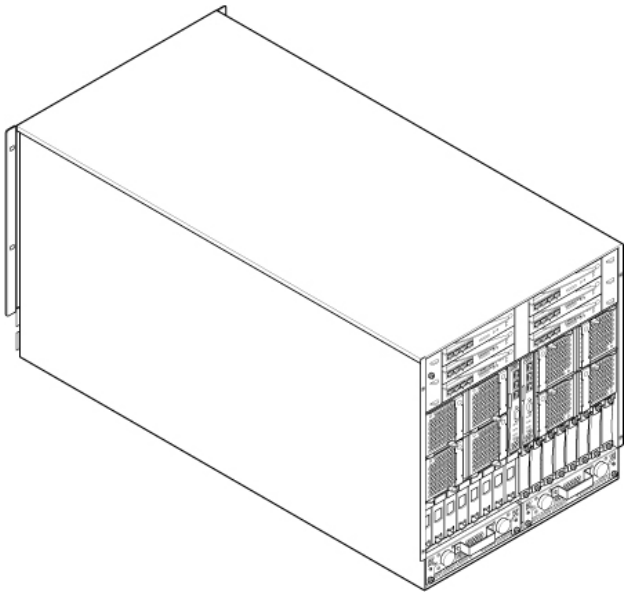
Names and functions

❑ Compute Blade system equipment

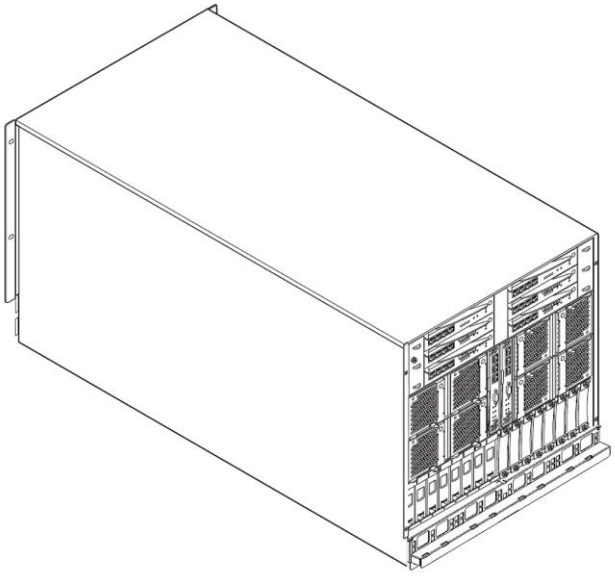
Front view of A1/A2 chassis



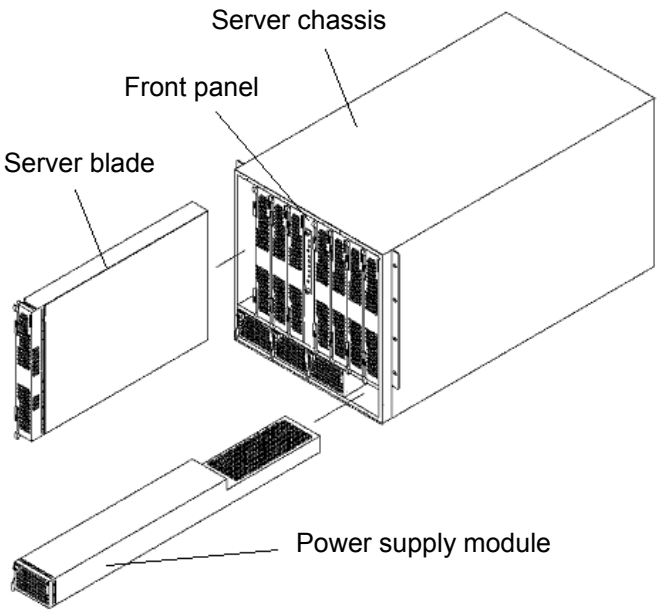
Rear view of A1 chassis



Rear view of A2 chassis



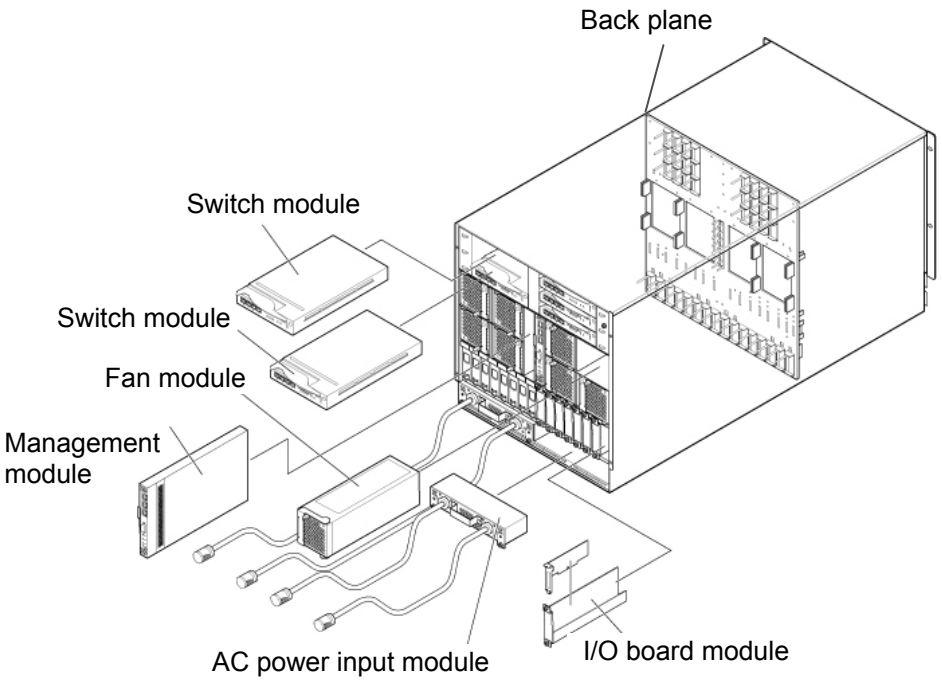
Front view of system configuration



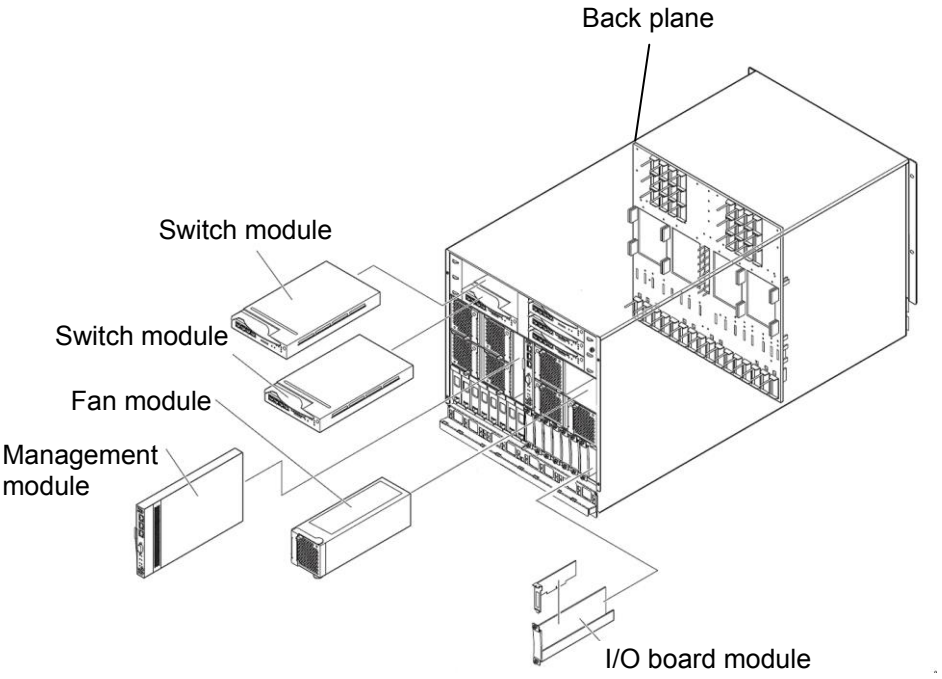
Tip

Respective types of power supply modules are installed in A1 chassis and A2 chassis. See “Power Supply Module Specifications per module” in the Appendix for details.

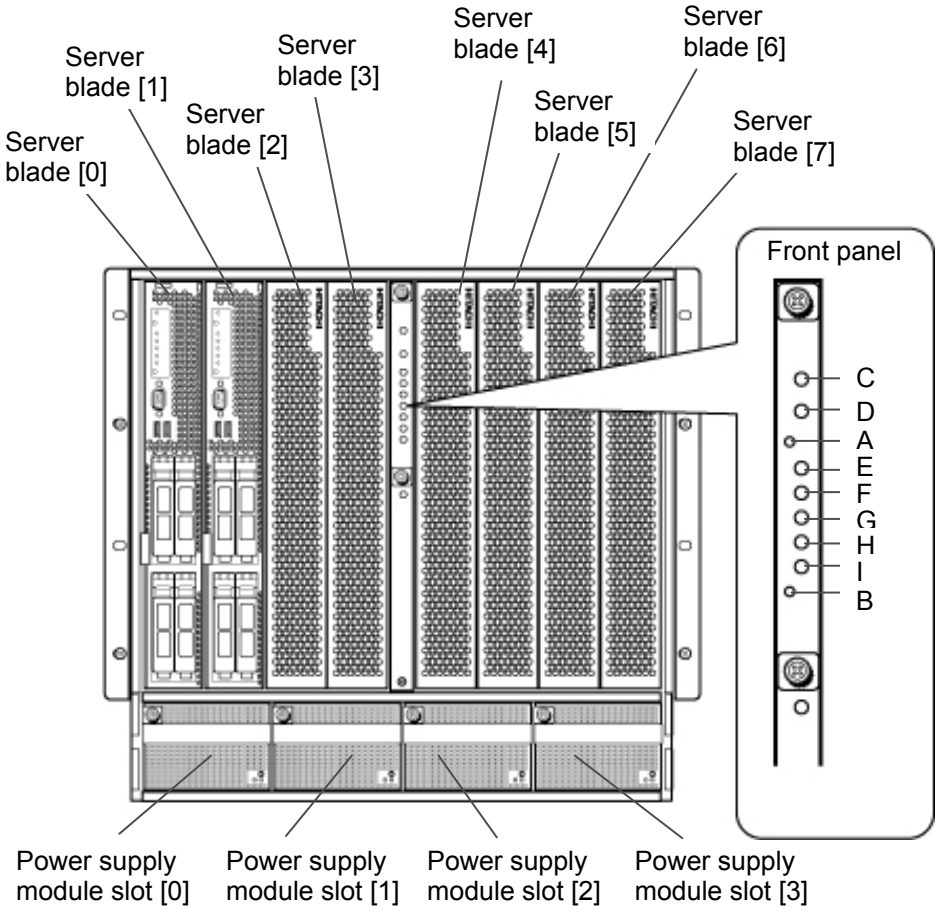
Rear view of system configuration
A1 chassis



Rear view of system configuration
A2 chassis



❑ System front view



A BUZZER button (BZR)

Stops the buzzer.

B Forcible power off button (POFF)

Press and hold this button for 4 or more seconds, and the system power is turned off forcibly.

To reboot the system, turn off and then on the circuit breaker to allow AC power to flow to the power supply module.

C Power light emitting diode (LED) (PWR)

Lights solid green when the main power of the server blade is on.

Lights solid orange when all server blades are powered off.

Blinks orange during initialization when power is supplied to the server chassis.

D ERR LED (ALM)

Lights solid red when an error occurs in the server chassis.

E NODE LED (NODE)

Lights solid orange when an error occurs in a server blade.

F SW MOD LED (SWM)

Lights solid orange when an error occurs in a switch module or management module.

G FAN LED (FAN)

Lights solid orange when an error occurs in a fan module.

H PS LED (PS)

Lights solid orange when an error occurs in a power supply module.

I TEMP LED (TEMP)

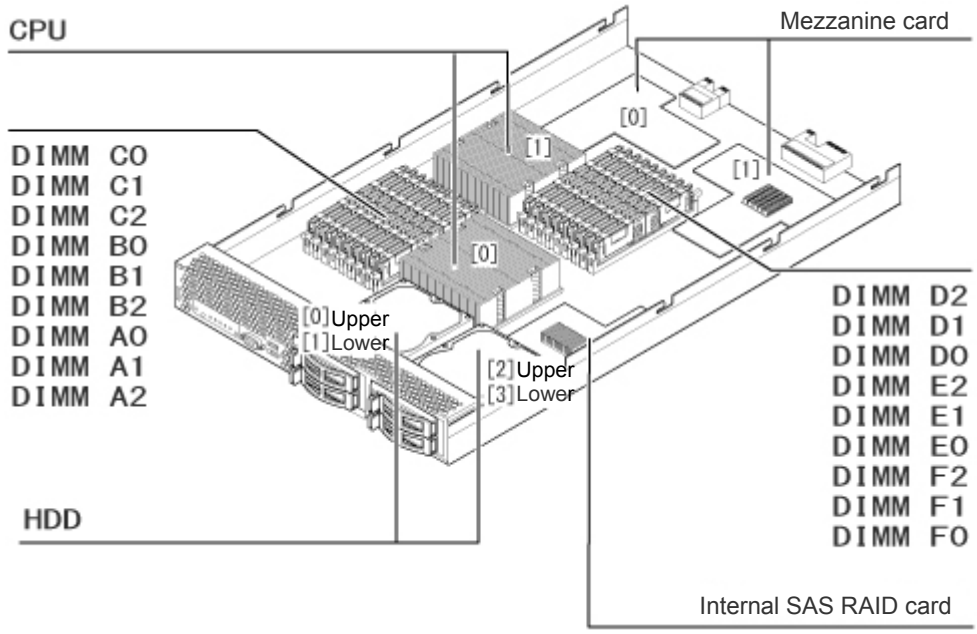
Lights solid orange when the temperature is abnormal in the server chassis.



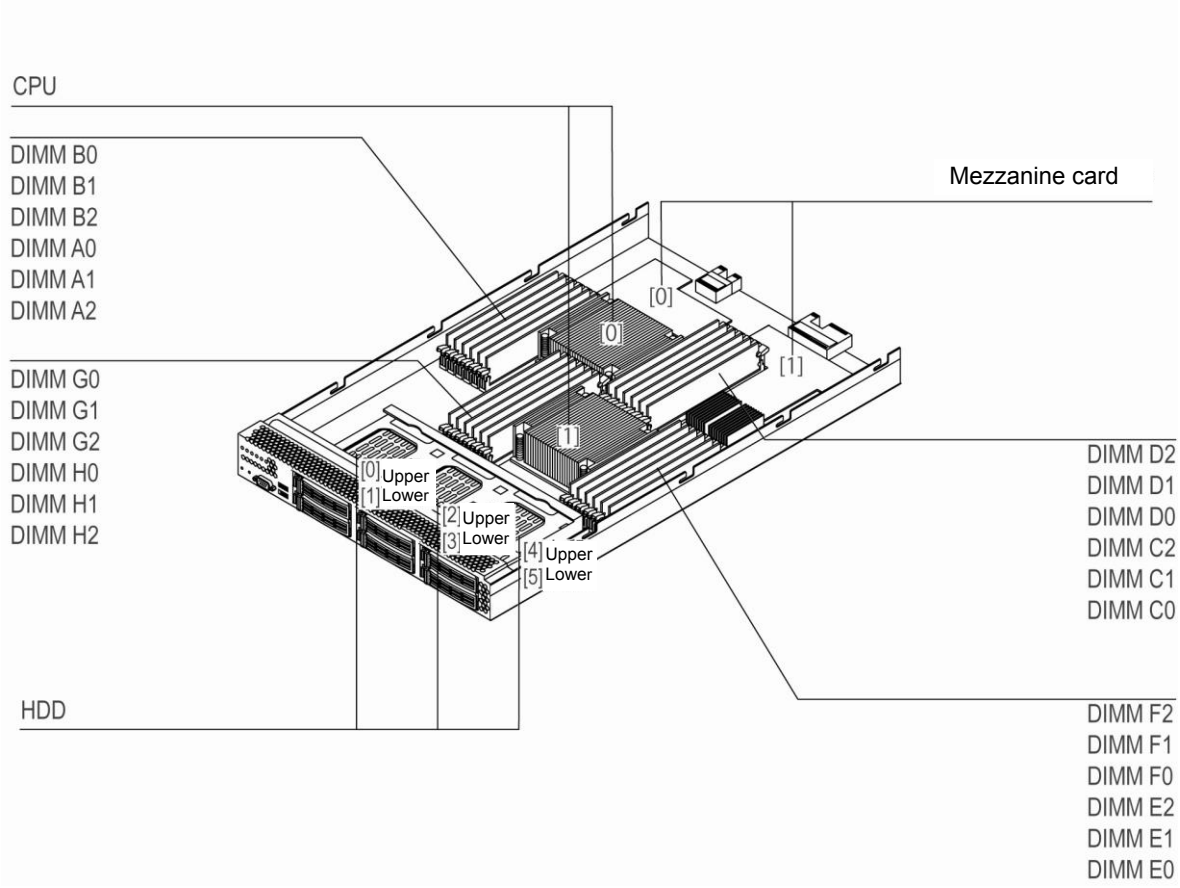
A plastic stick is attached to the front panel of the system equipment. Use this stick to press a button when it is difficult to reach using your finger.

❑ Standard server blade

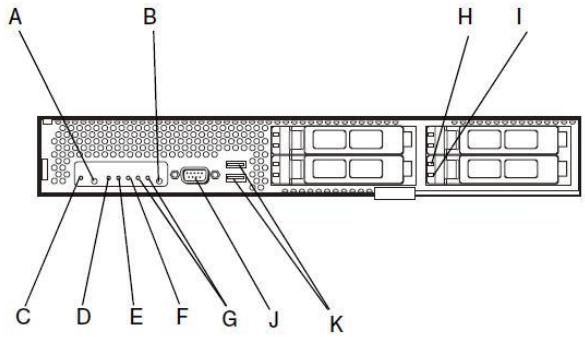
X55A1/X55A2



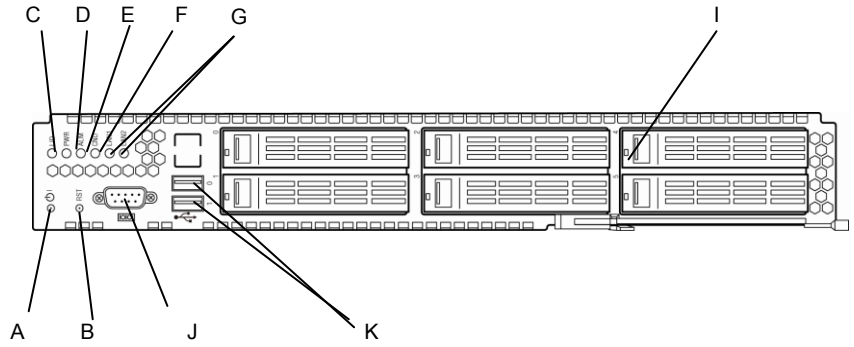
X55R3/X55S3/X55R4



X55A1/X55A2



X55R3/X55S3/X55R4



A Power button

Press and hold this button for at least one second to turn on main power to the server blade. If you press and hold this button for 4 seconds or more while the OS is running, it will shut off main power to the server blade without an orderly OS shutdown. You should avoid a forcible power cycle whenever possible.

B Reset button (RST)

Press and hold this button for one or more seconds to reset the server blade.

C Location ID LED (LID)

Lights solid blue when a server blade is identified.

D POWER LED (PWR)

Lights solid green during operation. Blinks green during sleep mode.

Lights solid orange while in standby mode.

E Error LED (ALM)

Lights solid red when an error occurs.

Lights solid red, when Watch Dog Timer (WDT) of Baseboard Management Controller (BMC), a management microcomputer for the blade server, expires if the ServerConductor (SC) /Agent is installed.

Tip To set WDT (Watch Dog Timer) of the BMC, see the *Guide for Administrator of ServerConductor/BladeServer Manager system*.

F Condition LED (CND)

Lights solid green during BMC initialization.

G Local area network (LAN) 1/2 LED (LAN1) (LAN2)

Lights solid orange when a link to the network is established.

Blinks orange when the network is running.

H Hard disk drive (HDD) active LED

Blinks green when booting or accessing the HDD. Lights solid green when the HDD is idle.

I HDD Error LED

Lights solid red when an error occurs. Blinks red when rebuilding the HDD.

J Serial port

Used to connect a device using a serial interface.

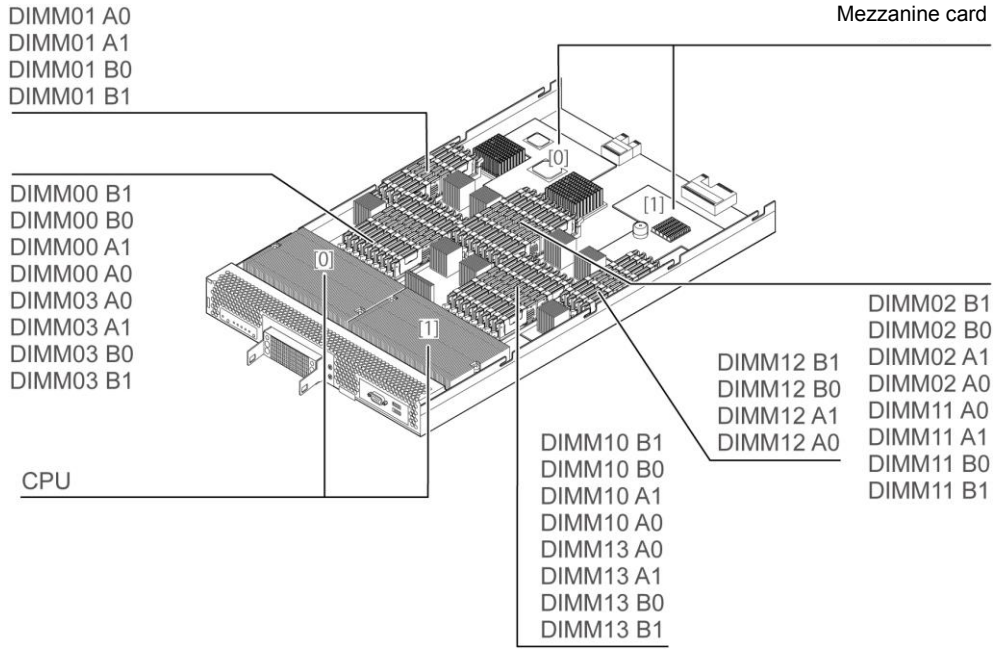
K Universal Serial Bus (USB) port

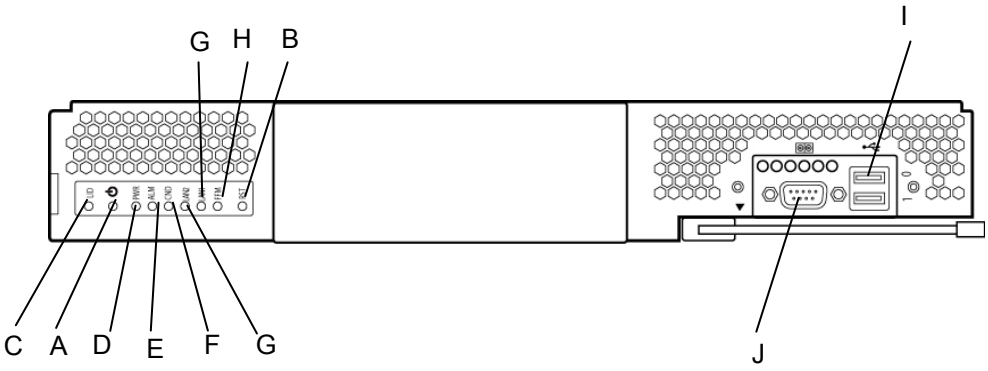
Two USB ports



It is not guaranteed that every device connected to those USB ports will work well.

❑ High-performance server blade (X57A1/X57A2)





A Power button

Press and hold this button for at least one second to turn on main power to the server blade. If you press and hold this button for 4 seconds or more, it will shut off main power to the server blade without OS shutdown. You should avoid a forcible power cycle whenever possible.

B Reset button (RST)

Press and hold this button for one or more seconds to reset the server blade.

C Location ID LED (LID)

Lights solid blue when a server blade is identified.

D POWER LED (PWR)

Lights solid green during operation. Blinks green while in the sleep mode.

Lights solid orange while in the standby mode.

E Error LED (ALM)

Lights solid red when an error occurs.

Lights solid red, when timeout of WDT of BMC, a management microcomputer for the server blade, is detected if SC/Agent is installed.



To set WDT of BMC, see the *Guide for Administrator of ServerConductor/BladeServer Manager system*.

F Condition LED (CND)

Lights solid green to show BMC initialization.

G LAN 1/2 LED (LAN1) (LAN2)

Lights solid orange when a link to the network is established.

Blinks orange when the network is running.

H Primary LED

Lights solid green when the server blade is primary.

Blinks green when the server blade does not belong to any physical partition or SMP between blades is being configured.

I USB port

Two USB ports.

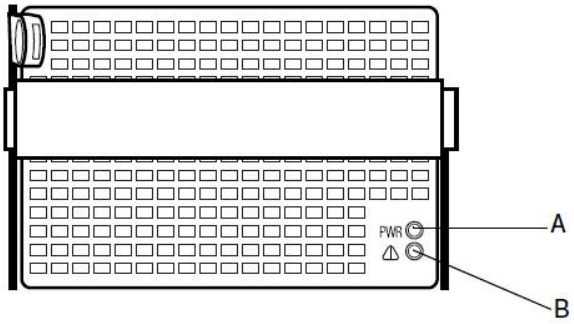
J Serial port

Used to connect a device using a serial interface.



It is not guaranteed that every device connected to the USB ports will work well.

❑ Power supply module



A POWER LED

Lights solid green when main power is on.

Blinks green when the sub-power is on.

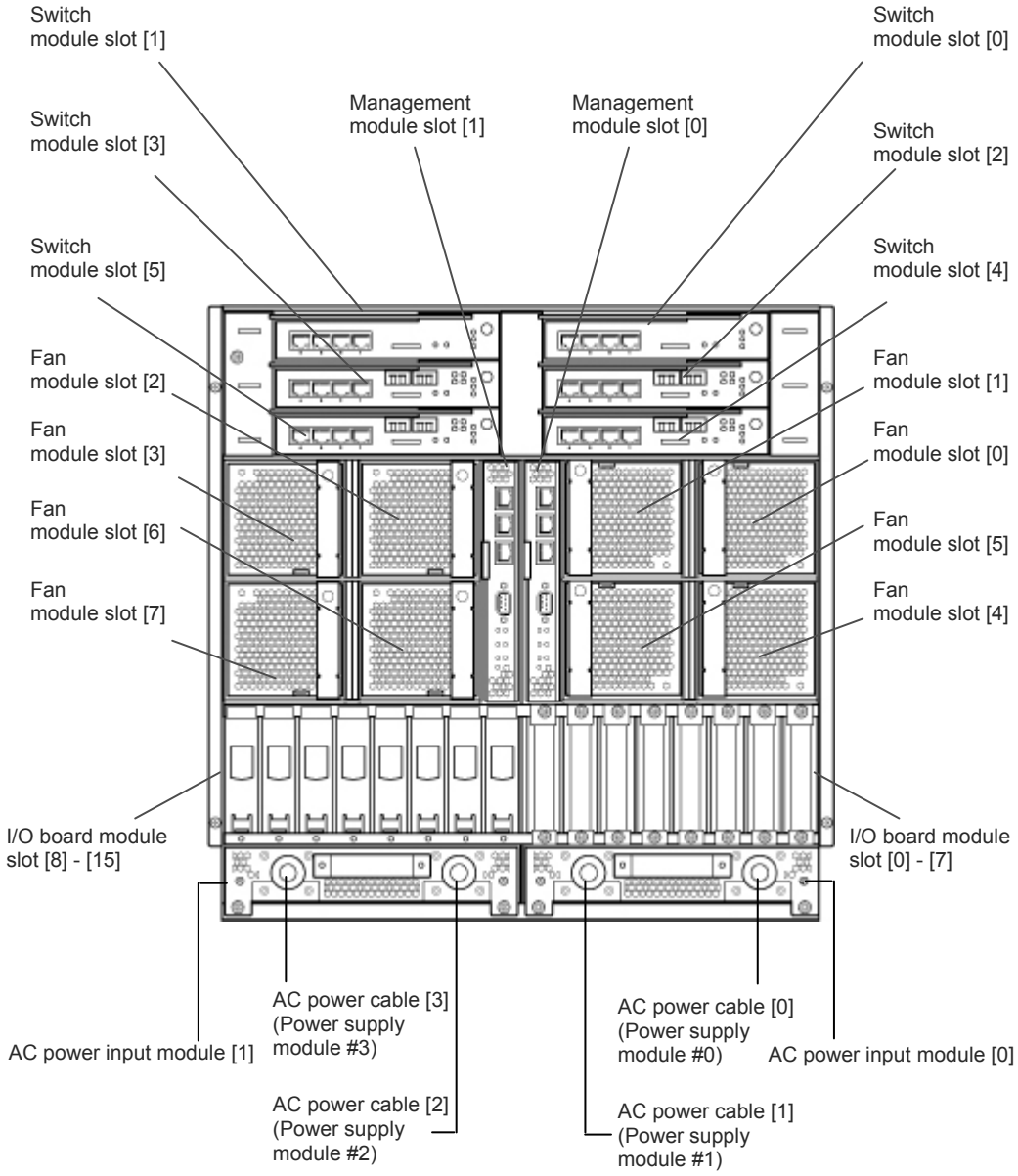
B FAIL LED

Lights solid orange when not working according to specifications due to an error.

Blinks orange when the AC input is off.

❑ System rear view

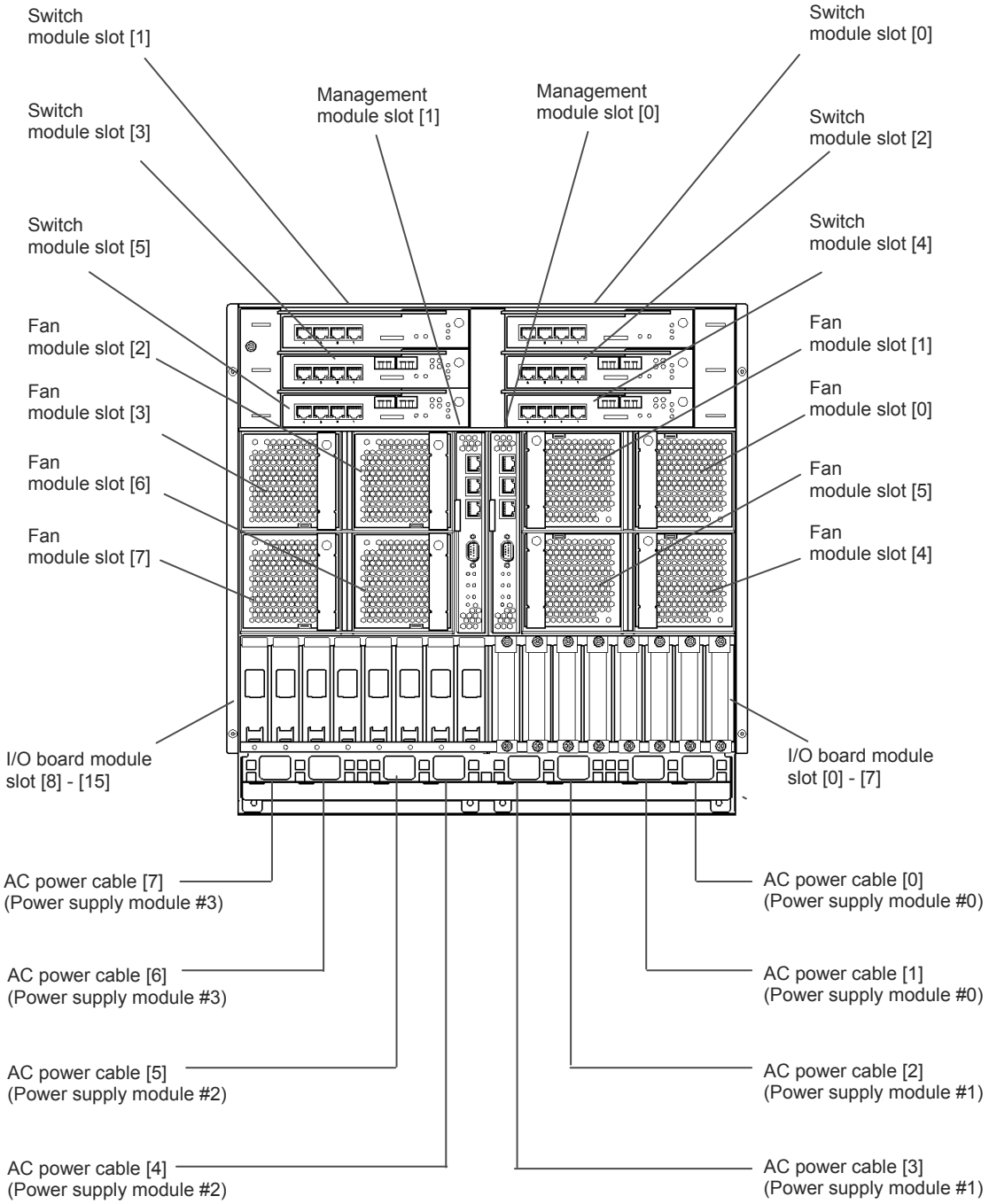
Rear view of A1 chassis



Tip

A plastic stick is attached to the lower right on the back of the front panel. Use this stick to press a button if it is difficult to reach.

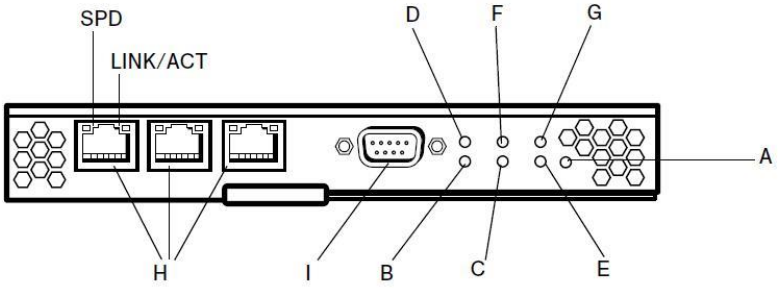
Rear view of A2 chassis



Tip

A plastic stick is attached to the lower right on the back of the front panel. Use this stick to press a button if it is hard to reach.

❑ Management module



A Shutdown button (SHDN)

Press and hold for 4 or more seconds to shutdown the management module.

Keep pressing the button until the power LED blinks or turns off.

B Location ID LED (LID)

Lights solid blue when the management module is located.

C Power LED (PWR)

Lights solid green when this module is in operation.

Blinks green when it is booting or shutting down.

D Error LED (ALM)

Lights solid red when an error occurs.

E Heart Beat LED (HB)

Blinks green when the firmware is in operation.

F Primary LED (MSR)

Light solid green when this module is active.

G Remote (RMT)

Lights solid green when the module is accessed remotely.

H LAN interface connector

Used to connect LAN cables.

A condition LED on the upper right of the connector shows the link status:

Lights solid green when a link is established.
Blinks green during communication.

A condition LED on the upper left shows the link rate:

Lights solid yellow when linked at 1000BASE-T.
Lights solid green when linked at 100BASE-TX.
Turns off when linked at 10BASE-T or not linked.

MGMT0 on the left: port 0 for the management network

MGMT1 in the middle: port 1 for the management network

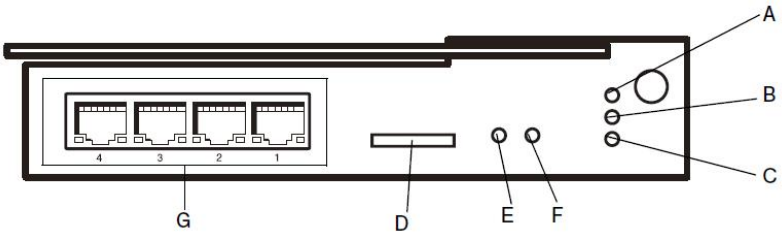
MAINT on the right: port for maintenance (Not available for users.)

I Serial port for system console

A port for a system console:
Use this port when the LAN interface for the system console is not available.

❑ Switch module

◆ 1-Gbps LAN switch module



A POWER LED (PWR)

Turns off when the power fails or no power is supplied.

B STATUS1 LED (ST1)

Indicates the status of the module. Lights solid green during normal operation.

Blinks green during power-on diagnosis or software activation.

Blinks red when the temperature threshold is exceeded or a warning such as fan failure is detected.

Lights solid red when an alarm is detected.

C Location ID LED (LOCID)

Lights solid blue while the switch module is located.

D Memory Card slot (MC)

A slot for a Secure Digital (SD) memory card: used for upgrading software and collecting dump data.

E Access LED (ACC)

Lights solid green when the SD memory card is accessed.

Do not remove the SD memory card when the LED lights solid green. If you do, the memory card may be damaged or data might become corrupted.

F Reset button (RST)

Press and hold this switch for about 5 seconds to reset the LAN switch module.

G LAN interface connector 1 to 4

Used to connect LAN cables.

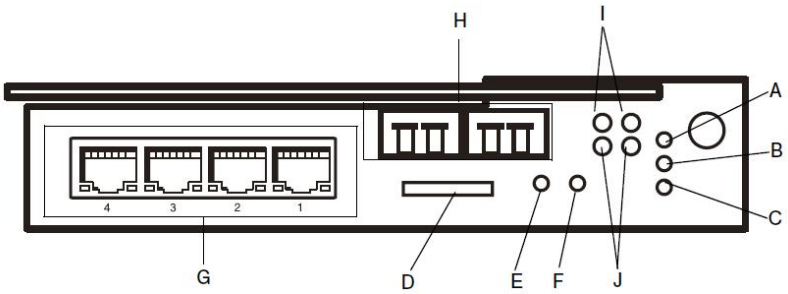
LED on the lower left of a connector shows the link status:

- Lights solid green when a link is established;
- Blinks green during communication.

Line1: Management port (at the shipment)

Line2-4: User ports

◆ **1/10 Gbps LAN switch module**



A POWER LED (PWR)

Turns off when power fails or no power is supplied.

B STATUS1 LED (ST1)

Indicates the status of the module.

Lights solid green during normal operation.

Blinks green during power-on diagnosis or software activation.

Blinks red when the temperature threshold is exceeded or a warning such as Fan failure is detected.

Lights solid red when an alarm is detected.

C Location ID LED (LOCID)

Lights solid blue when the switch module is located.

D Memory Card slot (MC)

A slot for a SD memory card: used for upgrading software and collecting dump data.

E Access LED (ACC)

Lights solid green when the SD memory card is accessed.

Do not remove the SD memory card when the LED lights solid green. If you do, the memory card may be damaged or data might become corrupted.

F Reset button (RST)

Press and hold this switch for about 5 seconds to reset the LAN switch module.

G LAN interface connectors 1 to 4

Used for LAN cables.

LED on the lower left of a connector to show the link status lights solid green when a link is established. Blinks green during communication.

Line1: Management port (at the shipment)

Line2-4: User ports

H 10GBASE-R slot s

Slots for 10GBASE-LR or 10GBASE-SR transceiver: Each slot has a link LED on the upper right and a TX/RX LED on the lower right.

I LINK LED for XFP

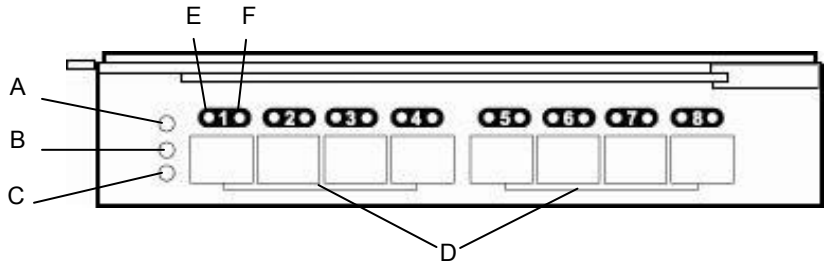
Lights solid green when a link is established.

Lights solid orange when a failure is detected.

J TX/RX LED for XFP

Lights solid green when a link is established or during communication.

◆ **10 Gbps Data Center Bridging (DCB) switch module**



A Location ID LED (LOCID)

Lights solid blue while the switch module is located.

B POWER LED (PWR)

Lights solid green when power is supplied.

Turns off when the power fails or no power is supplied.

C STATUS1 LED

Indicates the status of the module. Lights solid green during normal operation.

Blinks green during power-on diagnosis or software activation.

Blinks red during a warning when the temperature exceeds the threshold or a deconfiguration occurs while the switch is working.

Lights solid red when the switch has a serious failure causing improper performance.

D SFP interface connector 1 to 8

SFP+ modules, SFP modules (1000Base T connection), or direct attach cables can be connected. Connect optical fiber cables to SFP+ modules.

E Uplink port diagnostics LED

Indicates a state of uplink port diagnostics.

Lights solid orange when the signal is received but not online.

Blinks orange at low speed when the port is disabled by setting Disable with a command or performing diagnostics.

Blinks slowly when the port is disabled due to the disable setting with a command, or under diagnosis.

Blinks orange at high speed when the port is in failure.

Turns off when the signal is not received.

F Uplink port status LED

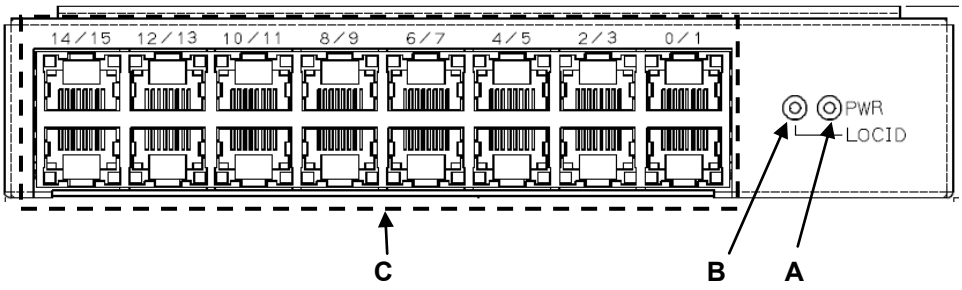
Indicates the state of an uplink port.

Lights solid green when online; blinks green when link is active; blinks green at low speed when online but segmented.

Blinks green rapidly when performing diagnostics using inner loopback.

Turns off when the signal is not received.

◆ **1 Gbps LAN pass-through module**



A POWER LED (PWR)

Turns off when the power fails or no power is supplied.

B Location ID LED (LOCID)

Lights solid blue when the 1 Gbps LAN pass-through module is located.

C LAN interface connectors 0 to 15

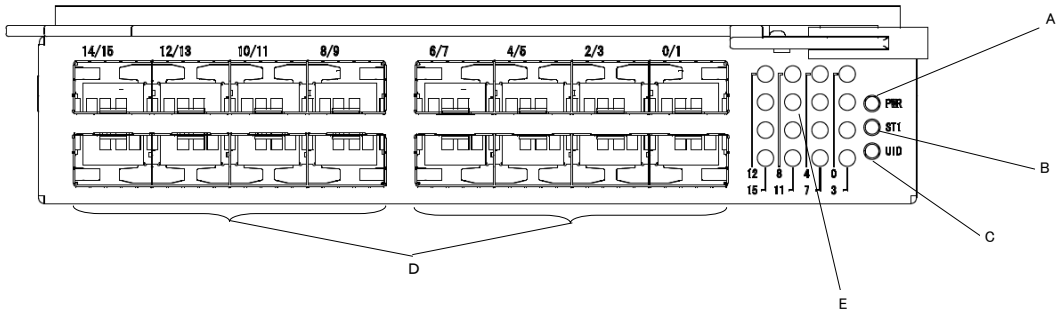
Used for LAN cables.

Even numbers (0, 2, 4 … 14) are assigned to the upper side connectors; odd numbers (1, 3, 5 … 15) to the lower side connectors.

LED on the left of a connector to show the link status lights solid green when a link is established. Blinks green during communication.

However, when the LED on the right of a connector lights solid orange, a link is not established either on the LAN interface or on the server blade. Thus, communication is not available.

◆ **10 Gbps LAN Pass Through module**



A POWER LED (PWR)

Lights solid green when the power is on.

Turns off when the power fails or no power is supplied.

B STATUS1 LED

Indicates the module status. Lights solid green in normal operation.

Blinks green during power-on diagnostics or executing initial settings in the module.

Blinks red at warning when the temperature is beyond the threshold while the module is working.

Lights solid red when the module has a serious failure causing improper behavior.

C Location ID LED (LOCID)

Lights solid blue when the 10 Gbps LAN pass through module is located.

D SFP interface connector 0 to 15

SFP+ modules or direct attach cables can be connected. Connect optical fiber cables to SFP+ modules.

Even numbers (0, 2, 4 … 14) are assigned to the upper side connectors; odd numbers (1, 3, 5 … 15) to the lower side connectors

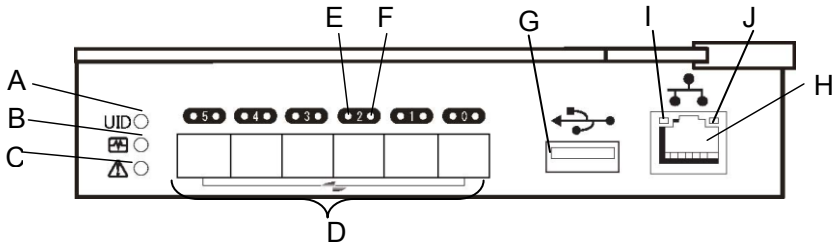
E Port status LED 0 to 15

Indicates internal and external port status.

Lights solid green when a link is established on ports for the LAN interface and for the server blade. Blinks green during communication.

Lights solid orange when a link is not established on ports of the LAN interface and for the server blade. Communication is not available.

◆ **8 Gbps Fibre-channel switch module**



A Location ID LED (LOCID)

Lights solid blue when the switch module is located.

B POWER LED (PWR)

Lights solid green when power is on.

Turns off when the power fails or no power is supplied.

C STATUS LED

Indicates the status of the module.

Lights solid green during normal operation.

Blinks green during power-on diagnosis or software activation.

Blinks red when the temperature threshold is exceeded or a warning is detected.

Lights solid red when an alarm is detected.

D Fibre channel (FC) interface connectors: 0 - 5

These connectors are equipped with optical modules: small form-factor pluggable plus (SFP+).

Connect a Fibre-channel cable to this optical module.

E FC port diagnosis LED: orange

Shows a diagnosis of a FC port status.

Lights solid orange when a signal is received but not on line.

Blinks slowly when the port is disabled due to the disable setting with a command, or under diagnosis.

Blinks orange rapidly when the port fails.

Both FC port diagnosis LED and FC port status LED are turned off when no signal is received.

F FC port status LED: green

Shows a FC port status.

Lights solid green online. Blinks green when the link is active.

Blinks green slowly when the port is online but segmented.

Blinks green rapidly when the port is diagnosed with the internal loopback.

Both FC port diagnosis LED and FC port status LED are turned off when no signal is received.

G USB connector
(for optional USB memory devices dedicated to the Fibre-channel)

To use an optional USB memory device, connect it to this connector.

Do not connect any devices other than USB memory devices dedicated to the Fibre-channel to this connector.

H LAN interface connector

LAN for managing Fibre-channel switch modules.

This LAN port is disabled during shipment.

Management LAN for the Fibre-channel switch module can be connected to the LAN port of the management module or to this LAN port, which can be switched via the management module system console.

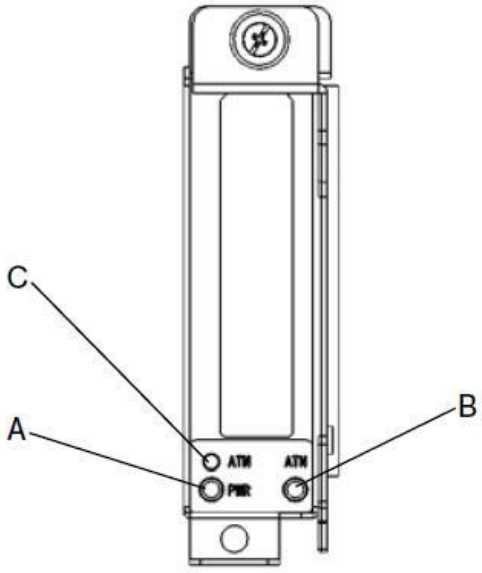
I LAN interface status LED1: orange

Lights solid orange online. Blinks orange when the link is active.

J LAN interface status LED2: green

Lights solid green at 1000 Mbps full duplex.

❑ I/O board module



A Power LED (PWR)

Lights solid green when main power is turned on.

B Attention LED (ATN)

Lights solid orange when the I/O board module fails.

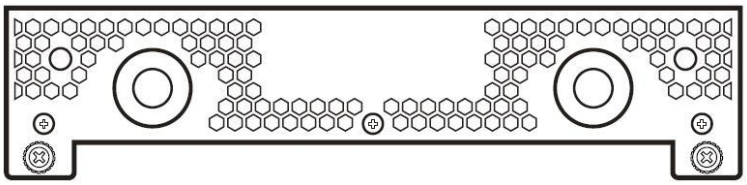
C Attention button (ATN)

Used for hot-inserting or hot- removing the I/O board module.

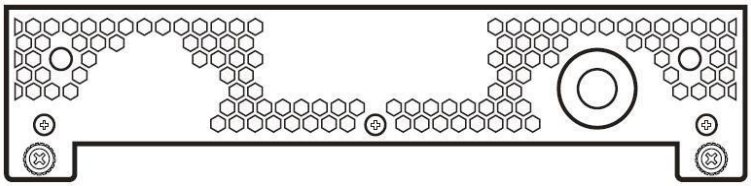
Note: This hot-plug function is currently not supported. To obtain information on when the hot-plug function will be supported, consult your reseller.

❑ AC power input module

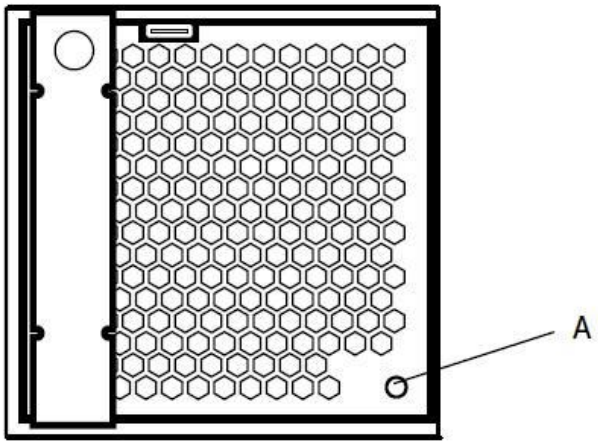
- With two input connectors



- With one input connector



❑ Fan module



A ACTIVE LED

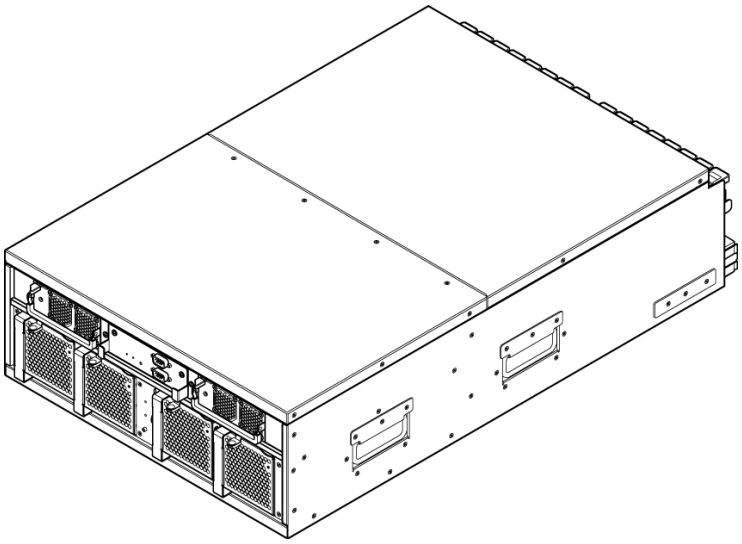
Lights solid green while the fan is working normally.
Lights solid orange when the module is not working due to a failure.

I/O slot expansion unit

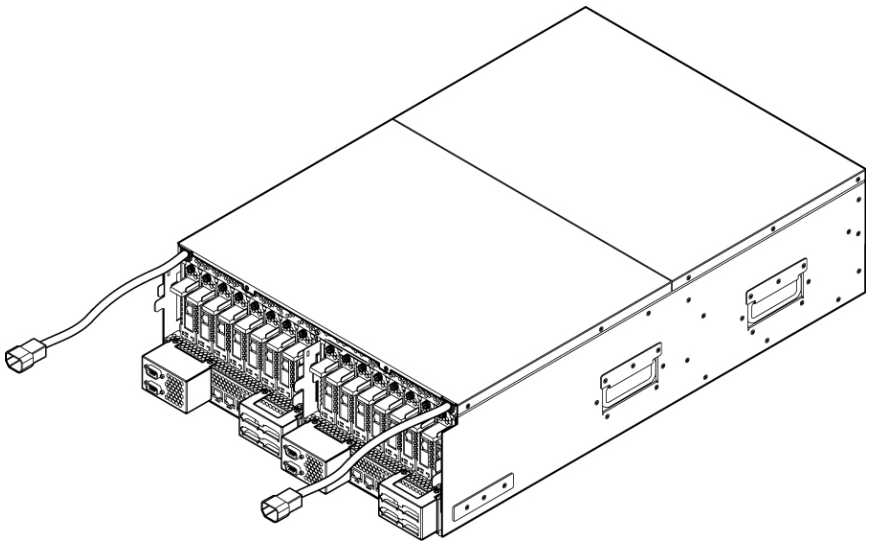
Names and functions

❑ Overview of I/O slot expansion unit

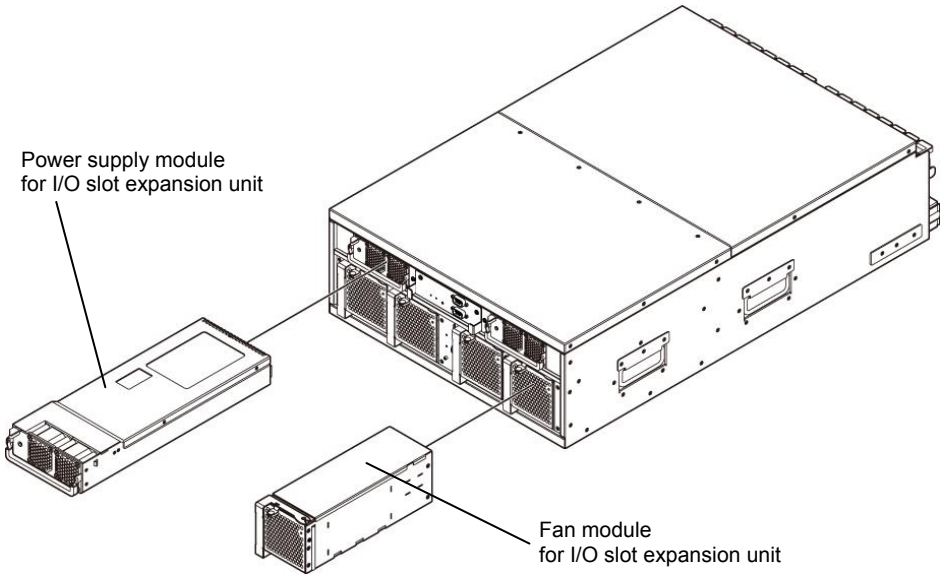
■ Front view of I/O slot expansion unit



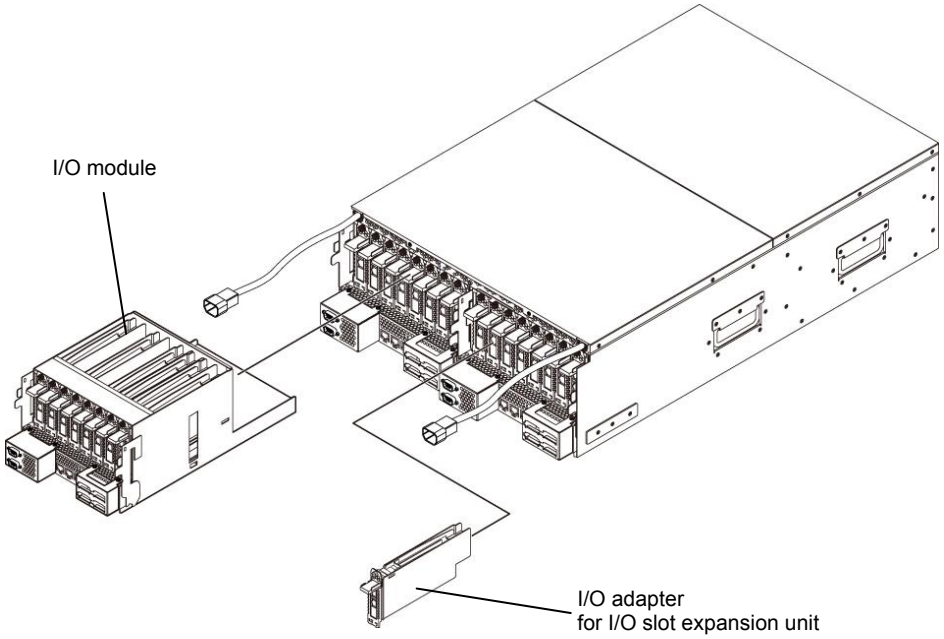
■ Rear view of I/O slot expansion unit



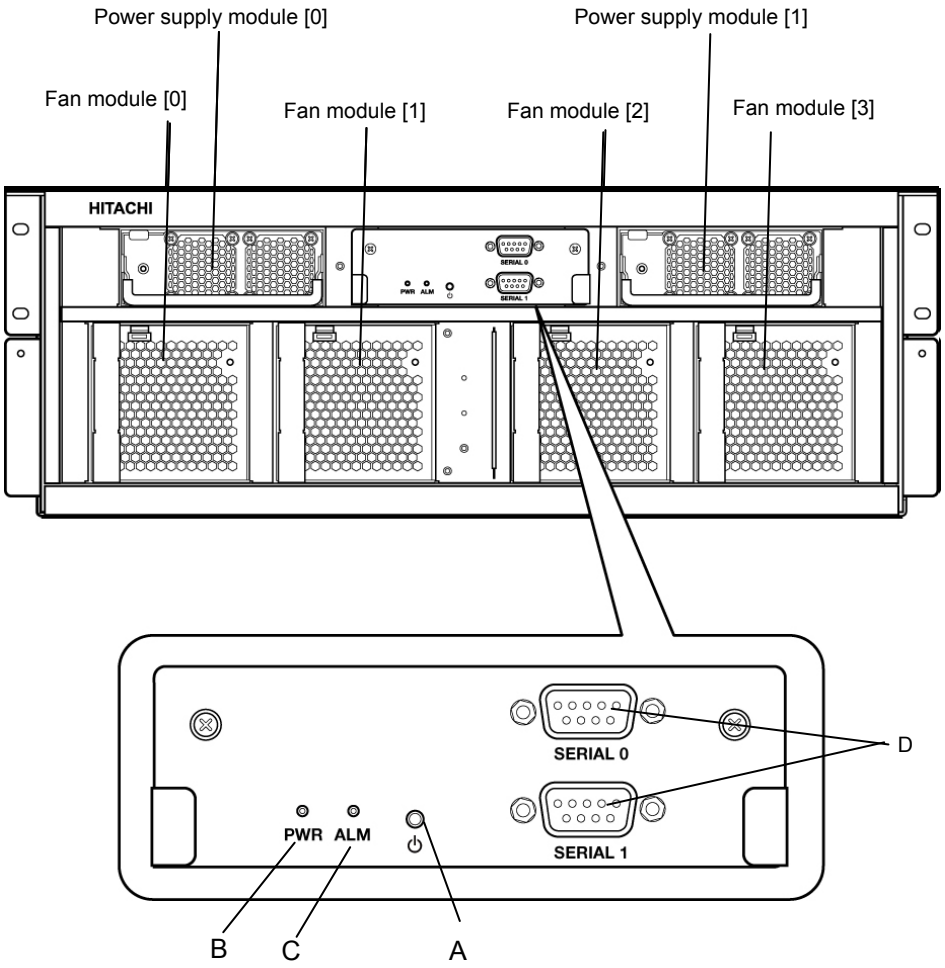
■ **Front view of I/O slot expansion unit configuration**



■ **Rear view of I/O slot expansion unit configuration**



❑ Detailed front view of the I/O slot expansion unit



A Power button

Press and hold this button for at least one second to turn on the I/O module and fan module. If you press and hold this button for 4 seconds or more, the main power is forcibly powered off.

B POWER LED (PWR)

Lights solid green when the main power to the I/O module is on.

Lights solid orange when the main power to all I/O modules is off.

Blinks orange during initialization when the power is on.

Blinks green during shutdown.

C Error LED (ALM)

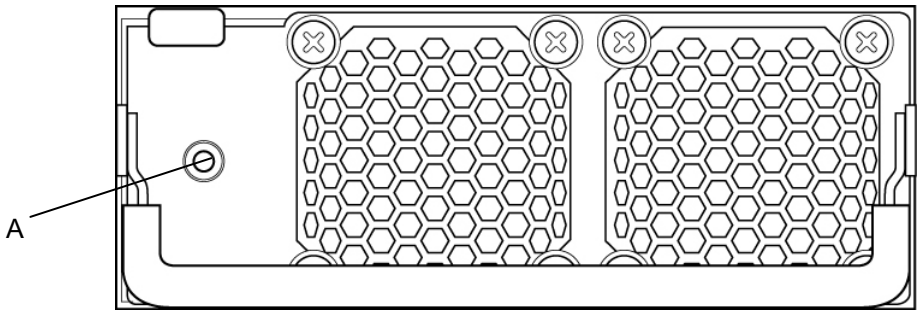
Lights solid red when an error occurs in the I/O slot expansion unit.

Lights solid orange during a warning.

D Serial port (SERIAL0/1)

Connects devices that use a serial interface.

❑ Power supply module for I/O slot expansion unit



A ACTIVE LED (ACT)

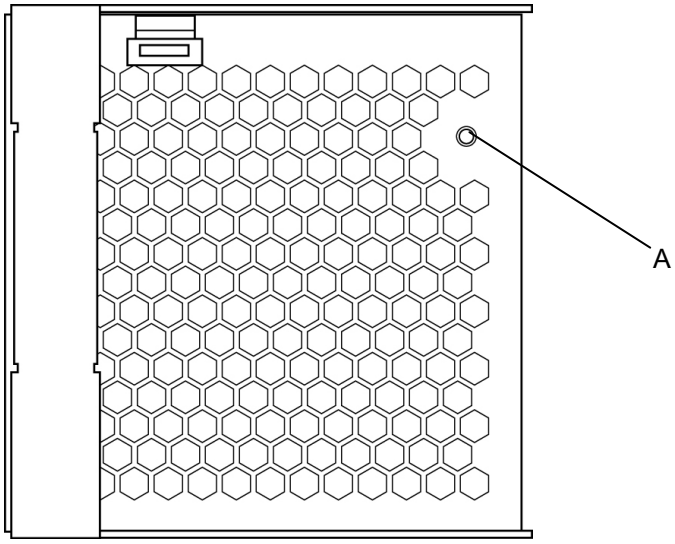
Lights solid green when the module is supplying power.

Blinks green when the module is in standby mode.

Blinks orange when the module is not working properly due to a failure.

Blinks orange when temperature exceeds its threshold, or if any fan works improperly.

❑ Fan module for I/O slot expansion unit

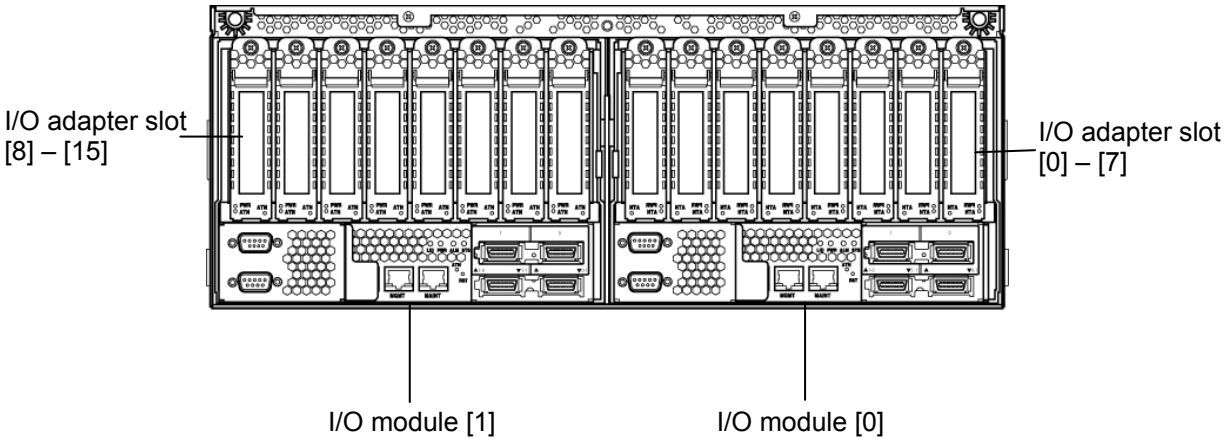


A ACTIVE LED (ACT)

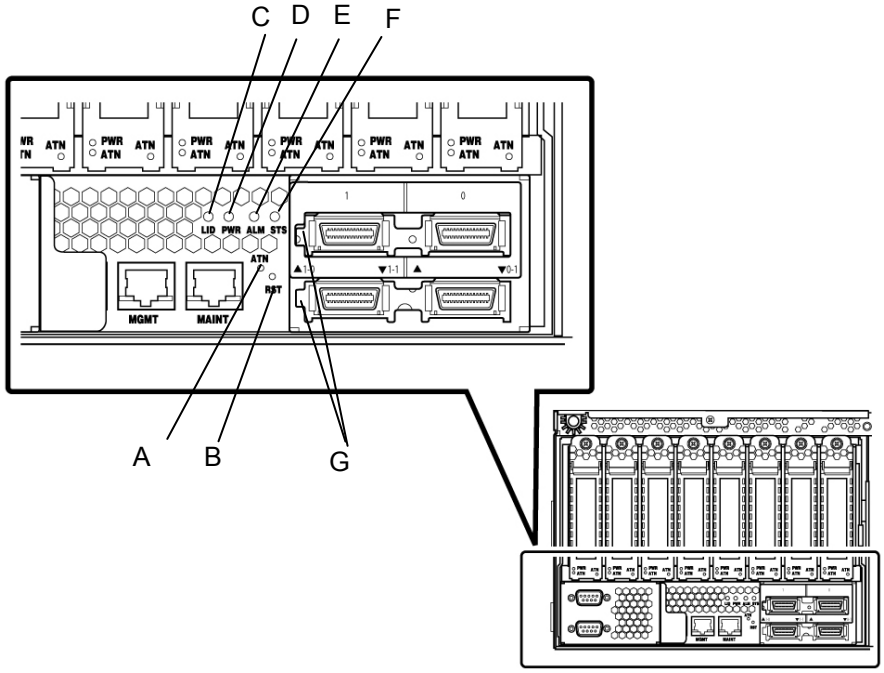
Lights solid green during normal operation.

Lights solid orange when the module is not working properly due to a failure.

❑ Details rear view of I/O slot expansion unit



❑ I/O module



A Attention button (ATN)

Starts the hot insertion and hot removal of the I/O module.

B Reset button (RST)

Resets the I/O module when it is pressed for a second or more and released.

Forcibly turns off main power to all components when it is pressed for 4 or more seconds.

C Location ID LED (LOCID)

Lights solid blue when the I/O module is located.

D POWER LED (PWR)

Lights solid green during the power-on.

Blinks green when the I/O module with power-on is in the standby mode.

E Error LED (ALM)

Lights solid red when a failure occurs in the I/O module.

F STATUS LED (STS)

Indicates the status of the module.

Lights solid green during normal operation.

Blinks green during power-on diagnosis or software activation.

Blinks red when a warning is detected.

Lights solid red when an alarm is detected.

G Link Status LED

Lights solid green when the link is established.

Blinks orange when a link alarm is detected.

H LAN interface connector

LAN cables are connected to these connectors.

The LED on the lower left of the connector shows the link status; lights solid green when the link is established, blinks green during communication.

LED on the lower right shows the link speed: lights solid yellow when link is at 1000BASE-T; lights solid green when at 100BASE-TX; turns off when at 10BASE-T or is offline.

MGMT: port for management network

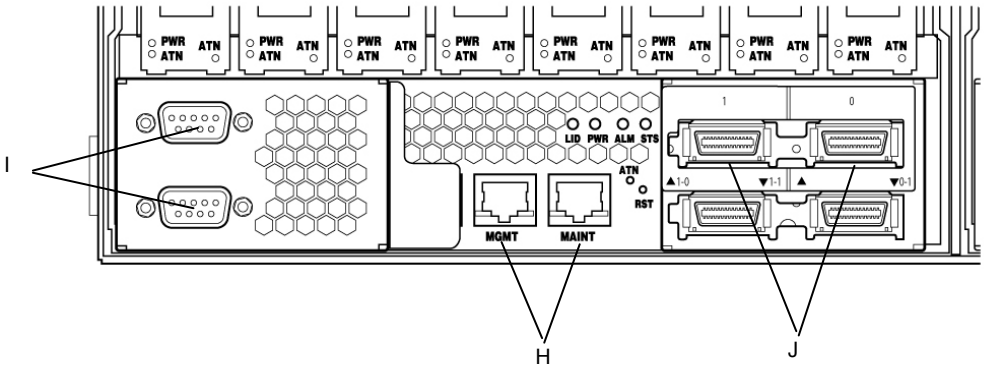
MAINT: port for maintenance (Customers are not permitted to use MAINT.)

I Control port 0/1

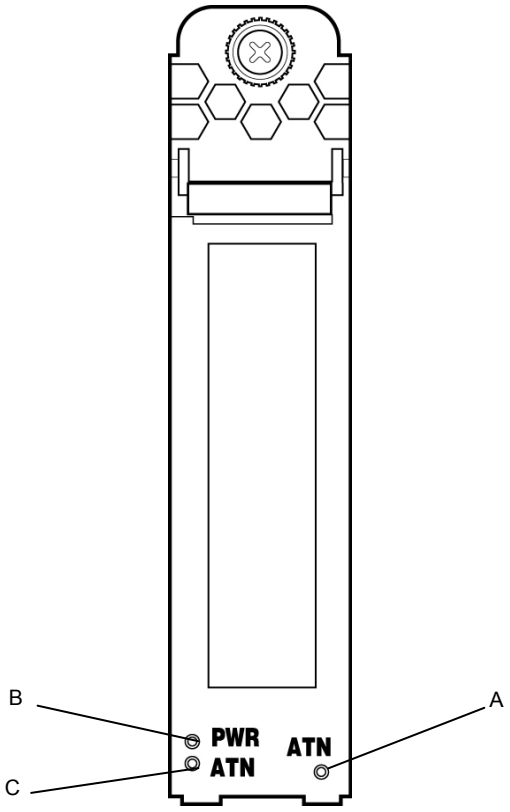
Control signal cables are connected to these ports for connecting a server chassis and I/O slot expansion unit.

J Server chassis connect port 0/1

The I/O slot expansion unit connect cables (metal) are attached to these ports for connecting a server chassis to an I/O slot expansion unit.



❑ I/O adapter for I/O slot expansion unit



A Attention button (ATN)

Starts the hot insertion and hot removal of the I/O adapter.

B POWER LED (PWR)

Blinks green when power to the I/O adapter is turning on or off.

C Attention LED (ATN)

Blinks orange when the I/O adapter is located.

3

Connecting the system equipment and powering on

This chapter describes how to install, connect, and turn on or off the power to the system.

Install the system 44
Connect the system 45
Connect the I/O slot expansion unit 68
Turning power on or off 70

Install the system

This section provides information on how to install the system equipment.

> **⚠ WARNING**
>
> - Since the equipment is heavy, be careful when you move it. Handling of this equipment without extra care can injure your arms or back.
> - To relocate or lift heavy loads such as this product, use tools or perform the task with the help of at least another person. If not, handling of heavy loads could lead to injury or equipment failure.

❑ Checking the parts in the packaging

Unpack and check all parts and accessories using the Part Check List. Check each part for damage. If you find damaged, missing parts or any other problem, contact your dealer.

❑ Check the location and installation

Referring to the requirements in Chapter 2; Installation Environment, check the installation environment and decide where to install this product.

Install the rack cabinet referring to the *Instruction Manual for Rack Cabin*et that is attached to the rack cabinet.

Only maintenance personnel can install the system equipment into the rack cabinet.

Connect the system

This section describes how to connect the remote console, Universal Serial Bus (USB) cable, and power cable.

Connect the remote console

The remote console is used as a console for each server blade of the Compute Blade 2000. The remote console enables users to power on and off the server blades, to setup basic input/output system (BIOS) configuration, and to install the OS using a remote console terminal connected to the server blades via a local area network (LAN).

You can use the remote console by running the Remote Console Application on a console terminal. There are two kinds of Remote Console Application available for Compute Blade 2000.

- Remote Console Application (Reclient)

  Remote Console Application (Reclient) is a Windows application that provides remote console functionality and can be installed on a console terminal where Windows OS is installed.

- Remote Console Application (Java application)

  Remote Console Application (Java application) is a Java application that provides Remote Console functionality. Remote Console Application is downloaded from a server blade and runs on a console terminal.



- To use the Remote Console Application (Java application), the following firmware version is required depending on the server blade model:
  - Standard server blade: X55A1/X55A2 models
    BMC: 03-91/X55R4
  - Standard server blade: X55R3/X55S3 models
    BMC: 05-01 or 07-01
  - High-performance server blade: X57A1/X57A2 models
    BMC:04-48 or 06-01
- For the following model or configuration, Remote Console Application (Reclient) is not available. You can use only Remote Console Application (Java application)
  - Standard server blade: X55R3/X55S3/X55R4 models
  - High-performance server blade: X57A1/X57A2 models with connection using Secure Socket Layer (SSL)/Transport Layer Security (TLS) enabled
- If changing the default port number of Remote floppy disk (FD) and Remote compact disc/digital versatile disc (CD/DVD), you cannot use Remote FD/Remote CD/DVD functions from Remote Console application (Reclient). Use Remote Console application (Java application).
- Only console terminal users with administrator privileges can use Remote console applications;

Reclient and Java. Users without administrator privileges might not be allowed to operate some functions.

Remote Console application (reclient)

See the Remote Console Application section in the *Hitachi Compute Blade 2000 User's Guide* on the Remote Console Application CD attached to the server blade for detailed information, usage, and restrictions on the Remote Console Application (Reclient).

Remote Console application (Java application)

This section describes the features and usage of the Remote Console Application (Java application).

❑ Key features

Remote KVM

This function enables users to have a video graphics array (VGA) console of extensible firmware interface (EFI) and OS running on server blades shown on a console terminal. This function also enables users to control the VGA console with a keyboard and mouse from a console terminal.

Remote FD and remote CD/DVD

Remote FD function enables server blades to use FD drives of a console terminal. The function also enables server blades to use FD image files on a console terminal as FD media.

Remote CD/DVD function enables server blades to use CD/DVD drives of a console terminal. The function also enables server blades to use CD/DVD image files on a console terminal as CD/DVD media.

When using these functions, you can install the OS and applications on server blades using FD drives and CD/DVD drives of a console terminal, or image files.



Use FDDUMP and MakeCDImg attached to the Remote Console Application (Reclient) to create image files for FD and CD/DVD. See the *Hitachi Compute Blade 2000 Remote Console Application User's Guide* contained in the Remote Console Application CD attached to the system equipment for details.



If the console terminal's OS is Windows Server 2008 or Windows Server 2008 R2, only the built-in user can use the physical drives for Remote FD and Remote CD/DVD. Non-built-in users should use image files.

Remote power operation

This function enables users to power on and off server blades, to reset server blades, and to generate a Non-Maskable Interrupt (NMI) to server blades.

❑ Requirements and restrictions

Requirements for console terminal

Remote Console Application works on console terminals that meet the following requirements.

Item	Requirements
Browser	Internet Explorer 6.0 or later *1 *2
Java VM	ORACLE Java Runtime Environment version 6 or later *2 *3 *4
OS*5	Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 Standard Windows Server 2012 Datacenter Windows 7 Professional Windows Server 2008 R2 Standard 32bit Windows Server 2008 R2 Enterprise 32bit Windows Server 2008 Standard 32bit Windows Server 2008 Enterprise 32bit Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows XP Professional Windows Vista Business
CPU	Clock 1 GHz or above
Memory	256 MB or above
Screen Resolution	1024x768 or above
LAN	100Base-TX or above
CD/DVD Drive	Console terminal's internal CD/DVD drives or USB CD/DVD drives connected to the console terminal. (If you use USB CD/DVD drives, it is recommended to use USB 2.0 compliant CD/DVD drives.)
FD Drive	Console terminal's internal FD drives or USB FD drives connected to the console terminal.
Keyboard	101/104 keyboard or 106/109 keyboard

*1: Any windows 6.0 or later browser is recommended.

*2: 64-bit version is not supported. Use 32-bit version even if using 64-bit OS.

*3: If using ORACLE Java Runtime Environment version 7, use update 2 or later.

*4: When enabling Remote Console connection using SSL/TLS, use ORACLE Java Runtime Environment (JRE) version 7, Update 2 or later.

*5 When connecting to the server blade Web console using TLS v1.1/1.2, use Windows 7 or later, or Windows Server 2008 R2 or later.

Other requirements and restrictions

- Requirements for the LAN Cable

  Use category 5 or better cables.

- Using Remote Console Application with Other Remote Console Program

  Starting the remote console application from another remote program, such as ServerConductor, causes improper operation. Do not use the remote console application with other remote programs.

- Requirements for server display settings

  Remote console application (Java application) supports the following resolutions and number of color bits.

Server OS	Resolutions	Color bits
Windows	640 x 480 (VGA mode)	8 bits
	800 x 600	16 bits
		32 bits
	1024 x 768 (recommended)	16 bits (recommended)
		32 bits
	1280 x 1024	16 bits(*)
Linux	640 x 480	16 bits
	800 x 600	16 bits
		32 bits
	1024 x 768 (recommended)	16 bits (recommended)
		32 bits
	1280 x 1024	16 bits

(*) For Windows Server 2012 and Windows Server 2012 R2, you can set only 32 bits as color bits due to the OS specifications. Set 1024 x 768 for resolution and 32 bits for color bits

  Combinations other than those above are not supported. Using other combinations may cause the screen to show nothing or to be distorted.

  See Chapter 12; Logical partitioning manager for requirements about the logical partitioning manager.

- Connection from Multiple Management PCs

  Multiple console terminals cannot log in to a single server blade at the same time.

- Number of sessions

  Up to 130 MB memory is used by the remote console application. If you perform too many remote console application sessions from a single console terminal while multiple console terminals are running, they may operate improperly due to the lack of memory.

- Numeric Keypad

  The numeric keypad on a keyboard connected to a console terminal depends on the state of the keyboard connected to the server blade regardless of the state of NumLock of the console terminal.

- Disabling CD/DVD AutoRun of Management PC

  Disable Windows CD/DVD AutoRun on the console terminal when using the remote CD/DVD.

- Remote Power Operation with logical partitioning manager (LP) mode

  Power operation by the remote console targets the server blade, which affects all logical partitions (LPARs) managed by the LPAR manager. Then, with a server blade in LP mode, power performance by remote console is disabled, which does not allow the following operation.

  Power ON, Force power OFF, Reset, and NMI

The Power ON, Force power OFF, Reset, and NMI operations are disabled, but no message is shown. With an LP-mode OS, operate the power of the server blade from the server blade Web console. See Chapter 5: Server Blade Setup.

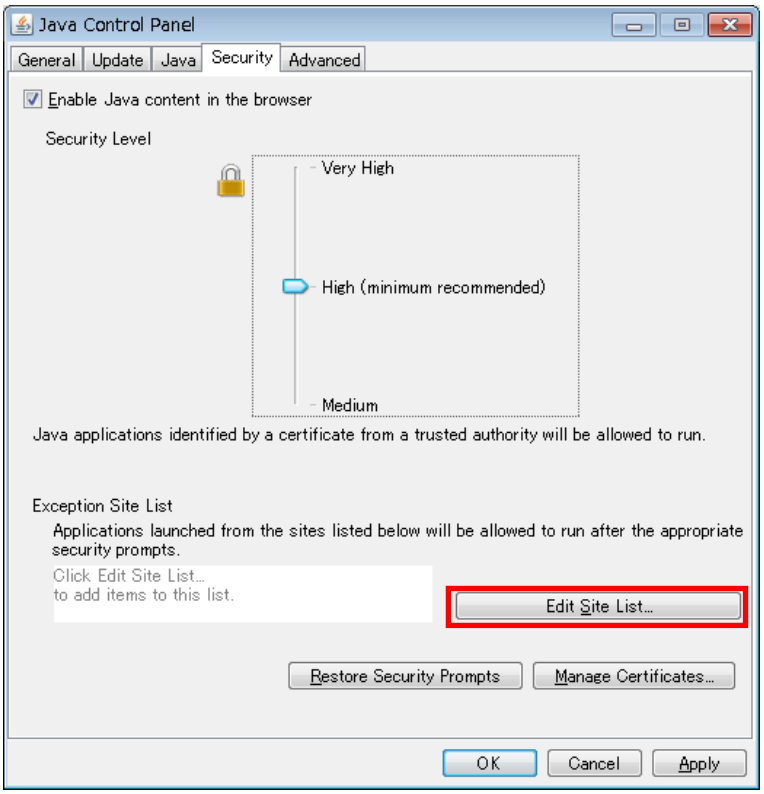
- Java Runtime Environment (JRE) version 7 update25 or higher

Since security policy has been changed with JRE 7 update25 or higher, the remote console application may not be able to start. If so, execute one of the following.

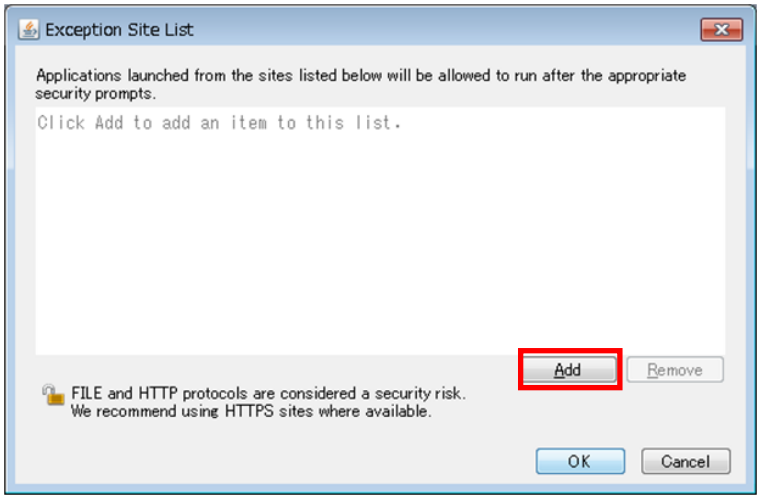
(a) Use Exception Site List (JRE 7 update51 or higher)

Add the Web console to the “Site List on the Exception Site List”, “Security” tab on “Java Control Panel”.

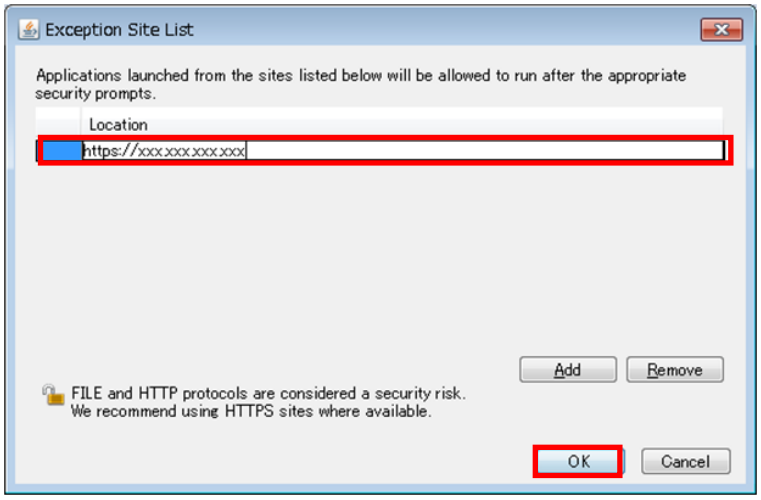
1. Click **Edit Site List**.



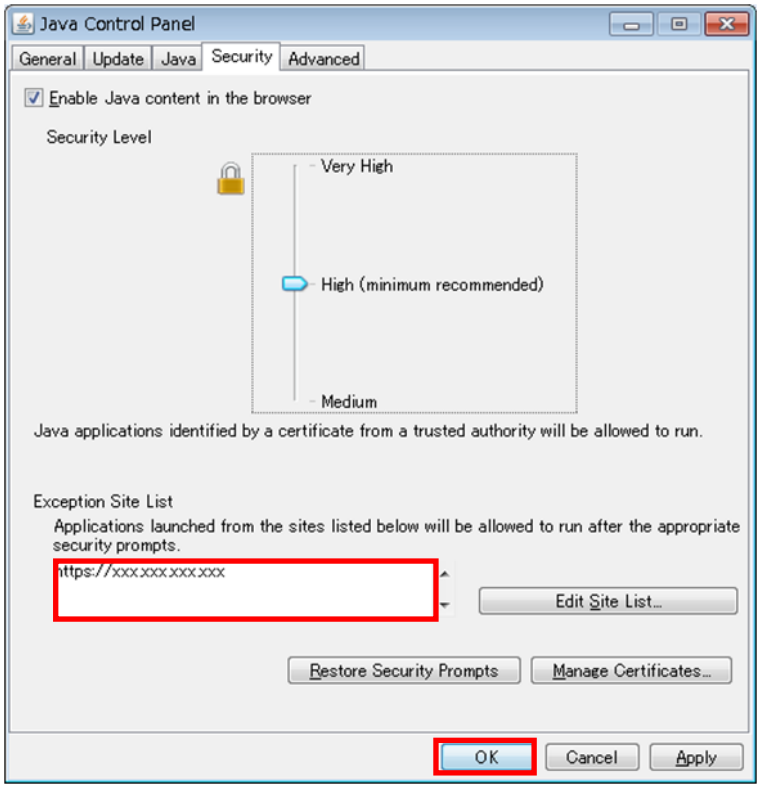
2. Click **Add**.



3. Enter "https://<serever blade Web console IP address>" and click **OK**.



4. Check that the IP address is shown in the Exception Site List and click **OK**.

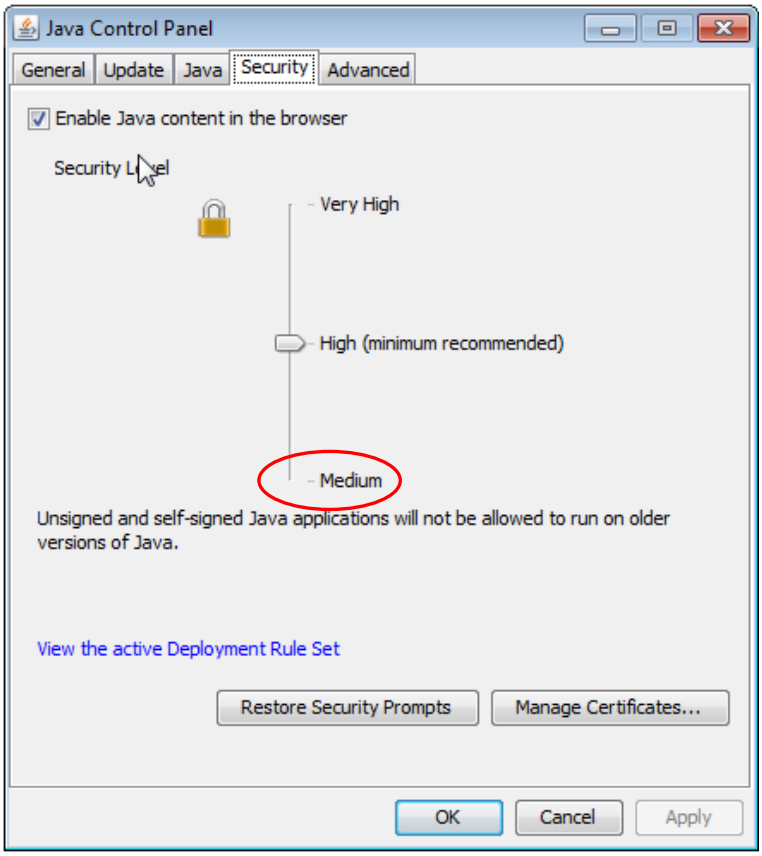


(b) Use Java Runtime Environment (JRE) version 7 update 21 or lower

Use JRE version before the security policy is changed. When enabling the remote console connection via SSL/TLS, use JRE7u2 or higher.

(c) Set the security level to Medium

Start Java Control Panel, and move the security level slider to **Medium**.

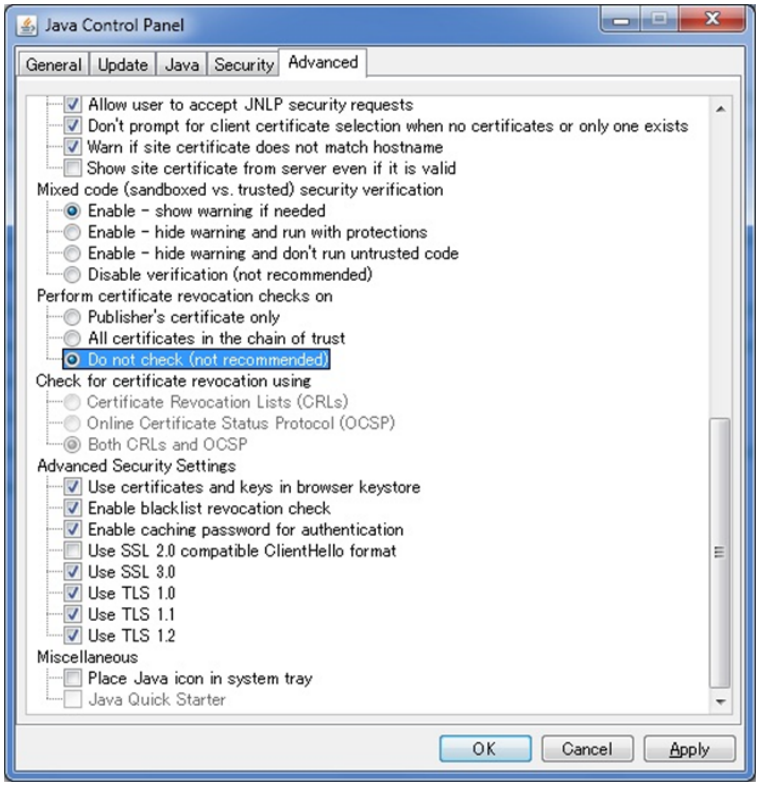


- Certificate revocation check

  Remote console application certificates with BMC 07-14/06-27 are the ones signed by the trusted certificate authority.

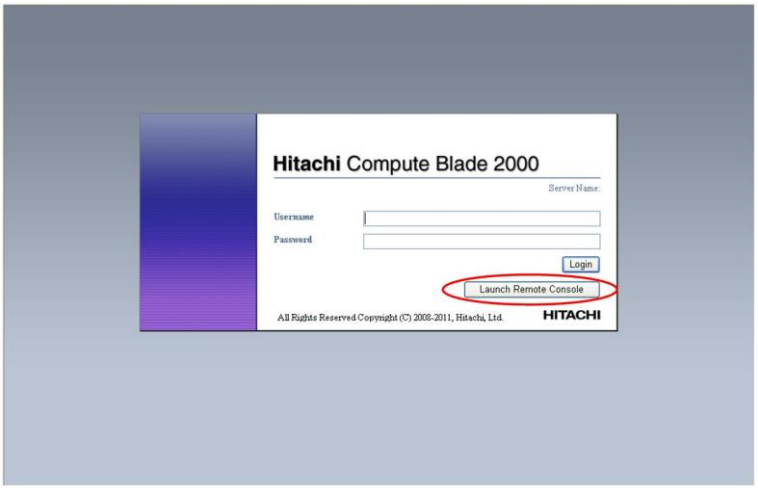
  Check “Do not check (not recommended)” under “Perform certificate revocation checks on” on the Java Control Panel. If not, startup may take longer or a warning message may appear showing the invalid certificate. For JRE 7 Update 21 or lower, certificate revocation is not checked by default.

  When you set this item, you also need to set Java Runtime Environment (JRE) version 7 update25 or higher.

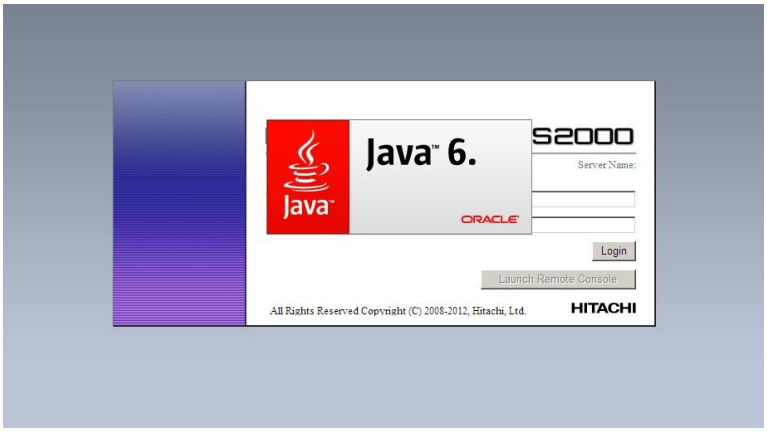


Starting Remote Console Application

1 Start a client browser and connect it to the Server Blade web console to display the login page.



2 Click **Launch Remote Console** on the login page. The Remote Console Application (Java application) will start.



3 If the following dialog box appears, click **Yes**.



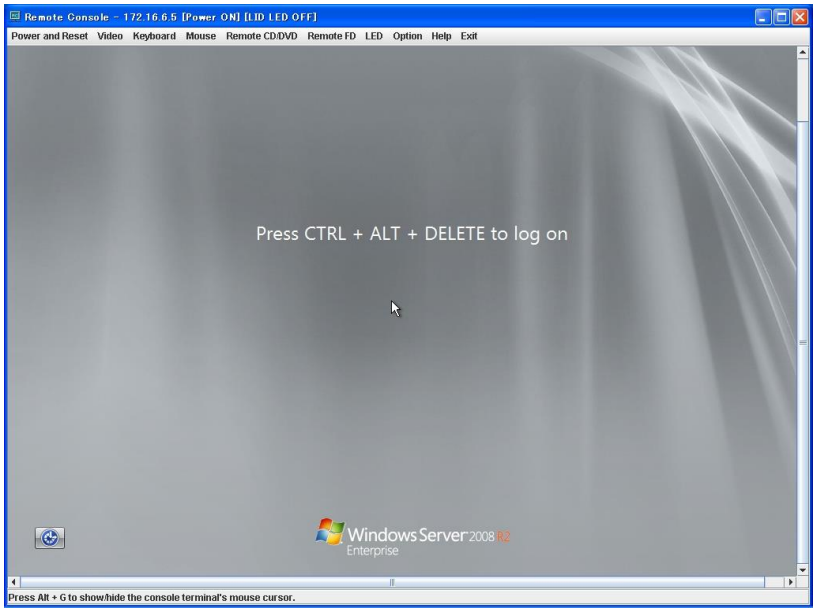
4 If the following dialog box appears, click **Run**.



5 When Remote Console Application is started, a login dialog appears. Enter the **User ID** and **Password**. Click **Connect**.



6 If user authentication succeeds, a window appears and the server blade VGA screen is displayed.



If you already logged in to the Server Blade Web Console, use **Launch Remote Console** on the left side of the page.

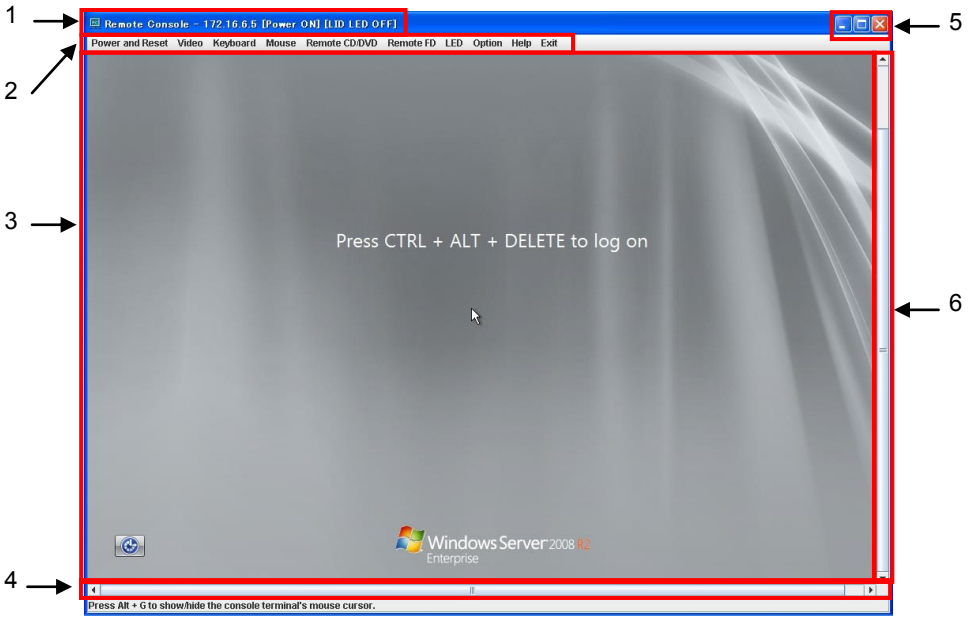


Terminating Remote Console Application

To terminate the Remote Console Application, select [Exit] on the menu bar, and click [Exit] on the submenu which appears by clicking [Exit] on the menu bar.

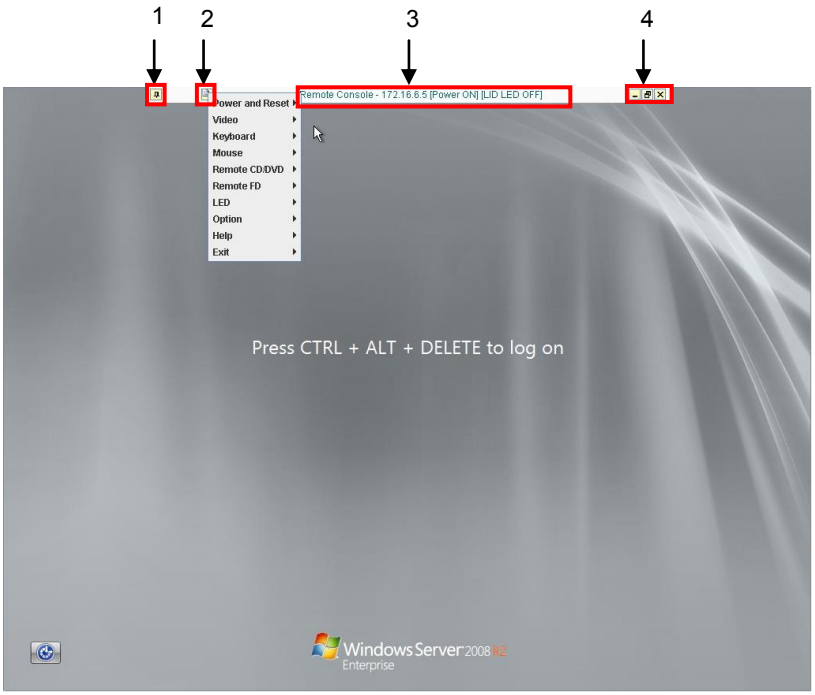
Functions of Window

This section describes the functions of the Remote Console Application window.



No.	Part	Function
1	Title bar	The title bar shows the IP address, power status, and Location ID Lamp (LID) light emitting diode (LED) status of the server blade.
2	Menu	The menu is used to execute the functions of the Remote Console Application. When a menu item is selected by the mouse cursor, the corresponding function is executed. See Menu items and functions for the functions of the menu items.
3	Remote screen	This area shows the video screen of the server blade.
4, 5	Scroll bars	The scroll bars are used to change the displayed part of the server screen.
6	Window control buttons	These buttons are used to minimize, maximize, and terminate the Remote Console Application window.

In full screen mode, you can use the bar at the top of the screen, which appears when the mouse cursor is moved to the top of the screen, to operate the Remote Console Application.



No.	Part	Function
1	Pin button	The button is used to have the bar always displayed.
2	Menu button	The button is used to display the menu that runs the functions of Remote Console. See Menu items and functions for the functions of the menu items.
3	Title	The title shows the IP address, power status, and LID LED status of the server blade.
4	Window control buttons	These buttons are used to minimize, maximize and terminate the window of Remote Console Application.

Menu items and functions

The following table lists the menu items and their functions.

Menu Item		Function
Power and Reset	Power ON	Power on the server blade.
	Forced power OFF	Power off the server blade.
	Reset	Reset the server blade.
	NMI	Generate NMI to the server blade.
Video	Refresh screen	Redraw the remote screen to show the latest server blade video screen.
	Full screen	Switch between Full Screen Mode and Window Mode.
Keyboard	Hold left Alt key	Press the left Alt key. Once this item is selected, the key is kept pressed until the item is selected again.
	Hold right Alt key	Press the right Alt key. Once this item is selected, the key is kept pressed until the item is selected again.
	Hold left Windows key	Press the left Windows key. Once this item is selected, the key is kept pressed until the item is selected again.
	Hold right Windows key	Press the right Windows key. Once this item is selected, the key is kept pressed until the item is selected again.
	Ctrl+Alt+Del	Press the Ctrl+Alt+Del key.
Mouse	Hide cursor	Hide the mouse cursor of the console terminal. Use the Alt+G key to display the mouse cursor again.
Remote CD/DVD	Redirect CD/DVD drive	Open a dialog to select CD/DVD drive. When CD/DVD drive is selected on the dialog, Remote CD/DVD is started. If this item is selected when Remote CD/DVD is running, Remote CD/DVD is terminated.
	Redirect CD/DVD image	Open a dialog to select CD/DVD image file. When CD/DVD image file is selected on the dialog, Remote CD/DVD is started. If this item is selected when Remote CD/DVD is running, Remote CD/DVD is terminated.
	Change CD/DVD image	Change the CD/DVD image file used for Remote CD/DVD. This item is activated when Remote CD/DVD is started with a CD/DVD image file. When this item is used, the media inserted in the virtual CD/DVD drive is replaced.
Remote FD	Redirect FD drive	Open a dialog to select FD drive. When FD drive is selected on the dialog, Remote FD is started. If this item is selected when Remote FD is running, Remote FD is terminated.
	Redirect FD image	Open a dialog to select FD image file. When FD image file is selected on the dialog, Remote FD is started. If this item is selected when Remote FD is running, Remote FD is terminated.
LED	Turn on LID LED	Turn on the Location ID LED of the server blade.
	Turn off LID LED	Turn off the Location ID LED of the server blade.
Option	Disable auto logout	Disable the auto logout function. If this item is selected again, the auto logout function is enabled.
Help	Shortcut keys	Show the list of shortcut keys.
	Version info	Show the version information of Remote Console Application.
Exit	Exit	Terminate Remote Console Application.

Shortcut keys

Some functions of Remote Console Application can be executed using the keyboard.

Shortcut Key	Function
Alt+Z	Press the left Alt key. The key is kept pressed until this shortcut key is used again.
Alt+M	Press the right Alt key. The key is kept pressed until this shortcut key is used again.
Alt+X	Press the left Windows key. The key is kept pressed until this shortcut key is used again.
Alt+N	Press the right Windows key. The key is kept pressed until this shortcut key is used again.
Alt+L	Press the Ctrl+Alt+Del key.
Alt+R	Redraw the remote screen to show the latest server blade video screen.
Alt+G	Hide the mouse cursor of the console terminal. If this shortcut key is used again, the mouse cursor is displayed.
Alt+W	Switch between Full Screen Mode and Window Mode.
Alt+E	Terminate Remote Console Application.

Mouse mode (Java application settings)

The remote console (Java application) supports the following two mouse modes:

ABSOLUTE mode

With this mode, you can remotely operate the mouse by using the mouse cursor displayed by the console terminal's OS.

RELATIVE mode

With this mode, you can remotely operate the mouse by using the mouse cursor displayed by the server OS.

To use the mouse remote control, you need to use the appropriate mouse mode depending on the server OS, as follows:

- For standard server blade X55A1/X55A2 models, or high-performance server blade X57A1/X57A2 models
  - On Windows, use ABSOLUTE mode.
  - On Red Hat Enterprise Linux, use RELATIVE mode.
  - If you use VMware vShpere 4 on a server blade, use RELATIVE mode.
- For standard server blade X55R3/X55S3/X55R4 models
  - On Windows or Red Hat Enterprise Linux 6, use ABSOLUTE mode.
  - On Red Hat Enterprise Linux 5, use RELATIVE mode.
  - If you use VMware vShpere 4 on a server blade, use RELATIVE mode.

You can change the mouse mode using the Server Blade web console. See "Remote KVM Settings" in Chapter 5 for details. You need to restart Remote Console Application to have the mouse mode effective after changing the mouse mode.

With Relative mode, disable the mouse cursor shown by the OS on the console terminal using the remote console application menu items or shortcut key. If the mouse cursor is not disabled, the mouse cursor shown by the OS on the server blade may not work properly.

Auto logout

If there are no keyboard or mouse operations for 15 minutes, the user is automatically logged off the remote console and the Remote Console Application is terminated.

The auto logout function can be disabled via the **Option-Disable Auto Logout** menu item.

Keyboard input

Remote Console Application supports the 101/104 keyboard and 106/109 keyboard. Other types of keyboards may not work correctly with the Remote Console Application. To use the 101/104 keyboard, both the server OS and console terminal's OS must be configured to use the 101/104 keyboard. To use the 106/109 keyboard, both of them must be configured to use the 106/109 keyboard.

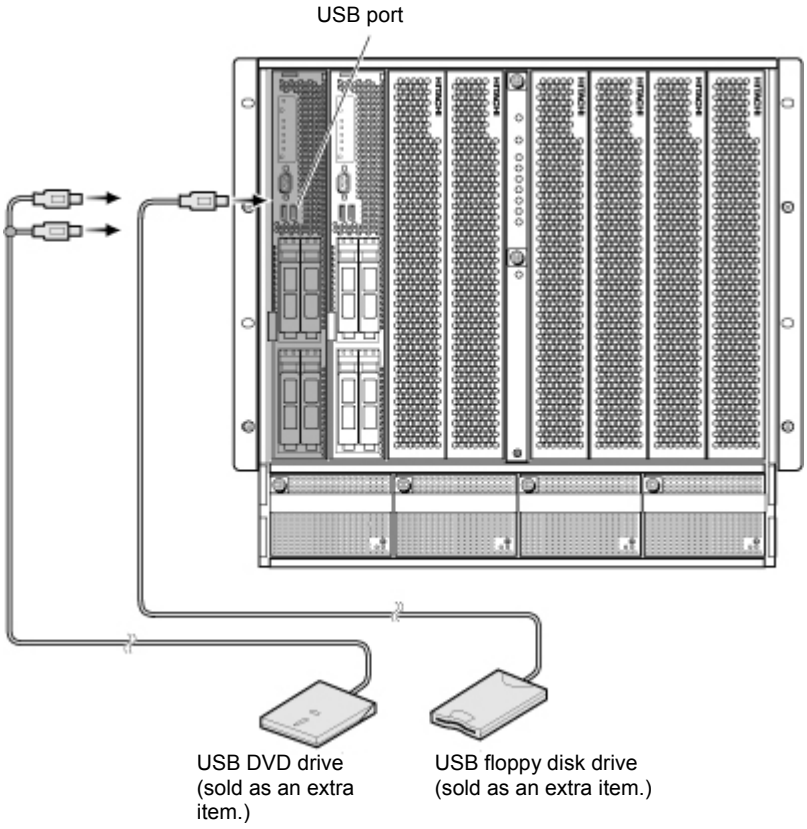
The following table shows that the keys work different when the keyboard is directly connected to a server blade.

Key	Status	Solution
Alt on the left Alt on the right	Keyboard input is not sent to the server blade.	Use menu or shortcut keys for keyboard input to the server blade.
Windows on the left Windows on the right	Keyboard input is not sent to the server blade.	Use menu or shortcut keys for keyboard input to the server blade.
Alphanumeric keys	For Linux on the server blade, Shift + Caps Lock key may be input every few seconds after an alphanumeric key is pressed.	For a case shift, use **S**hift + Caps Lock key. If Shift + Caps Lock key is repeatedly input, press the alphanumeric key once again.

When the Remote Console does not work properly, terminate it and then restart it. If re-startup does not work, see the *Compute Blade 2000 Remote Console Application Guide* in the remote console application CD that is attached to the system equipment.

Connect the USB cable to the server blade

One server blade is equipped with two USB ports.



A USB device such as DVD or floppy disk drive (FDD) drive can be connected to the USB connector.

The figure above shows an example with the standard server blade. USB port locations of the high-performance server blade are different from those of the standard server blade. See “High-performance server blade (X57A1/X57A2)” in Chapter 2 for more information.

Note

When using a server blade by connecting one plug of a combined cable to the USB port, do not connect the other plug of the combined cable to another server blade.

Connect the power cables

⚠ WARNING

Do not connect multiple power cables to a single electrical outlet. Overheating the power cables or outlet could cause a fire and trip the circuit breaker, which affects other devices on the same circuit.

When unplugging a power connecter, wait 10 or more seconds before reconnecting the power cable because the system equipment may not boot.

Note

- Provide one circuit on the branch circuit in the distribution panel with one outlet. Do not connect any other electrical device to the branch circuit to which this equipment is connected.
- Use a fuse free breaker (FFB) to equip with the distribution circuit panel as a circuit breaker.

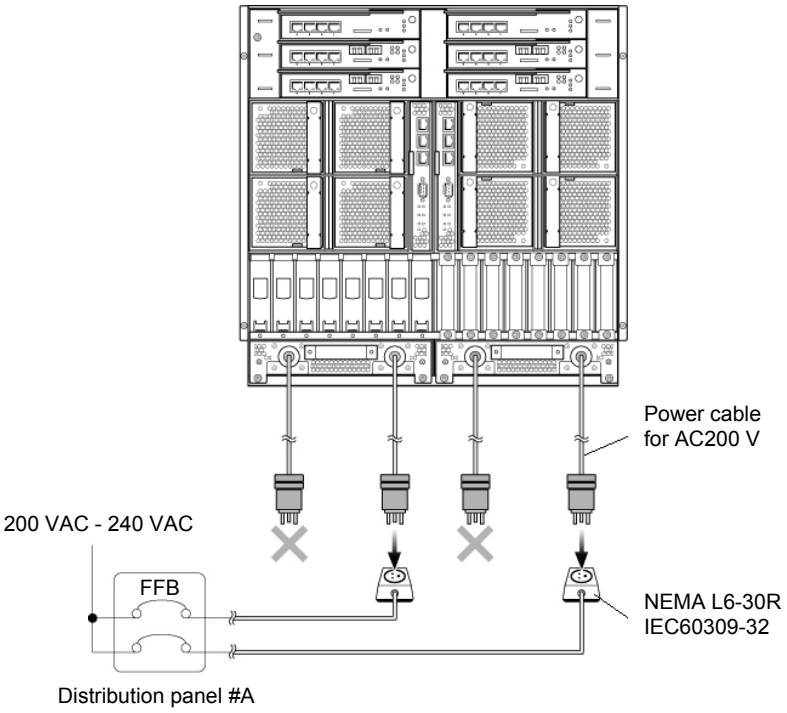
The number of power outlets National Electrical Manufacturers Association (NEMA) L6-30R (30A/250V) required is the same as that of power cables. (One in the smallest configuration; four in the largest configuration)

When changing the redundant configuration of the power module, make sure to contact the reseller from which you have purchased the equipment.

❑ A1 chassis

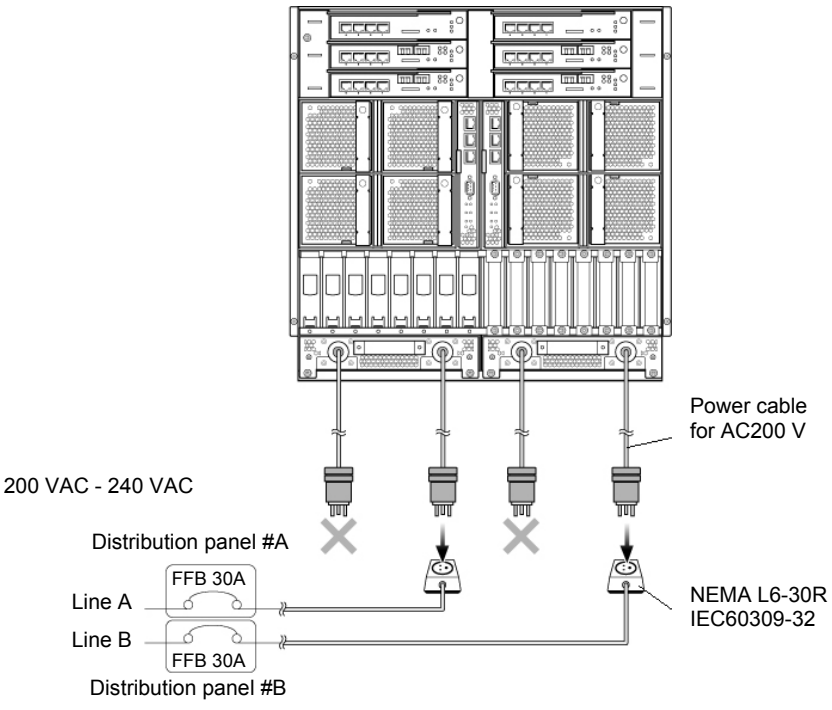
■ 1+1 power module redundant configuration

Connect power cables to each outlet from the distribution panel #A.



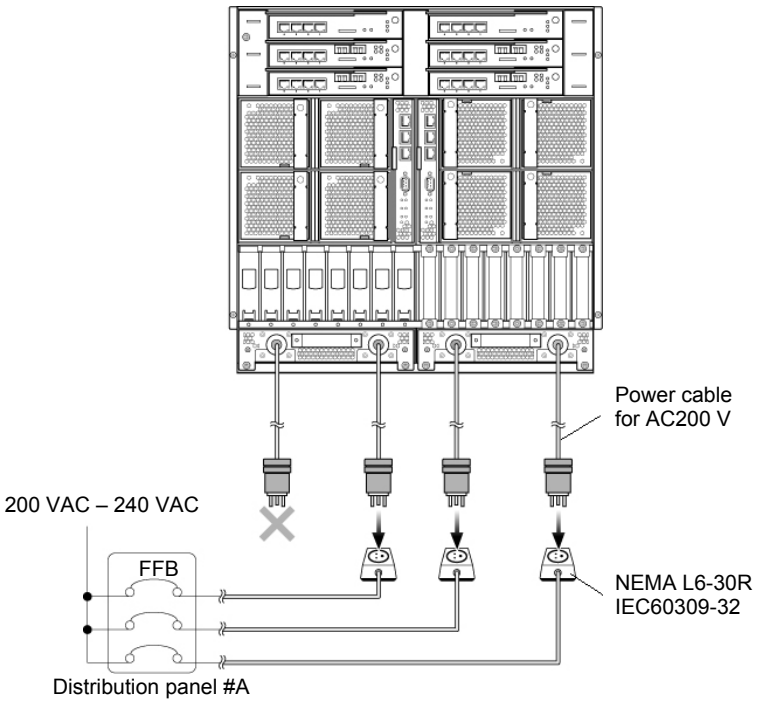
■ 1+1 AC power module redundant configuration

Connect power cables to each outlet from the distribution panel #A or # B.



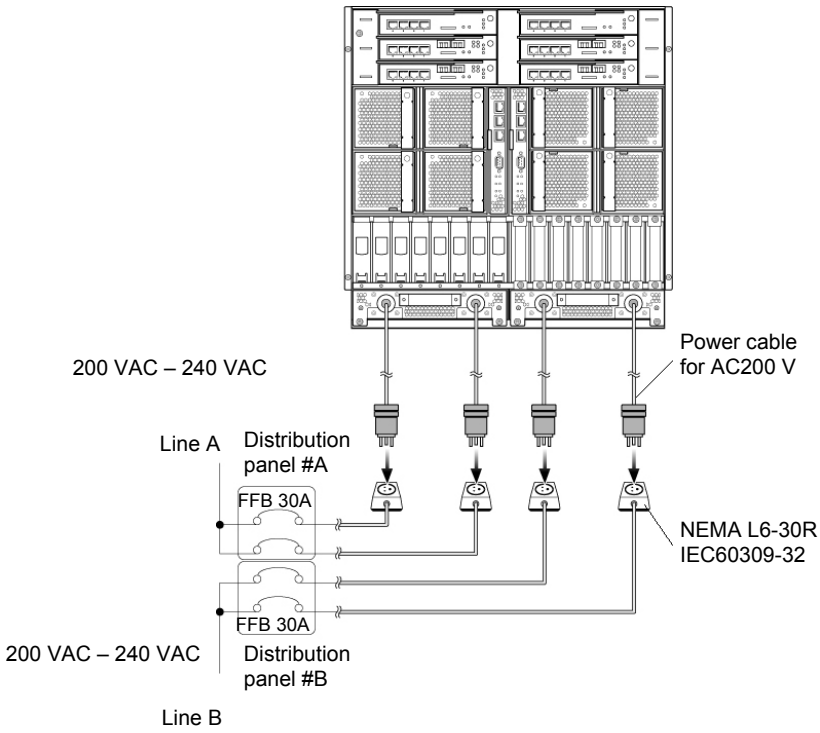
■ 2+1 power module redundant configuration

Connect power cables to each outlet from the distribution panel #A.



■ 2+2 AC power module redundant configuration

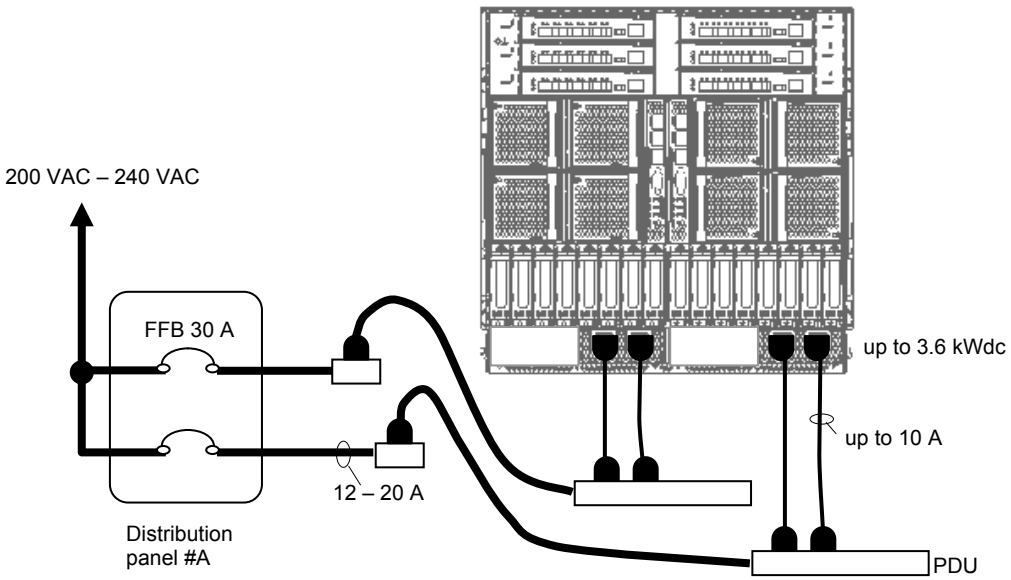
Connect power cables to each outlet from the distribution panel #A or # B.



❑ A2 chassis

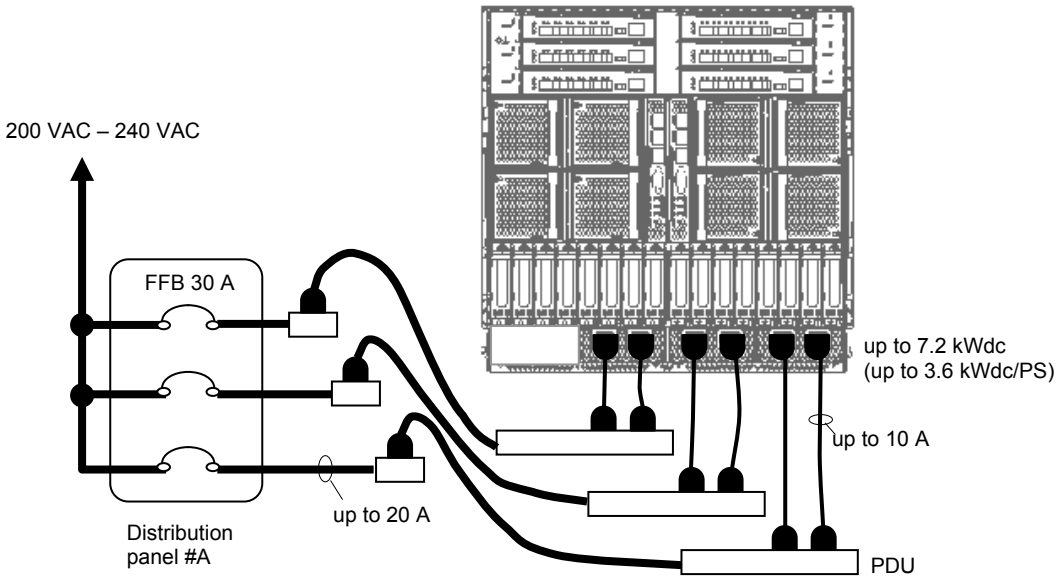
- 1+1 DC power module redundant configuration (up to 3.6 kWdc)

  Connect power cables to each outlet from the distribution panel #A.



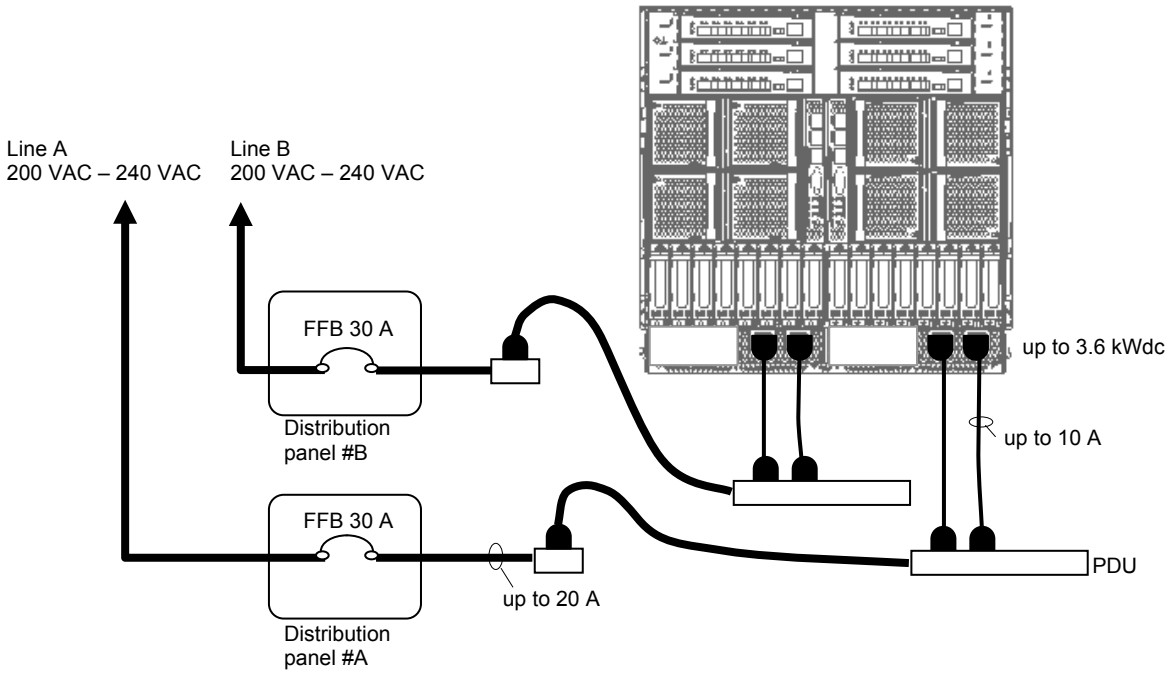
- 2+1 DC power module redundant configuration (up to 7.2 kWdc)

  Connect power cables to each outlet from the distribution panel #A.



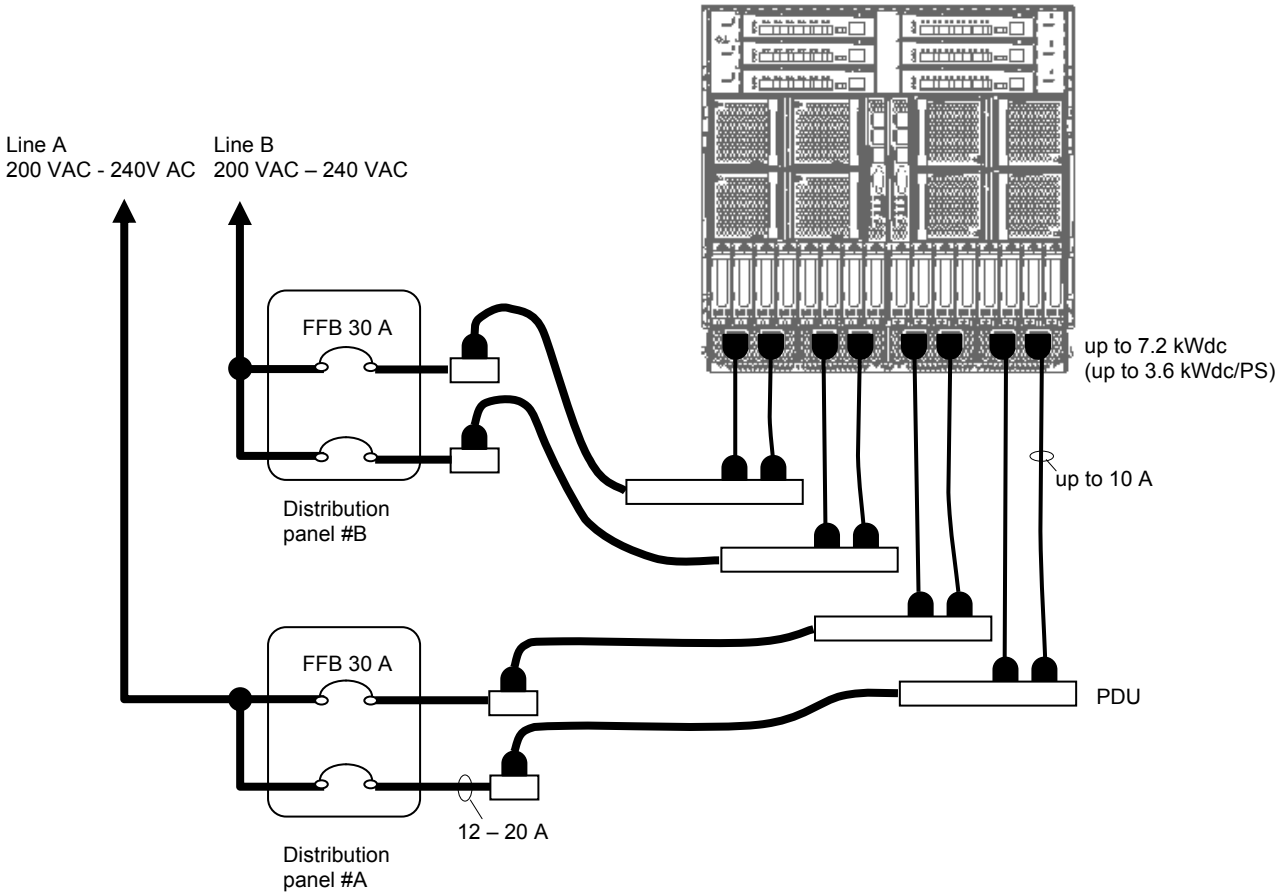
■ 1+1 AC power module redundant configuration (up to 3.6 kWdc)

Connect power cables to each outlet from the distribution panel #A or #B.



■ 2+2 AC power module redundant configuration (up to 7.2 kWdc)

Connect power cables to each outlet from the distribution panel #A or #B.



Connect the I/O slot expansion unit

This section describes how to connect power cables to the I/O slot expansion unit.

Connect the power cables

⚠ WARNING

Do not connect multiple power cables to a single electrical outlet. Overheating of the power cables or outlet could cause a fire and trip the circuit breaker, which affects other devices on the same circuit.

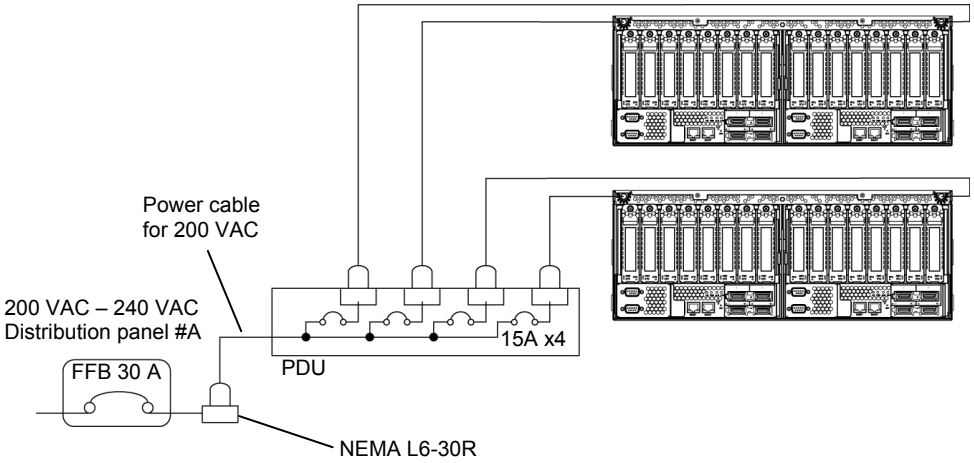
When unplugging a power connecter, wait 10 or more seconds before reconnecting the power cable. Otherwise the system equipment may not boot.

Note

- Install the outlet beside the equipment side because this has no circuit breaker.
- Provide one circuit on the branch circuit in the distribution panel with one outlet. Do not connect any other electrical device to the branch circuit to which this equipment is connected.
- Use a fuse free breaker (FFB) to equip the distribution circuit panel as a circuit breaker.

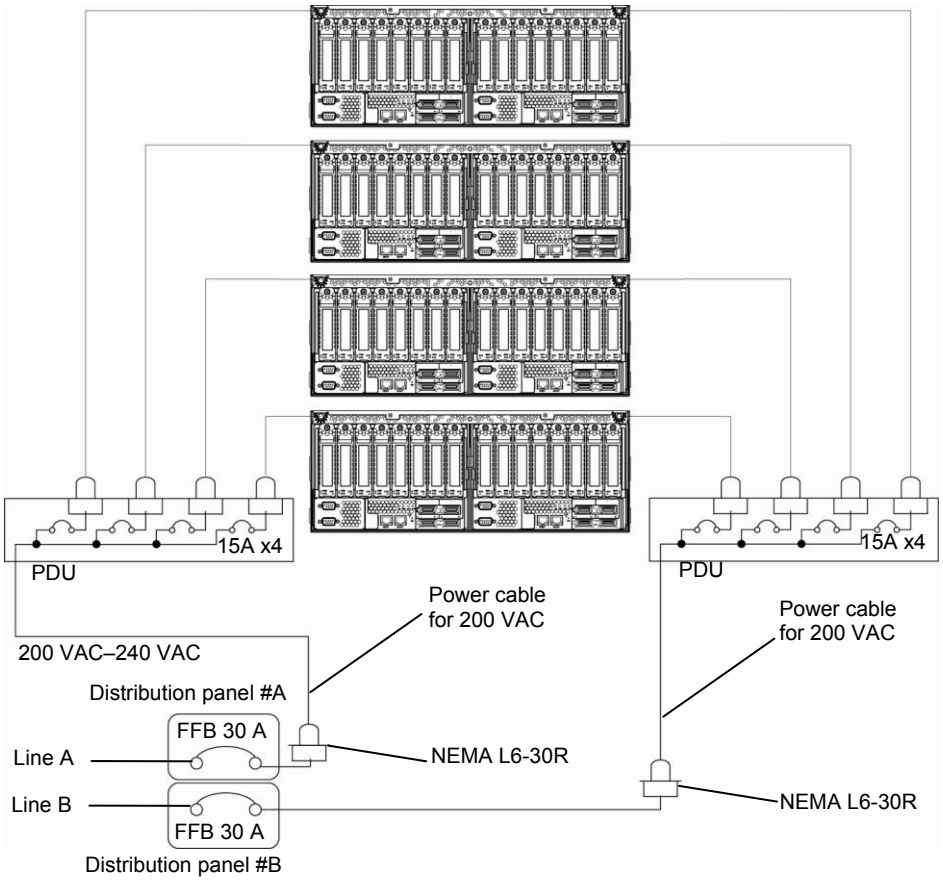
1 + 1 DC Input redundancy configuration

Connect the power cable to the power distribution unit (PDU), and connect the PDU to the socket outlet through the distribution panel #A.



1 + 1 AC Input redundancy configuration

Connect the power cable to the PDU, and connect the PDU to the socket outlet through the distribution panel #A.



Turning power on or off

This section describes how to turn on and off power to the system equipment.

> ***NOTICE***
>
> Follow the prescribed procedure for power operation. Powering on or off not according to the prescribed procedure can cause equipment failure.

Note After turning off or on the power to the system equipment, wait at least 10 seconds before turning on or off the power again.

Turn on power

1 Turn on power to peripheral equipment, such as a storage unit.

Note Some peripheral devices may need to be turned on before the system equipment is turned on. For details, see the manuals for those peripheral devices.

2 Open the rear door of the rack cabinet, and connect the power cable of the alternating current (AC) power input module to the power outlet.

The POWER LED of the power supply module blinks.

See the *Instruction Manual* that came with the rack cabinet. This is often located inside the front door of the rack cabinet.

3 When the POWER LED on the front panel stops blinking and lights solid orange, press and hold the power switch of the server blade for one second or more.

> ***NOTICE***
>
> When the N+M cold standby function is enabled, the power LED on the front panel lights solid orange, Smart Configure is automatically executed, and then the status LED: condition lamp (CND) on the server blade lights solid green. Confirm that the power LED of the front panel lights solid orange to show Smart Configure is complete before pressing the power button of the server blade for a second or more.

Turn off power

Some peripheral devices may need to be turned off before the system equipment is turned off. For details, see the manuals of the peripheral devices.

1 Execute shutdown for each server blade from the OS.

When power is turned off, the POWER LED on the server blade lights solid orange.

❑ Turn off the power forcibly

When the OS does not operate normally, the shutdown or normal power-down process of the server blade may not be possible. If this happens, press and hold the power switch for at least 4 seconds to turn off power.

If the power is forcibly turned off, subsequent normal operation of the OS or applications and data security cannot be guaranteed.

❑ Turn off the power of the system equipment

When turning off system equipment power, power off all server blades, and then execute the shutdown of the management module by using the Software Defined Networking (SDN) Command from the system service processor (SVP) console. See “SDN Command” in Chapter 6 for further details.

❑ Power saving

System Standby and Hibernate functions are not supported.

Do not select **System Standby** and **Hibernate** from **Shutdown** in the **Start** menu.

System Standby, **HDD Power Off**, and **Hibernate** in the power supply options are not available. Leave them set to **None**.

If **Standby** is selected in Windows, the system goes into standby and the power LED starts blinking green. To recover from standby, press the **Power** button on the front panel of the blade for a short period -- less than a second. This will recover the system and return the power LED to solid green.

Reboot the OS after recovering from standby, and the OS will return to normal operation.

4

Adding optional components

This chapter provides information about installing optional components.

Mounting internal optional components 74

Mounting internal optional components

Optional internal components can be mounted into the system equipment.

Only maintenance personnel are permitted to add each optional component to the system. Contact the reseller from which you have purchased the equipment, or call maintenance personnel.

⚠ CAUTION

Adding or replacing optional components inside the system equipment must be performed by maintenance personnel. Do not attempt to remove the cover of the equipment. Do not attempt to install or remove optional components. Since parts implemented in the system equipment are high-density, operation or maintenance by inexperienced persons might lead to injury or equipment failure. When you need to add or replace optional components, contact your reseller or call for maintenance personnel.

5

Server blade setup

This chapter describes the server blade setup.

Standard server blade settings (X55A1/X55A2/X55R3/X55S3 models).....76
Standard server blade setup menu (X55A1/X55A92 Models).....127
Standard server blade setup menu (X55R3/X55S3/55R4 models).....141
Remote CD/DVD boot procedure.....158
Hardware memory dump.....167
MegaRAID WebBIOS.....175
High-performance Server Blade settings (X57A1/X57A2 models).....402
High-performance server blade setup menu (X57A1/X57A2 models).....415

Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models)

This section describes the standard server blade setup with the Web console.

See Standard server blade setup menu (X55A1/X55A2 models) or Standard server blade setup menu (X55R3/X55S3/55R4 models) for the basic input/output system (BIOS) menu.

Initial settings with server blade web console

A server blade can be managed remotely by using the server blade web console.

This section describes how to perform initial settings of the server blade via the server blade web console.

The following items require initial settings:

- User account configuration
- Logical partition (LPAR) manager boot settings
- Mouse mode settings for the remote console
- Baseboard Management Controller (BMC) time settings

❑ Connection

Connect to the server blade Web console via the management network of the management module. See “External Interface of the Management Module” in Chapter 6 for information about how to connect to the network.

Confirm that the client web browser is properly configured before using the server blade Web console. If the settings are not appropriate, the server blade Web console will not work properly.

To use the server blade Web console, you need one of the web browsers shown in the following table.

#	Web browser
1	Internet Explorer 6.0 or later* (Browser tabs are not available.)
2	Firefox 2.0 or later
* When connecting to the server blade Web console using TLS v1.1/1.2, use Windows 7 or later, or Windows Server 2008 R2 or later.	

1 Disable the pop-up blocker of the client web browser to enable the pop-up windows. If there are other pop-up-blocker-like features, those features also need to be disabled.

2 Enable JavaScript.

❑ Login

1 Start the client web browser.

2 Enter `http://<server blade` Internet Protocol (IP) `address>:<port number>` to the URL address field. You can omit the port number only when the port number is “80”.

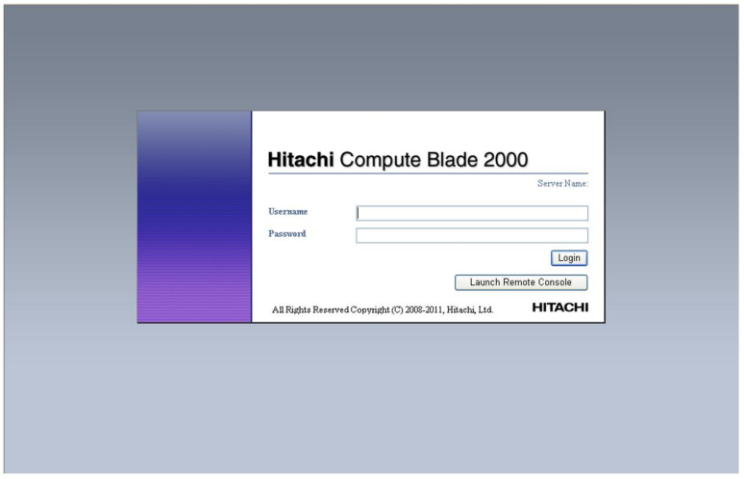
To find the server blade IP address, see “LC Command” in Chapter 6.

Ex. Blade IP address: 192.168.0.2 and Port number: 80



To use the HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) protocol, enter `https://<server blade IP address>:<port number>` to the URL address field. You can omit the port number only when the port number is **443**.

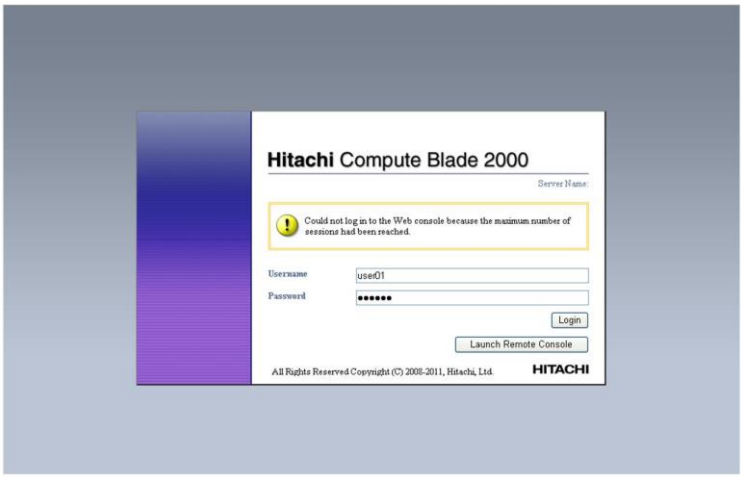
3 When the connection is established, the following login screen is displayed.



Launch Remote Console shown in the login screen is available with the following system firmware revisions or later.

- Standard server blade: X55A1/X55A2 models
  BMC: 03-91
- Standard server blade: X55R3/X55S3/X55R4 models
  BMC: 05-01 or 07-01
- High-performance server blade: X57A1/X57A2 models
  BMC: 04-48 or 06-01

4 Enter the user name and password on the login screen. When the user is authenticated, the following screen is displayed. Up to two users are allowed to log in to the server blade Web console at the same time. If two users have already logged in, the following screen is displayed.



Tip Using the default server blade setting configured during shipment, you can log in to the server blade as an administrator by entering `user01` to the user name field and “pass01” to the password field on the login screen.

- If a user account is set in the server blade different from the above, you cannot log in using the method mentioned above.
- Hitachi Data Systems recommends selecting a user account name different from the default setting value for security purposes.

When the login is successful, the server information menu screen is displayed.



You can select menu items using the upper tabs and tree menu on the left. When a menu item is selected, the screen for displaying or changing the corresponding settings is displayed. To finish your operation and log out, click **Logout** on the upper right of the screen.

Tip

- Remote console application (Java application) is available with the following system firmware revisions or later:
  Standard server blade: X55A1/X55A2 models
  BMC: 03-91
  Standard server blade: X55R3/X55S/X55R4 models
  BMC: 05-01 or 07-01
  High-performance server blade: X57A1/X57A2 models
  BMC: 04-48 or 06-01
- If no operation is run for more than 30 minutes, the system will log out automatically.
- Make sure to log out by clicking **Logout** on the upper right of the screen before closing the browser. When closing the browser without clicking Logout, you remain in the server blade web console until automatically logging out after 30 minutes. If you close out the browser without logging out, you cannot log in for 30 minutes.
- For this automatic log out feature, the server blade web console session will be closed if the BMC time is set back or set ahead more than 30 minutes. (The BMC time can be adjusted by a user, synchronization to Network Time Protocol (NTP) server, or management software such as SC (ServerConductor) Agent installed:
  Time synchronization function agent and LPAR manager firmware.) You can log in to the server blade web console again when the automatic logout occurs.

❑ User account configuration

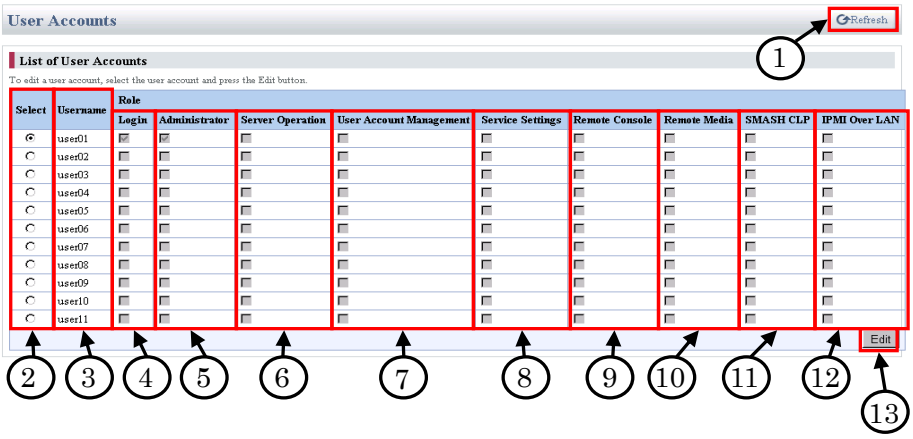
Configure user accounts to operate the server blade remotely.

Privileges to operate the server blade, validity, username, and password can be configured for each user account.

Select the **Server Settings** tab and then select **User Accounts** in the tree menu to display the following screen.

(1) List of user accounts screen

This screen shows the list of user accounts.



#		Item	Description
1	Refresh		Reloads user account information
2	Select		Option buttons to select a user account
3		Username	Shows the names of user accounts.
4	Role	Login	Shows the roles given to user accounts. Systems Management Architecture for Server Hardware (SMASH) IPMI: intelligent platform management interface
5		Administrator	
6		Server Operation	
7		User Account Management	
8		Service Settings	
9		Remote Console	
10		Remote Media	
11		SMASH CLP	
12		IPMI Over LAN	
13	Edit		Goes to the **Edit User Account** screen. If no option button is checked, the screen remains as it is.

Role

You can configure the range of operations allowed for a user by giving roles to the user account. The following table describes each role.

#	Role name	Description
1	Login	Role to log in to the services of the server blade. A user without this role is considered invalid and cannot log in to any service.
2	Administrator	Role that represents the privilege of administrator. A user with this role can operate every operation of a server blade.
3	Server Operation	Role to operate the power control, reset of a server blade and also to edit extensible firmware Interface (EFI) and LPAR manager settings.
4	User Account Management	Role to edit the user account setting.
5	Service Settings	Role to configure the services of the server blade.
6	Remote Console	Role to use the remote console, which enables the console terminal to display the video graphics array (VGA) screen of the server blade and remote control of the keyboard and mouse. This role also allows users to use the OS console.
7	Remote Media	Role to use the remote floppy disk (FD) function and remote compact disc/digital versatile disc (CD/DVD) function.
8	SMASH CLP (*1)	Role to use SMASH CLP/WS-MAN
9	IPMI Over LAN (*2)	Role to use IPMI Over LAN.

Notes:

*1 This role is available for the following BMC firmware version or later.
BMC: 05-50 or later with standard server blades, X55R3, X55S3 or X55R4 model
BMC: 06-01 or later with a high-performance server blade, X57A2 model

*2 This role is available for the following BMC firmware version or later.
BMC: 05-18 or 07-01 with a standard server blade, X55R3 or X55S3 model
BMC: 04-71 or 06-01 with a high-performance server blade, X57A1 or X57A2 model



For information about the remote console (Reclient), see the *Hitachi Compute Blade 2000 Remote Console Application User's Guide* contained in the remote console application CD that came with the system equipment.

For information about the remote console (Java application), see "Remote Console Application (Java Application)" in Chapter 3.

(2) Initial setting of user accounts

The following table shows the initial setting of user accounts.

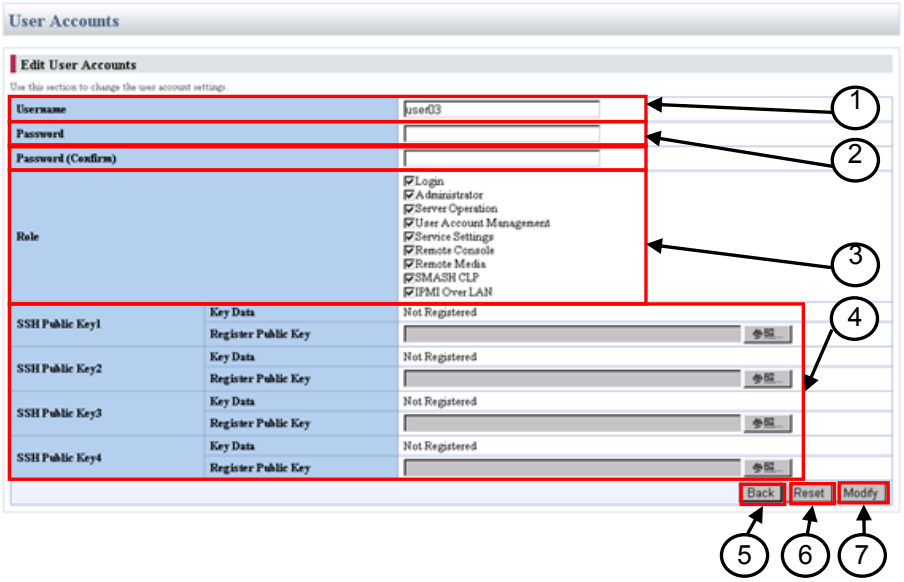
#	User name	Password	Role	Description
1	user01	pass01	Login Administrator	User as the server blade administrator. The role of the user cannot be changed.
2	user02	pass02	None	Ordinary users
3	user03	pass03		
4	user04	pass04		
5	user05	pass05		
6	user06	pass06		
7	user07	pass07		
8	user08	pass08		
9	user09	pass09		
10	user10	pass10		
11	user11	pass11		

(3) Changing and deleting user account

Click the **option** button of the user account to change or delete, and click **Edit**.
The screen to change the settings of the selected user account is displayed.

(4) Edit user accounts screen

You can change the user account settings on this screen.

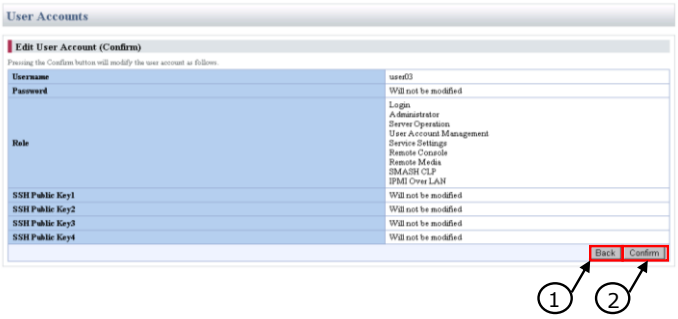


#	Item	Description
1	Username	Enter user account name: up to 32characters
2	Password	Enter password: up to 32 characters.
	Password (Confirm)	Re-enter the password for confirmation.
3	Role	
	Login	Check the roles to assign to the user account.
	Administrator	
	Server Operation	
	User Account Management	
	Service Settings	
	Remote Console	
	Remote Media	
	SMASH CLP	
	IPMI Over LAN	
4	SSH Public Key 1-4: Settings of the public key used for Secure Shell connection.	
	Key Data	Displays key data. If not data, “Not Registered” is displayed.
	Register Public Key	Uploads and registers the public key
5	Back	Cancels the edited contents and returns to the List of User Accounts screen.
6	Reset	Cancels the edited contents in this screen.
7	Modify	Validates the edited settings and moves to Edit User Accounts (Confirm) screen.



- You cannot omit entering username.
- When setting a password, enter the same password in the password field and the password confirm field.
- When editing a user account, entering the password is not essential. If no password is entered, it is handled as no password change.
- SSH public key files generated by OpenSSL are supported.
- The maximum file size allowed is 2 Kbytes.
- If you install an OS, check each box of “Remote Console” and “Remote Media” of the user account to operate the remote console application.
- Roles of the user account for server blade administrator cannot be changed.
- Only the user with the Administrator role can change roles of user accounts.
- If your server blade was installed with BMC03-59 or earlier versions, the following symbols: &, <, >, “, are not available for a user name and password.

When you click **Modify**, the following confirmation screen is displayed.



#	Item	Description
1	Back	Cancels the edited settings and returns to Edit User Account screen.
2	Confirm	Allows the edited settings to become effective.

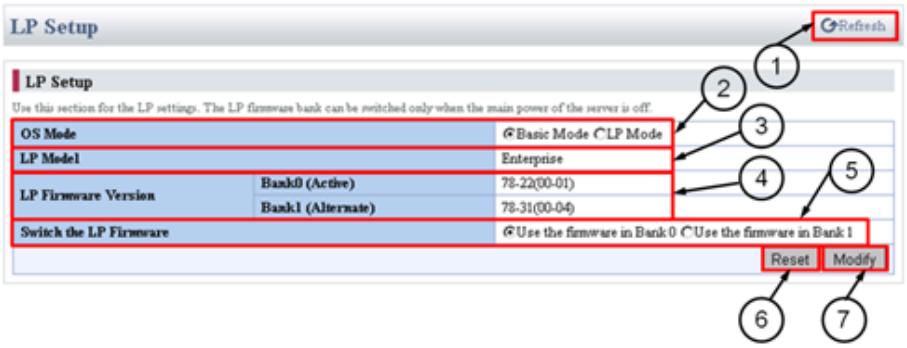
❑ LPAR manager boot settings

Configure the LPAR manager boot settings.

Select **Server Operation** in the upper tabs and then select **LP Setup** in the tree menu on the left to display the following screen.

If you do not use LPAR manager, set OS mode to Basic mode, which is the default setting.

If you use LPAR manager, set OS mode to logical partitioning manager (LP) mode.



#	Item	Description
1	Refresh	Reloads the information.
2	OS Mode	Basic mode: Select this not to use LPAR manager. LP mode: Select this to use LPAR manager.
3	LP Model	Displays the LP model string.
4	LP Firmware Version	Bank0, Bank1: Displays LP firmware version of each bank. Active: shows the firmware bank currently selected. Alternate: shows the firmware bank not currently selected. When firmware exists, its version is shown. When no firmware exists, “N/A” is shown.
5	Switch the LP firmware	Selects which bank (Bank0 or Bank1) is to be used for next LPAR manager boot. Switching banks is executed at the next power-on or reset.
6	Reset	Cancels the edited settings.
7	Modify	Validates the edited settings and moves to the confirmation screen.

Tip

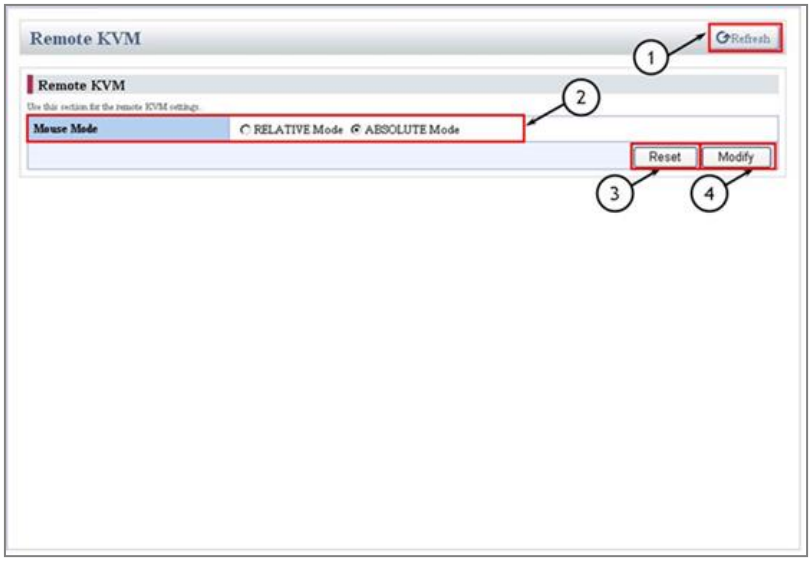
- See ‘LP Mode Setting’ in “LPAR manager Boot” in Chapter 12 for more information.
- LP Model is displayed only when the BMC firmware 03-45 or above and LPAR manager firmware 57-10 or above are installed on the server blade.

❑ Mouse mode settings for the remote console

Set a mouse mode to operate the server blade with the Remote Console Application.

Select **Server Settings** in the upper tabs and then select **Remote KVM** in the tree menu.

Select an appropriate mouse mode to install according to the OS.



#	Item	Description
1	Refresh	Reloads the information.
2	Mouse Mode	ABSOLUTE mode: Operates the remote console mouse using the mouse cursor of the console terminal. RELATIVE mode: Operates the remote control mouse using the mouse cursor on the server blade screen. Use a mouse mode appropriate for the server OS. For details about Reclient, see the *Remote Console Application User's Guide Compute Blade 2000*; for details about Java application, see “Mouse Mode (Java application settings)” in Chapter 3.
3	Reset	Cancels the edited settings.
4	Modify	Validates the edited settings and moves to the confirmation screen.

Tip

For the remote console (Reclient), see the *Hitachi Compute Blade 2000 Remote Console Application User’s Guide* contained in the remote console application CD that came with the system equipment.

For the remote console (Java application), see “Remote Console Application (Java Application)” in Chapter 3.

❑ BMC time settings

Set the time of the server blade BMC (Baseboard Management Controller).

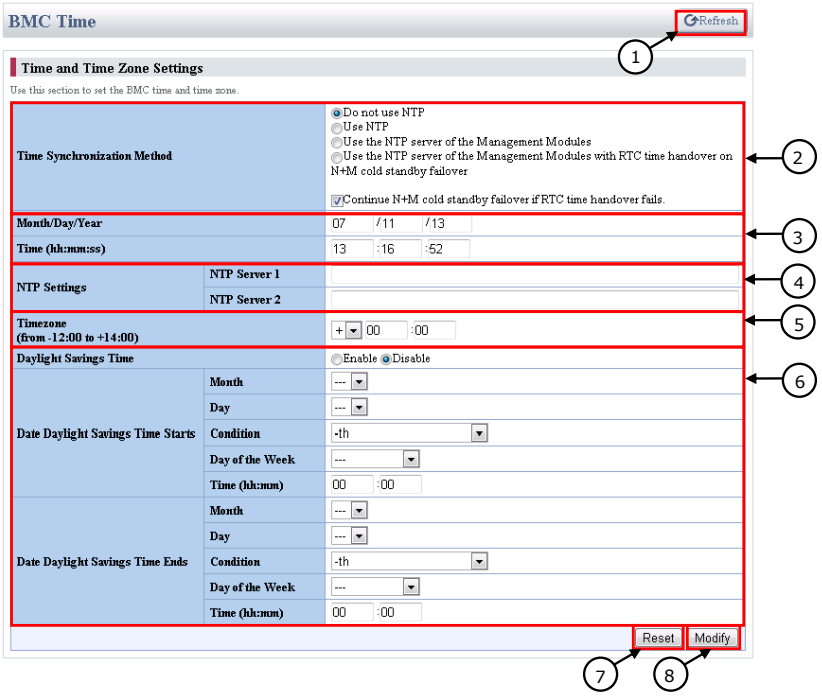
Select **Server Settings** in the upper tabs and then select **BMC Time** in the tree menu on the left to display the following screen.

BMC time is used for (1) time stamp of error logs, and (2) the schedule operations linked with ServerConductor.

Tip

In addition to the BMC time setting using the server blade web console, set the time in the EFI Menu during the installation of the server blade.

See 'EFI Setup Screen' in "Standard server blade setup menu (X55A1/X55A2 models)" for setting the time in the EFI menu.

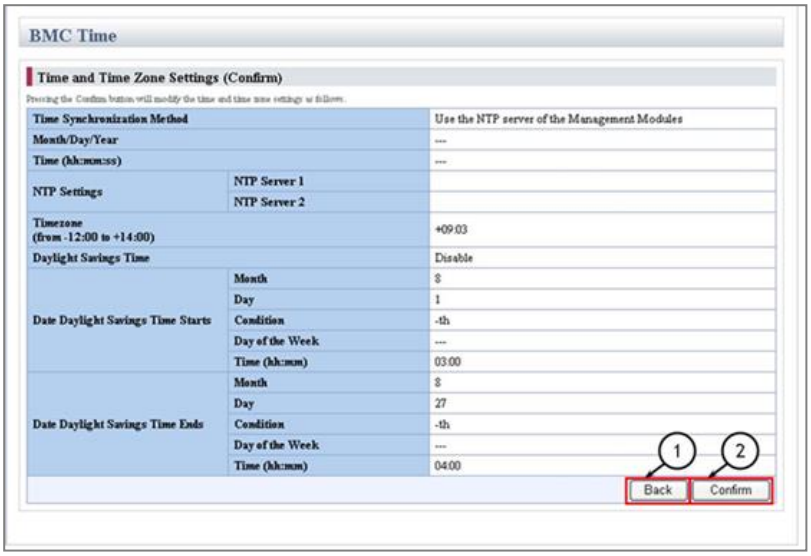


#	Item	Description
1	Refresh	Reloads the information.
2	Time Synchronization Method	Do not use NTP: The BMC time is set as follows: (1) Basic mode (not using LPAR manager) with SC (ServerConductor) Agent installed: Time synchronization function of SC Agent sets the BMC time to the OS time. - The BMC time will be updated after OS startup. - Change the OS time when you want to change the BMC time. The BMC time settings via server blade Web console is rewritten or ignored. (2) Basic mode without SC Agent installed: the BMC time is set and/or adjusted manually via the BMC Time screen.

#	Item	Description
		The BMC time is independent of the OS time and is determined by a clock that has an error by ± 4 minutes per month. Check the time on the BMC Time Screen, and adjust the time if the error is large. (3) LP mode: LPAR manager sets BMC time to "LP system time". - The BMC time will be updated after LPAR manager startup. - Change the LP system time when you want to change the BMC time. BMC time settings via server blade Web console is rewritten or ignored. "Use NTP" (displayed on the screen) The BMC time is synchronized to the time provided by the external NTP server. Set the NTP server address referring to the #4. "Use the NTP server of the Management Modules" (displayed on the screen) BMC time is synchronized to the time of the management module. "Use the NTP server of the Management Modules with RTC time handover on N+M cold standby failover" * (displayed on the screen) - BMC time is synchronized with the management module time. - Real time clock (RTC) time of the active partition is taken over to the standby partition at N+M failover. "Continue N+M cold standby failover if RTC handover fails." * (displayed on the screen) - Available only when "Use the NTP server of the Management Modules with RTC time handover on N+M cold standby failover" is checked - See "N+M Cold Standby" in Chapter 13 for details.
3	Month/Day/Year Time	Enter each item of your local time.
4	NTP Settings	Enter the NTP server IP address when setting "Use NTP" in item #2, the Time Synchronization Method field.
5	Timezone (from -12:00 to +14:00)	Set the local time zone where the server blade is installed. This should be identical to the time zone set in the OS of the server blade. If you use LP mode, this should be identical to the time zone of "LP system time".
6	Daylight Savings Time	If DST setting is necessary in the area where the server blade is installed, enable DST and set the start and end time.
7	Reset	Cancels the edited settings.
8	Modify	Validates the edited settings and moves to the confirmation screen.
*This function can be used only with standard server blade X55R4.		

Tip

- Details for setting the timezone of the LP system time are described in Logical partitioning manager-LPAR manager Screen Operations-Summary of LPAR manager Screens-Date and Time.
- If Use NTP or Use the NTP server of the Management Modules is selected in #2 Time Synchronization Method, the time synchronization between the BMC time and the OS time by the SC agent is disabled. The time synchronization between the BMC time and LP system time is also disabled.



#	Item	Description
1	Back	Cancels the edited settings and returns to BMC Time screen.
2	Confirm	Allows the edited settings to be effective.

❑ Logout

Click **Logout** on the log out screen of the server blade Web console.

Server blade web console function

This section describes the functions of the server blade web console.

(1) List of user accounts screen

The following table shows functions provided by the server blade web console.

#	Menu	Function
Server Operation tab		
1	Server Information	Shows the server blade information
2	Power and LEDs	Controls the power status and reset operation. Shows the power status and light emitting diode (LED) status.
3	EFI Setup	Configures the EFI settings.
4	LP Setup	Configures the LPAR manager boot settings.
5	Server Configuration and Reduction	Shows the central processing unit (CPU) and memory configuration and sets the planned reduction.
Server Settings tab		
6	Language Settings	Sets the language to use on the server blade Web console.
7	Asset Information	Sets the asset information.
8	Network Settings	Shows the network settings and configures access restriction settings.
9	Service Settings *1	Enables or disables the services of the server blade and configures the port numbers for the services.
10	Security and Service Settings *2	Enables or disables security and services, and sets port numbers for the services.
11	User Accounts	Configures user accounts.
12	BMC Time	Sets the BMC time and time zone.
13	Remote KVM	Sets the mouse mode of the remote console.
14	SSH Server	Sets the authentication method of SSH and shows the fingerprints of the Host Keys.
15	SSL Server	Sets up Secure Socket Layer (SSL) server certificate.
16	DNS Client	Sets the DNS server used by a server blade.
17	IPMI Over LAN	Sets IPMI Over LAN user account. (*3)
18	LDAP	Configures Lightweight Directory Access Protocol (LDAP) user authentication. (*4)
Maintenance tab		
19	EFI Firmware Management	Updates EFI firmware.
20	BMC Firmware Management	Updates BMC firmware and switches firmware banks.
21	Backup System Settings	Backups EFI settings and LPAR manager boot settings.
22	Restore System Settings	Restores EFI settings and LPAR manager boot

#	Menu	Function
		settings.
23	Backup Server Management Settings	Backups the server blade settings except for EFI and LPAR manager settings.
24	Restore Server Management Settings	Restores the server blade settings except for EFI and LPAR manager settings.
25	Restart BMC	Restarts BMC.
26	FPGA ROM Management	Updates field programmable gate array (FPGA) Read Only Memory (ROM). (*5)
27	Cancel PCI Express Deconfiguration	Cancels peripheral components interconnect (PCI) Express deconfiguration. (*6)
Log tab		
28	Download Logs	Downloads the server blade logs.
29	Operation Log	Downloads operation logs.

*1: This menu is available for the following system firmware version or later.
Standard server blade X55R3/X55S3 models: BMC 07-01
High-performance server blade X57A1/X57A2: BMC 06-20

*2 This menu is available for the following system firmware version or later.
Standard server blade X55R3/X55S3/X55R4 models: BMC 07-01
High-performance server blade X57A1/X57A2: BMC 06-20

*3 This menu is available for the following system firmware version or later.
Standard server blade X55R3/X55S3/X55R4 models: BMC 05-18 or 07-01
High-performance server blade X57A1/X57A2: BMC 04-71 or 06-01

*4: This menu is available for the following system firmware version or later.
Standard server blade X55A1/X55A2 models: BMC 03-60
Standard server blade X55R3/X55S3 models: BMC 05-00 or 07-01
High-performance server blade X57A1/X57A2: BMC 04-00 or 06-01

*5: This menu is available only for high-performance server blades.

*6: This menu is not available for this system equipment.

(2) Roles for operation

The roles assigned to the user account determine the operations of the server blade web console that the user can execute. The following table shows the relation between the roles and the operations enabled by the roles.

#	Menu	Available operation with each role			
		Admin-istrator	Server Operation	Service Settings	User Account Management
Server Operation tab					
1	Server Information	All	All	Information display only.	Information display only.
2	Power and LEDs				
3	EFI Setup				
4	LP Setup				
5	Server Configuration and Reduction	Information display only.	Information display only.	Information display only.	Information display only.

#	Menu	Available operation with each role			
		Admin-istrator	**Server Operation**	**Service Settings**	**User Account Management**
Server Settings tab					
6	Language Settings	All	Information display only	All	Information display only.
7	Asset Information				
8	Network Settings				
9	Service Settings				
10	Security and Service Settings				
11	User Accounts		Your own account only	Your own account only	Settings of ordinary user accounts
12	BMC Time		Information display only.	All	Information display only.
13	Remote KVM				
14	SSH Server				
15	SSL Server				
16	DNS Client				
17	LDAP		None	None	None
Maintenance tab					
18	EFI Firmware Management	Information display only.	Information display only.	Information display only.	Information display only.
19	BMC Firmware Management				
20	Backup System Settings	None	None	None	None
21	Restore System Settings				
22	Backup Server Management Settings				
23	Restore Server Management Settings				
24	Restart BMC				
25	FPGA ROM Management	Information display only	Information display only	Information display only	Information display only
26	Cancel PCI Express Deconfiguration	All	All		
Log tab					
27	Download Logs	All	All	None	None
28	Operation Log	All	None	None	None



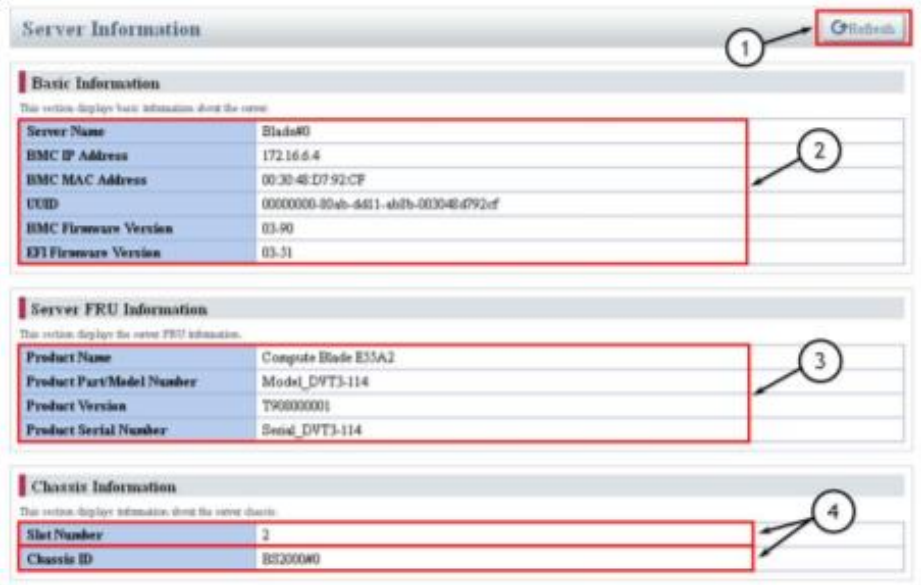
- The Remote Console, Remote Media, and SMASH CLP roles are not related to the operations of the server blade Web console.
- With X57A1/X57A2 model, you can operate all menus in the server configuration and reduction settings using the Administrator role.

Server Operation tab

Using the Server Operation tab, you can display the information of the server blade, control the power status, and configure the boot settings of the server blade.

❑ Server information

The following screen shows the server blade information.

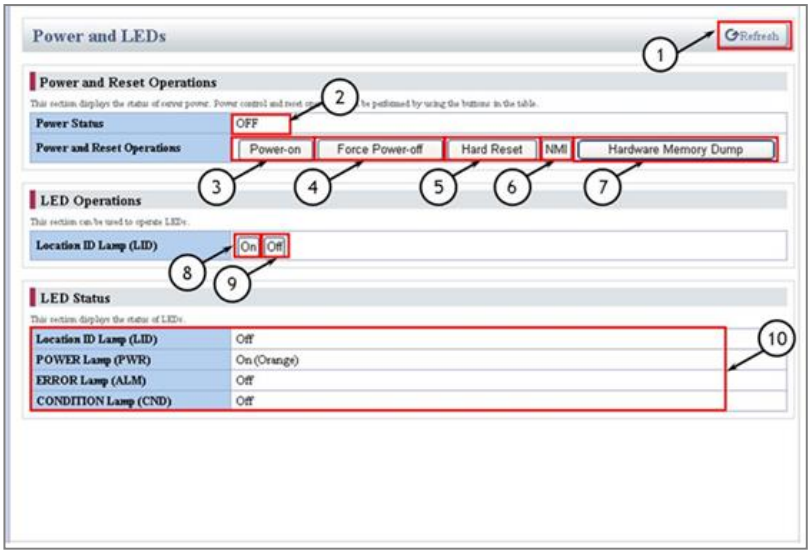


#	Item	Description
1	Refresh	Reloads the information.
2	Basic Information	Server Name shows the server blade name set on the ”Asset Information”. BMC IP Address shows the BMC IP address of the server blade. For BMC IP address settings, see ‘LC Command’ in Chapter 6. BMC MAC Address shows the BMC MAC address. UUID (Universal Unique ID) shows the UUID of the server blade. BMC Firmware Version shows the BMC firmware version. EFI Firmware Version shows the EFI firmware version.
3	Server Field Replaceable Unit (FRU) Information	Shows the product information of the server blade. Product Name shows the product name of the server blade. Product Part/Module Number shows the product part number of the server blade. Product Version shows the hardware version of the server blade. Product Serial Number shows the serial number of the server blade.

#	Item	Description
4	Chassis Information	Slot Number shows the slot number of the slot where the server blade is inserted. Chassis ID shows the chassis ID set in the management module.

❑ Power and LEDs

This screen shows the power and LED status of a server blade. You can control the power state and reset the server blade on this screen.



#	Item	Description
1	Refresh	Reloads the information.
2	Power Status	Shows the current power state of the server blade. OFF: The power of the server blade is off. ON: The power of the server blade is on. OFF (Power-on is disabled): The power cannot be turned on due to a power failure.
3	Power-on	Turns on the power of the server blade.
4	Force Power-off	Turns off the power of the server blade without OS shutdown. You can do a shutdown on the OS screen or use the SC function to turn off the power.
5	Hard Reset	Hardware resets the server blade. Enabled when the server blade power is on.
6	NMI	Sets the operation mode of the memory system. Independent Channel Mode (default) Mirrored Channel Mode Lockstep Channel Mode Spare Channel Mode Note: Do not use Lockstep Channel Mode because it is not supported. Note: If Xeon 5500 is installed on the server

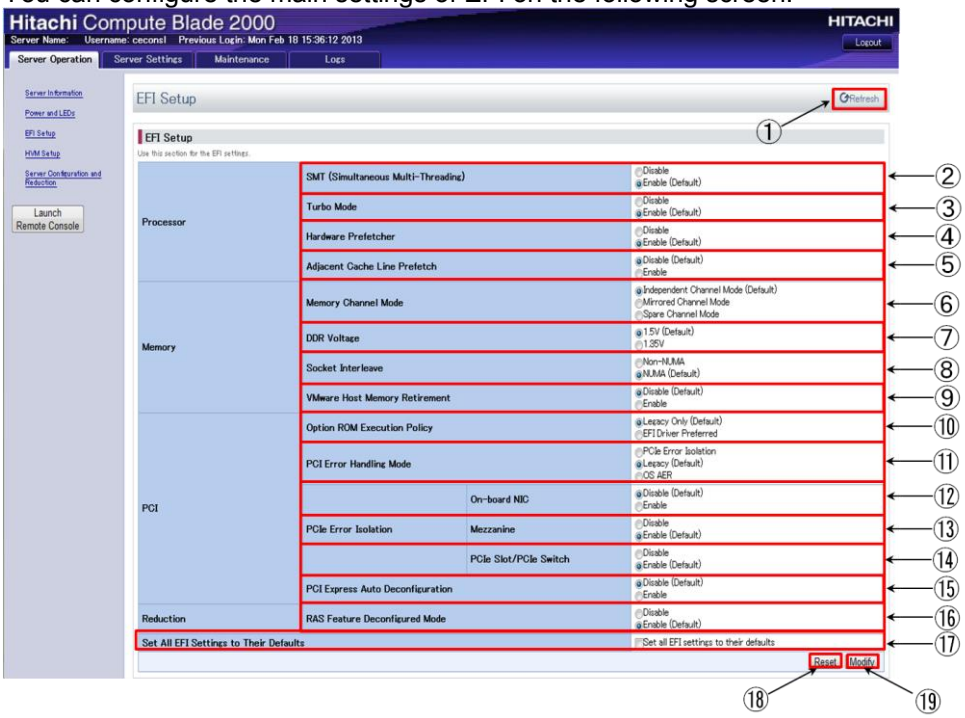
#	Item	Description
		blade, Spare Channel Mode cannot be used.
7	Hardware Memory Dump	Performs hardware memory dump of the server blade.
8	LID On	Turns on LID (Location ID Lamp).
9	LID Off	Turns off LID (Location ID Lamp).
10	LED Status	Shows the state of the LEDs on the front panel of the server blade. Location ID Lamp (LID) POWER Lamp (PWR) Alarm Lamp (ALM) Condition Lamp (CND) For the color and description of each LED, see “Standard Server Blade (X55A1/X55A2)” in Chapter 2.



- In the following cases, power-on requests are ignored and the server blade is not powered on.
  (1) Power-on is disabled due to failure in the server blade.
  (2) The number of power supply modules installed is not enough for the installed server blades.
- To prevent the EFI firmware storage from being corrupted, power-off requests issued during EFI firmware update are ignored and the server blade is not powered off. The EFI firmware update process is executed during the first EFI boot after the EFI firmware image is uploaded to the server blade.

❑ EFI setup

You can configure the main settings of EFI on the following screen.



#	Item	Description
1	Refresh	Reloads the information.
2	SMT (Simultaneous Multi-Threading)	Disables or enables the SMT function of Intel CPU. Disable / Enable (Default)
3	Turbo Mode	Disables or enables the Turbo mode of Intel CPU. Disable / Enable (Default)
4	Hardware Prefetcher	Disables or enables the Prefetch function of the memory controller in Intel CPU. Disable / Enable (Default)
5	Adjacent Cache Line Prefetch	Disables or enables the Adjacent Cache Line Prefetch function of the memory controller in Intel CPU. Disable (Default) / Enable
6	Memory Channel Mode	Sets the operation mode of the memory system. Independent Channel Mode (Default) Mirrored Channel Mode Lockstep Channel Mode Spare Channel Mode Note: Do not use Lockstep Channel Mode because it is not supported. Note: If Xeon 5500 is installed on the server blade, Spare Channel Mode cannot be used.
7	DDR Voltage (*1) DDR: double data rate	Sets the voltage for the memory system. 1.5 V (Default) 1.35 V

#	Item	Description
8	Socket Interleave (*2)	Sets the shared memory configuration of the memory system. Non-NUMA NUMA (NUMA: Non-Uniform Memory Access)
9	VMware Host Memory Retirement (*3)	Enables or Disables the error memory report function for VMware. Disable (Default) / Enable
10	Option ROM Execution Policy	Sets execution mode of the expansion ROM of the mezzanine cards and the PCI-Express boards. Legacy Only (Default): Use the code for the legacy BIOS. EFI Driver Preferred: Use the code for EFI.
11	Storage Option ROM Execution Policy (*5)	Sets execution mode of the Storage Option ROM (10*). Do not launch: Not executes. Unified extensible firmware interface (UFEI) only: Executes codes only for UEFI. Legacy Only (Default): Use the code for the legacy BIOS. Legacy first: Prioritize codes for the legacy BIOS to execute. UEFI first: Prioritize codes for UEFI to execute.
12	PXE Option ROM Execution Policy (*5)	Sets execution mode of the storage option ROM (*9). Do not launch: Not executes. UFEI only: Executes codes only for UEFI. Legacy Only (Default): Use the code for the legacy BIOS. Legacy first: Prioritize codes for the legacy BIOS to execute. UEFI first: Prioritize codes for UEFI to execute.
13	PXE LAN1 Option ROM Scan (*5) PXE LAN2 Option ROM Scan (*5)	Sets Option ROM for Network Interface Card (NIC) on port (*9). Disable (Default): Not executes Option ROM. Enable: Executes Options ROM.
14	Network Stack (*5)	Enables or Disables UEFI Network Stack (*10). Disable (Default) or Enable
15	IPv4 PXE Support (*5) IPv6 PXE Support (*5)	Enables or Disables IPv4 and IPv6 Preboot eXecution Environment (PXE) (*10). Disable (Default) / Enable (Default)
16	Other PCI Device ROM Priority (*5)	Sets execution mode of the IO expansion card and expansion ROM on PCI-Express board (*8). Legacy Option ROM (Default): Prioritize the code for legacy BIOS. UEFI Option ROM: Prioritize the code for UEFI.
17	PCI Error Handling Mode	Sets EFI error handling when PCI Express

#	Item	Description
	(*6)	(PCIe) is in failure: PCIe Error Isolation: EFI isolates a failed PCI Express. Legacy (Default): EFI does not isolate a failed PCI Express. OS AER: OS performs Advanced Error Reporting (AER). Available only for OS that support AER.
18	PCI Error Isolation - On-board NIC (*7)	Disables or enables PCI Express Error Isolation for the on-board NIC. Disable (Default) / Enable This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
19	PCI Error Isolation - Mezzanine (*7)	Disables or enables PCI Express Error Isolation for mezzanine cards. Disable / Enable (Default) This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
20	PCI Error Isolation - PCIe Slot/PCIe Switch (*7)	Disables or enables PCI Express Error Isolation for PCIe slots and PCIe switches. Disable / Enable (Default) This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
21	PCI Express Auto Deconfiguration	Disables or enables PCI Express Auto deconfiguration. You cannot change this value due to non-support for the item.
22	Reliability availability serviceability (RAS) Feature Deconfigured Mode	Disables or enables the processor and memory deconfiguration (or reduction) that is executed when a component fails. Disable / Enable (Default)
23	Set All EFI Settings to their Defaults	Restores the EFI Default settings. All the EFI settings, including the settings #2 to #14 are set to the Default.
24	Reset	Cancels the edited settings.
25	Modify	Validates the edited settings and moves to the confirmation screen.

(*1) This item is available only for standard server blade X55R3/X55S3/X55R4 models. With LR dual inline memory module (DIMM) installed, the value is fixed at 1.35 V. This item is not yet supported.

(*2) Default value for server blade X55A1/X55A2 models: Non-NUMA
Default value for server blade X55R3/X55S3 models: *NUMA*

*(*3)* This item is available only with the following configuration.

X55R3/X55S3 models:

BMC firmware version 05-53 or later, or 07-01 or later
EFI firmware version 09-53/10-53 or later

X55R4 model

BMC firmware version 07-01 or later
EFI firmware version 11-01/12-01 or later

Select Independent Channel Mode for Memory Channel Mode when using this item.

(*4) This item is available only with X55R3/X55S3 models.

(*5) This item is available with X55R4.

(*6) If the BMC firmware version is 03-77 or earlier, the default value of this item is PCIe Error Isolation. If the BMC firmware version is 03-78 or later, the default value is Legacy.

(*7) To use these settings on the server blade X55A1/X55A2 model, BMC firmware version 03-77 or later must be installed in the server blade.

(*8) The UEFI boot can be set only when Windows Server 2012 or later is booted from the Hitachi 8 Gb fibre channel (PCI card/expansion card) or Hitachi 16 Gb fibre channel (PCI card). For Hitachi 16 Gb fibre channel, firmware version 11-40/12-40 or higher is required.

Setting item	UEFI boot	Legacy boot
Other PCI Device ROM Priority	UEFI Option ROM	Legacy Option ROM

For other boot devices and OSs than those shown in (*8), use the default value.

(*9) Set the following only for PXE boot.

Setting item	UEFI boot	Legacy boot
PXE Option ROM Execution Policy	UEFI only	Legacy only.
PXE LAN1 Option ROM Scan PXE LAN2 Option ROM Scan	Enable the LAN you use.	Enable the LAN you use.
Network Stack	Enable	Only for UEFI boot: Set the default value in Legacy boot.
IPv4 PXE Support IPv6 PXE Support	Set to Enable depending on your LAN environment.	Only for UEFI boot: Set the default value in Legacy boot.

See Selecting PXE booting for details.
For UEFI boot with PXE boot, firmware version 11-40/12-40 or higher is required

(*10) Use the default value.



The edited EFI settings will be enabled on the next power on or reset.

- When you use the remote FD or remote CD/DVD as a boot path, start Remote Console Application and start the remote FD or remote CD/DVD before you power on the server blade.
- You can display/hide the toolbar of Remote Console Application (Reclient) by pressing Alt+G keys.
- For details about Remote Console Application, see the *Remote Console Application User's Guide Hitachi Compute Blade 2000* in the CD attached to this equipment.

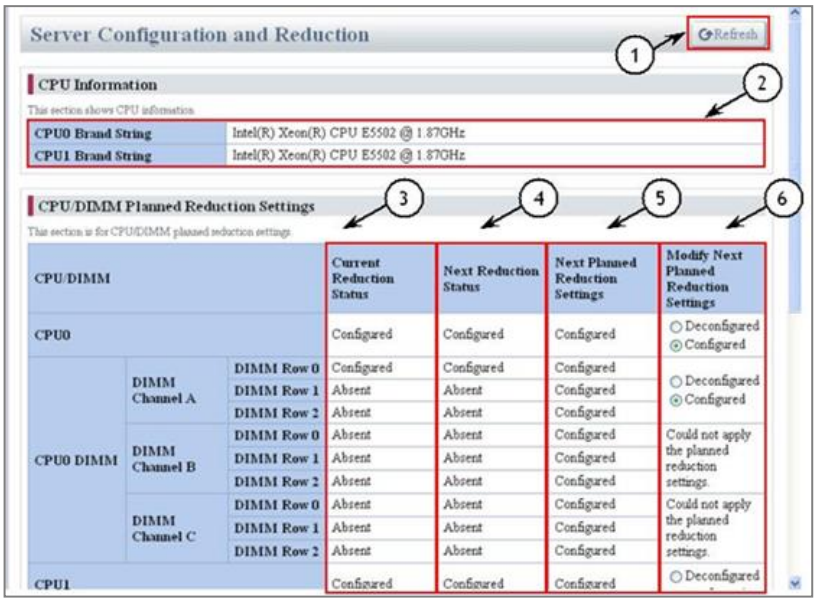
❑ LP setup

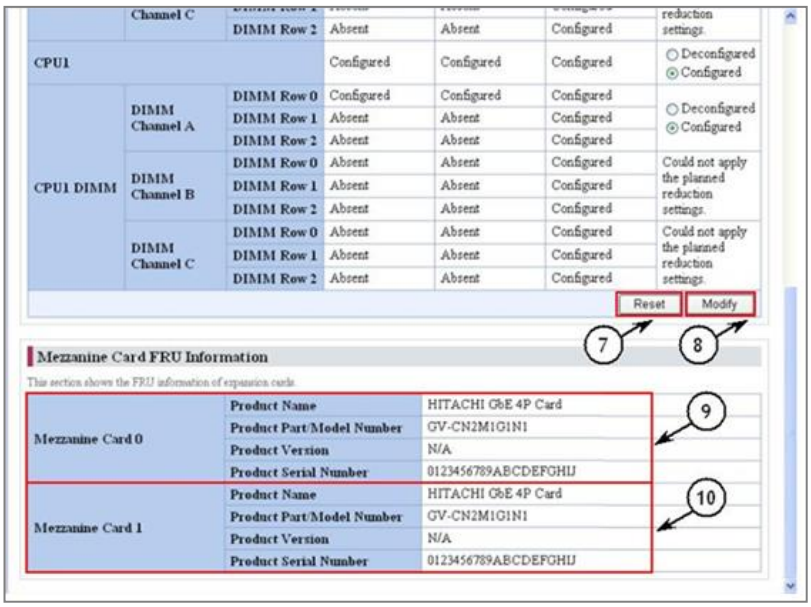
You can enable and disable the LPAR manager boot and set the LPAR manager firmware to be used for the LPAR MANAGER boot on this screen. See LPAR manager boot settings in “Initial Settings with Server Blade Web Console”.

❑ Server Configuration and Reduction

This screen displays information of the CPUs and mezzanine cards installed in the server blade, and also displays the reduction information on the CPUs and DIMMs.

Reduction information includes whether components are deconfigured due to a failure. You can also set up the planned reduction for the CPUs and DIMMs on this screen.





#	Item	Description
1	Refresh	Reloads the information.
2	CPU Information: CPU0 Brand String CPU1 Brand String	Shows the types of CPUs: information on the last EFI boot.
3	Current Reduction Status	Shows the current reduction status of CPU/DIMM. Configured: not deconfigured. Deconfigured: deconfigured as planned. Absent: not installed. Failed: deconfigured due to failure. Not Available: deconfigured due to failure of other CPU or DIMM.
4	Next Reduction Status	Shows the CPU/DIMM reduction status to be applied at the next power on or reset.
5	Next Planned Reduction Settings	Shows the planned CPU/DIMM reduction settings to be applied at the next power on or reset. Deconfigured: CPU/DIMM will be deconfigured. Configured: CPU/DIMM will not be deconfigured.
6	Modify Next Planned Reduction Settings	Changes the planned CPU/DIMM reduction settings to be applied at the next power on or reset. Deconfigured: CPU/DIMM will be deconfigured. Configured: CPU/DIMM will not be deconfigured.
7	Reset	Cancels the edited settings.
8	Modify	Validates the edited settings and moves to the confirmation screen.
9	Mezzanine Card FRU Information: Mezzanine Card 0	Shows the Field-Replaceable Unit (FRU) information of mezzanine card 0.
10	Mezzanine Card FRU Information: Mezzanine Card 1	Shows the FRU information of mezzanine card 1.



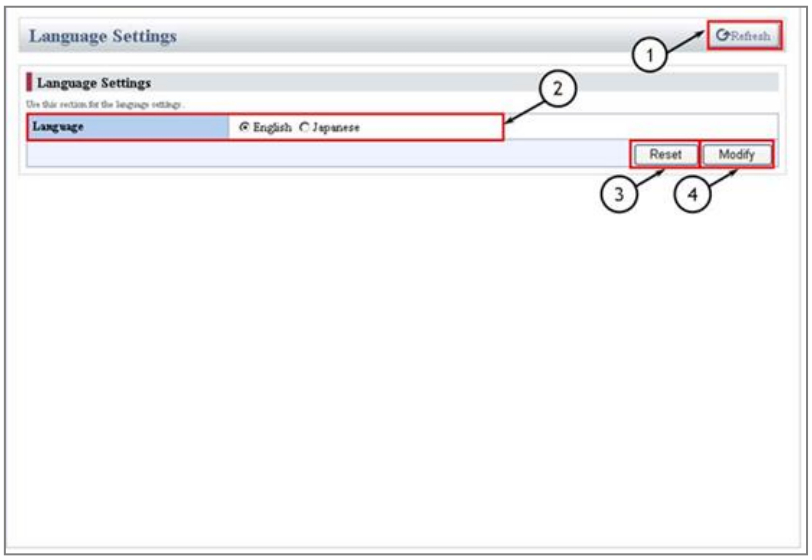
- You cannot deconfigure the CPU or DIMM below the minimum configuration.
- Only maintenance personnel can use **Modify**.

Server Settings tab

You can use the Server Settings tab to configure the functions to manage the server blade.

❑ Language settings

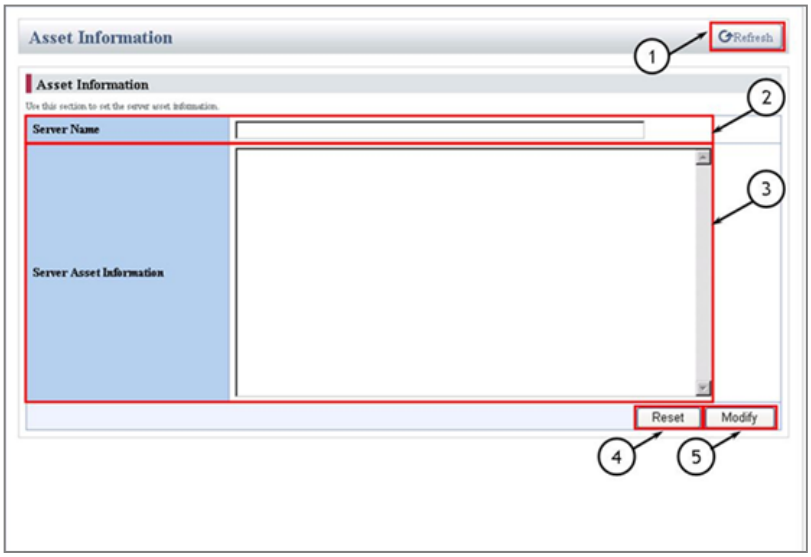
You can set the language used on the server blade web console on the following screen.



#	Item	Description
1	Refresh	Reloads the information.
2	Language	English: Sets English as the displayed language on the server blade Web console. Japanese: Set Japanese as the displayed language on the server blade Web console.
3	Reset	Cancels the edited settings.
4	Modify	Validates the edited settings and moves to the confirmation screen.

❑ Asset information

You can set the asset information on the server blade on this screen.

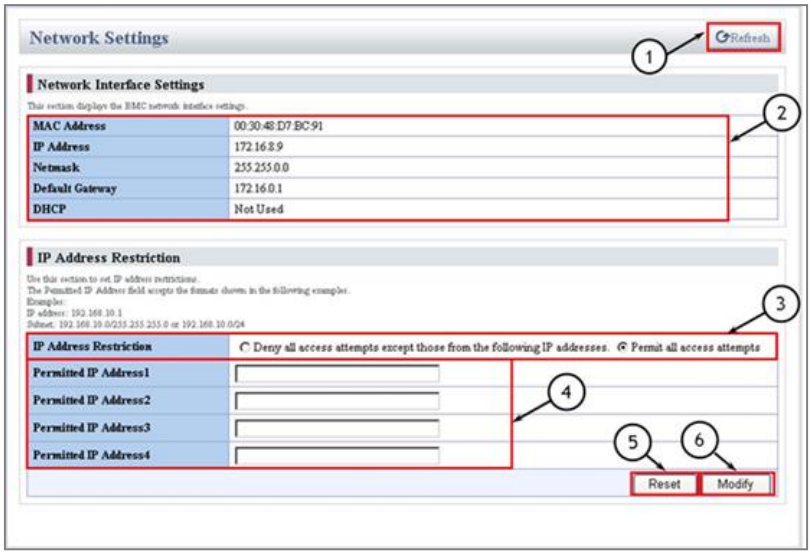


#	Item	Description
1	Refresh	Reloads the information.
2	Server Name	Sets the server blade name. The server name is shown in the Server name field at the left top of the screen and Server Information screen in the Server Operation tab.
3	Server Asset Information	A comment can be registered. This field can be used to record information such as the installed location and administrator of the server blade.
4	Reset	Cancels the edited settings.
5	Modify	Validates the edited settings and moves to the confirmation screen.

❑ Network settings

This screen shows the management network settings of the server blade.

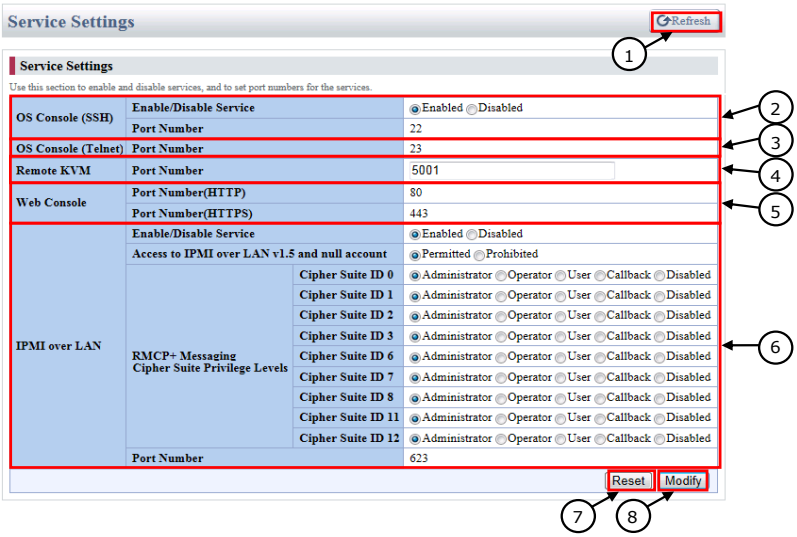
You can set restrictions on the IP address of the network device that can be connected to the server blade. You can specify up to four IP addresses to allow connection to the server blade.



#	Item	Description
1	Refresh	Reloads the information.
2	MAC Address IP Address Netmask Default Gateway DHCP	Shows the network settings of the server blade. To set or modify the IP address and netmask, use the LC Command of the management module. For DNS setting, see the DNS Client screen. DHCP: Dynamic Host Configuration Protocol
3	IP address Restriction	Enable or disable the restriction on the IP addresses.
4	Permitted IP Address 1-4	Enter IP addresses that you allow connection to the server blade. You can set a single IP address or subnet in each field. Ex. Single IP address: 192.168.10.1 Subnet: 192.168.10.0/255.255.255.0 or 192.168.10.0/24
5	Reset	Cancels the edited settings.
6	Modify	Validates the edited settings and moves to the confirmation screen.

❑ Service settings

You can enable or disable the services provided by the server blade and set the port numbers to be used by the services on this screen.



#	Item	Description
1	Refresh	Reloads the information.
2	OS Console (SSH)	Enables or disables the OS console via SSH. Shows the port number used by the OS console via SSH.
3	OS Console (Telnet)	Shows the port number used by the OS console via Telnet.
4	Remote KVM	Sets the port number used by the remote console application to connect to the server blade.
5	Web Console	Shows the HTTP port and HTTPS port used by the server blade Web console.
6	IPMI over LAN	Enables/disables IPMI over LAN; permits or not access over LAN v1.5 and null account; selects suite privilege levels.* Shows the port number used by the IPMI Over LAN.
7	WS-MAN (*1)	Enables or disables WS-MAN (Web Service Management). Sets a port number for connecting to WS-MAN.
8	Reset	Cancels the edited settings.
9	Modify	Validates the edited settings and moves to the confirmation screen.

Note:

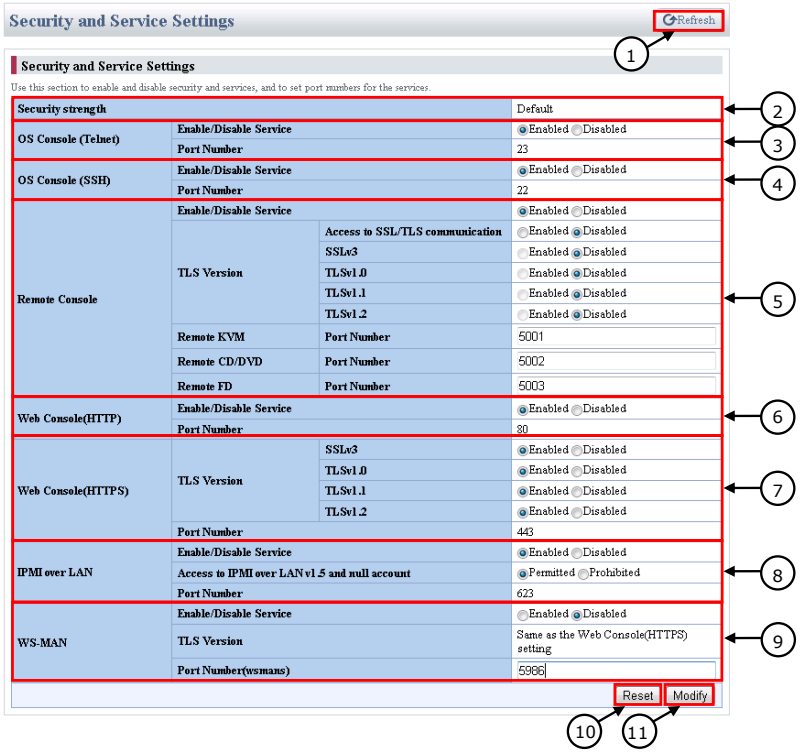
* This menu is available for the following BMC version or later.
BMC: 03-95 with X55A1/X5A2 model.

Tip

- To power on or off a server blade from SC/Blade Server Manager, register the server chassis as a target on SC/Blade Server Manager before setting IPMI over the LAN.

❑ Security and Service Settings

You can enable or disable security and services provided by server blades and set port numbers for the services.



#	Item	Description
1	Refresh	Reloads the information.
2	Security strength	Shows the security strength set on the server blade. See Chapter 13, Security Strength for details.
3	OS Console (Telnet)	Enables/disables access to the OS console via Telnet. Shows the port number used by the OS console via Telnet.
4	OS Console (SSH)	Enables/disables access to the OS console via SSH. Shows the port number used by the OS console via SSH.
5	Remote Console	Enables/disables remote console functions. Sets a connection method, TLS version, and port number used by the remote console application to connect to the server blade.
6	Web Console (HTTP)	Enables/disables access to the Web console via HyperText Transfer Protocol (HTTP). Shows the HTTP port used by the server blade Web console.
7	Web Console (HTTPS)	Enables/disables access to the Web console via

#	Item	Description
		HTTPS; selects TLS version used for HTTPS connection. Shows the HTTP port and HTTPS port used by the server blade Web console.
8	IPMI over LAN	Enables/disables IPMI over LAN; permits or not access over LAN v1.5 and null account; selects suite privilege levels.* Shows the port number used by the IPMI Over LAN.
9	WS-MAN	Enables or disables WS-MAN (Web Service Management). Sets a port number for connecting to WS-MAN.
10	Reset	Cancels the edited settings.
11	Modify	Validates the edited settings and moves to the confirmation screen.



- To power on or off a server blade from SC/Blade Server Manager, register the server chassis as a target on SC/Blade Server Manager before setting IPMI over LAN.

❑ User accounts

See User account configuration in “Initial Settings with Server Blade Web Console”.

❑ BMC time

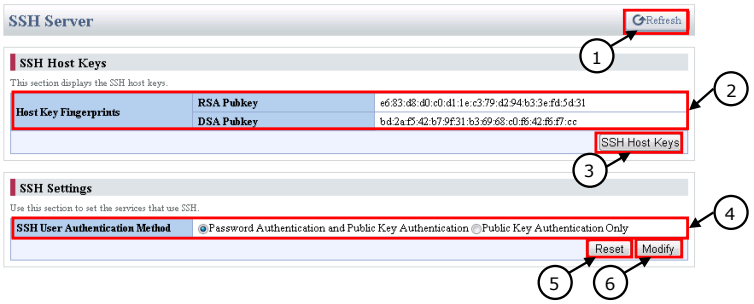
See BMC time settings in “Initial Settings with Server Blade Web Console”.

❑ Remote KVM

See Mouse mode settings for the remote console in “Initial Settings with Server Blade Web Console”.

❑ SSH Server

You can set the authentication method of SSH and check the fingerprint of the host keys on this screen.



#	Item	Description
1	Refresh	Reloads the information.
2	Host Key Fingerprints	Displays the fingerprint of host public keys that are used in the server blade SSH server.
3	SSH Host Keys *	Updates SSH host keys.
4	SSH User Authentication Method	Selects the authentication method that is used in the server blade SSH server.
5	Reset	Cancels the edited settings.
6	Modify	Validates the edited settings and moves to the confirmation screen.

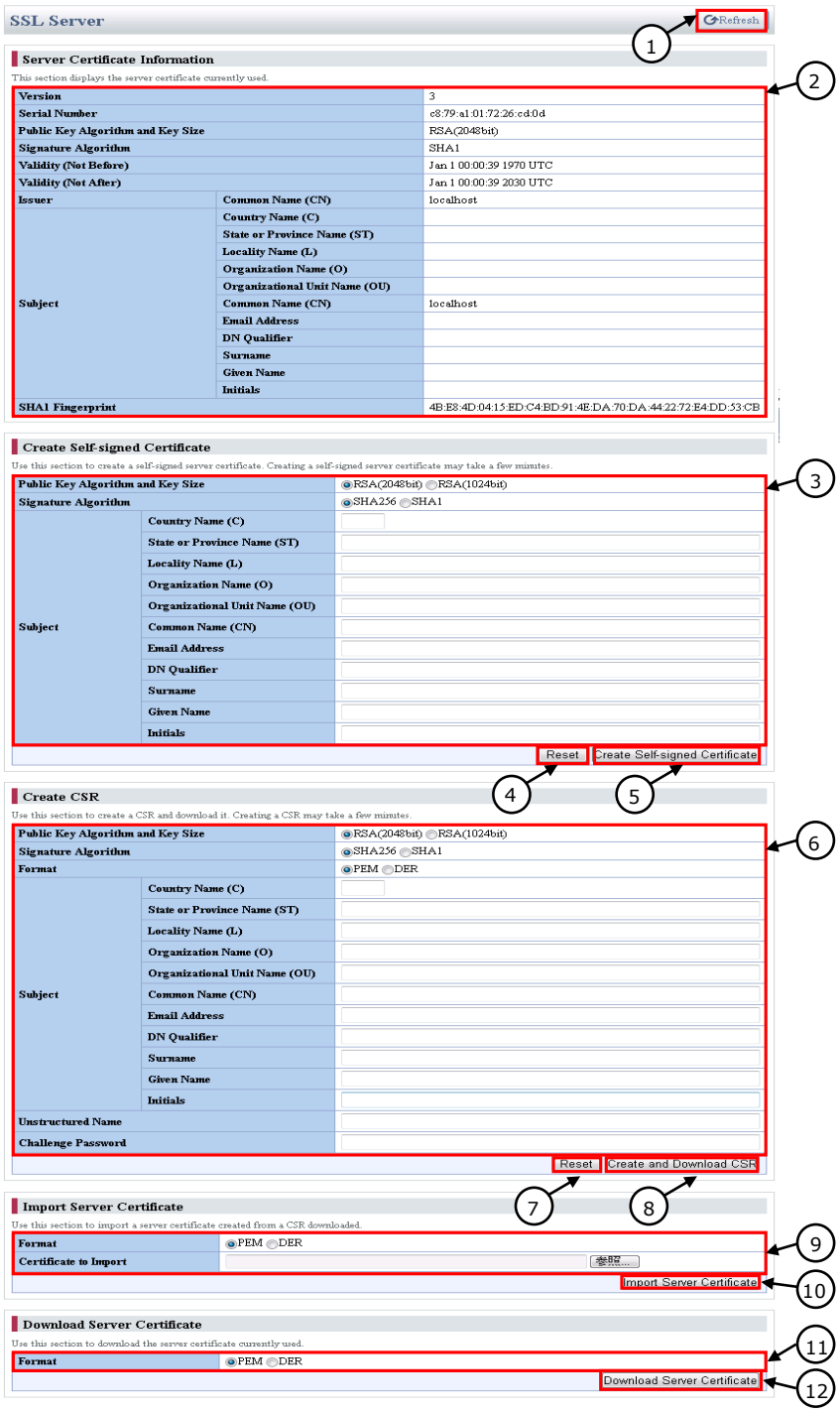
(*) This button is available with the following BMC firmware or later.

BMC: 07-01 on standard server blade: X55R3/X55S3/X55R4 model

BMC: 06-01 on high-performance server blade: X57A2 model

❑ SSL Server

You can set up the SSL server certificate on this screen. You can display the information of the server certificate used by the server blade, create a self-signed server certificate, create a certificate signing request (CSR), import a server certificate, and download the server certificate.

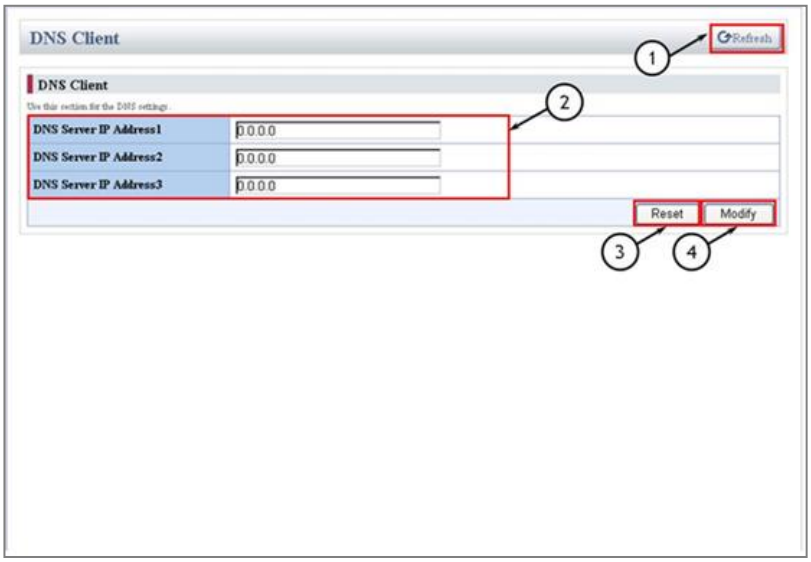


#	Item	Description
1	Refresh	Reloads the information
2	Server Certificate Information	Displays the information of the server certificate used by the server blade. The following information is displayed: Version Serial Number Public Key Algorithm and Key Size Validity (Not Before) Validity (Not After) Issuer (Only Common Name (CN) is displayed.) Subject SHA1 Fingerprint
3	Create Self-signed Certificate	Specifies the information for creating a self-signed server certificate. Public key algorithm, key size, signature algorithm, and the following information can be specified. Country Name (C): A string of 2 upper case letters can be specified. State or Province Name (ST), Locality Name (L), Organization Name (O), Organization Unit Name (OU) : A string of up to 60 characters can be specified. Common Name (CN): A string of up to 60 characters can be specified. Alphanumeric characters, “-“, and “.” can be used. Email Address: A string of up to 60 ASCII characters can be specified. DN Qualifier, Surname, Given Name: A string of up to 60 characters can be specified. Initials: A string of up to 30 characters can be specified. Common Name (CN) must be specified. Other items can be omitted. The characters that can be used in State or Province Name (ST), Locality Name (L), Organization Name (O), Organization Unit Name (OU), DN Qualifier, Surname, Given Name and Initials are as follows: Alphanumeric characters, White space, “’”, “-“, “,”, “=”, “/”, “(“, “)”, “.”, “:”, “+”, “?”
4	Reset	Cancels the edited settings in #3.
5	Create Self-signed Certificate	Creates a self-signed certificate using the information specified in #3. When the button is pressed, the confirmation screen is displayed.
6	Create CSR	Specifies the information for creating a self-signed server certificate. In addition to the items in #3, the following information can be specified. Format: Specifies the format of the certificate signing request (CSR) to download. “privacy enhanced mail (PEM)” or “Distinguished Encoding Rules (DER)” can be specified. Unstructured Name: A string of up to 60 characters can be specified. Challenge Password: A string of up to 30 characters can be specified.

#	Item	Description
		Unstructured Name and Challenge Password can be omitted. The characters that can be used in those items are the same as specified in #3.
7	Reset	Cancels the edited settings in #6.
8	Create and Download CSR	Creates a CSR using the information specified in #6. When the button is pressed, the confirmation screen is displayed.
9	Import Server Certificate	Specifies the server certificate to import to the server blade. Format: Specifies the format of the server certificate to import. "PEM" or "DER" can be specified. Certificate to import: Specifies the file of the server certificate.
10	Import Server Certificate	Imports the server certificate specified in #9 to the server blade. When the button is pressed, the confirmation screen is displayed.
11	Download Server Certificate	Specifies the format of the server certificate to download. "PEM" or "DER" can be specified.
12	Download Server Certificate	Downloads the server certificate registered to the server blade in the format specified in #11.

❑ DNS Client

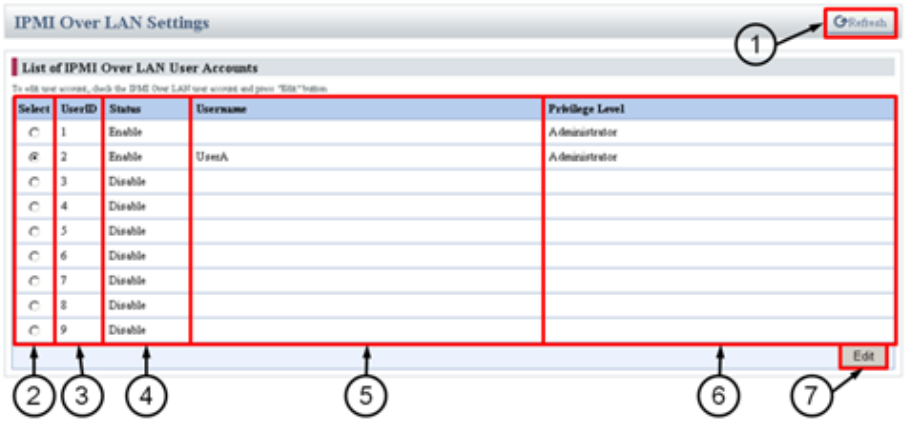
You can set the IP addresses of DNS servers on the following screen to have the server blade do name resolution using DNS. Up to 3 IP addresses can be specified.



#	Item	Description
1	Refresh	Reloads the information.
2	DNS Server IP Address 1-3	Sets the IP addresses of DNS servers. Up to 3 IP addresses can be specified. The IP address on the top of the screen is used first, then one in the middle, and the bottom one the last. If you do not use the second and/or third DNS servers, enter `0.0.0.0` to those fields. If you do not use DNS, set `0.0.0.0` to all the fields.
3	Reset	Cancels the edited settings.
4	Modify	Validates the edited settings and moves to the confirmation screen.

❑ IPMI Over LAN

You can set IPMI Over LAN to user accounts.

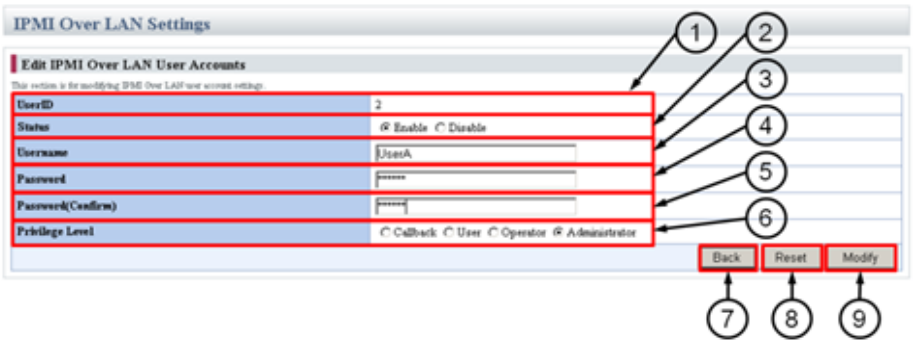


#	Item	Description
1	Refresh	Reloads the user account information.
2	Select	Selects user accounts.
3	User ID	ID for the user account
4	Status	Shows Enable or Disable the user account.
5	User name	User account name
6	Privilege Level	A privilege level given to the user account
7	Edit	Goes to the Edit IPMI Over LAN User Account screen, but does not go there without the option button checked,

Tip

- For User ID1, you can change only Status: Enable or Disable.
- User ID1 is set by default at the factory as follows:
  Status: Enable, User name: (blank); Password: (blank); Privilege Level: Administrator.
- When you turn a server blade on or off from ServerConductor/Blade Server Manager, add the server chassis to management targets for Server/Conductor/Blade Server Manager before changing settings for IPMI user ID 1.

When you click **Edit**, the Edit IPMI Over LAN User Account screen appears.



#	Item	Description
1	User ID	ID for the user account
2	Status	Shows Enable or Disable the user account.
3	User name*1	User account name consists of up to 16 alphanumerics.
4	Password*1*2	Type a password consisting of up to 16 alphanumerics.
5	Password (Confirm) *1*2	Retype the password.
6	Privilege Level*1	Set a privilege level.
7	Back	Returns to the List of IPMI Over LAN User Accounts screen without saving edits.
8	Reset	Returns settings to the previous state without saving edits.
9	Modify	Saves the edits and goes to the confirmation screen.

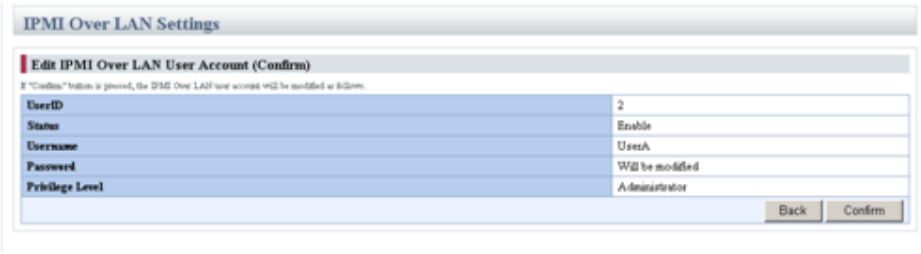
*1: User ID1 cannot be changed.

*2: You can set a password depending on the BMC firmware versions as follows.

BMC: 04-71 or later, or 05-18 or later: 16-byte password compatible with IPMI 1.5

BMC: 03-95 or later, 07-01 or later, or 06-20 or later: 20-byte password compatible with IPMI 2.0

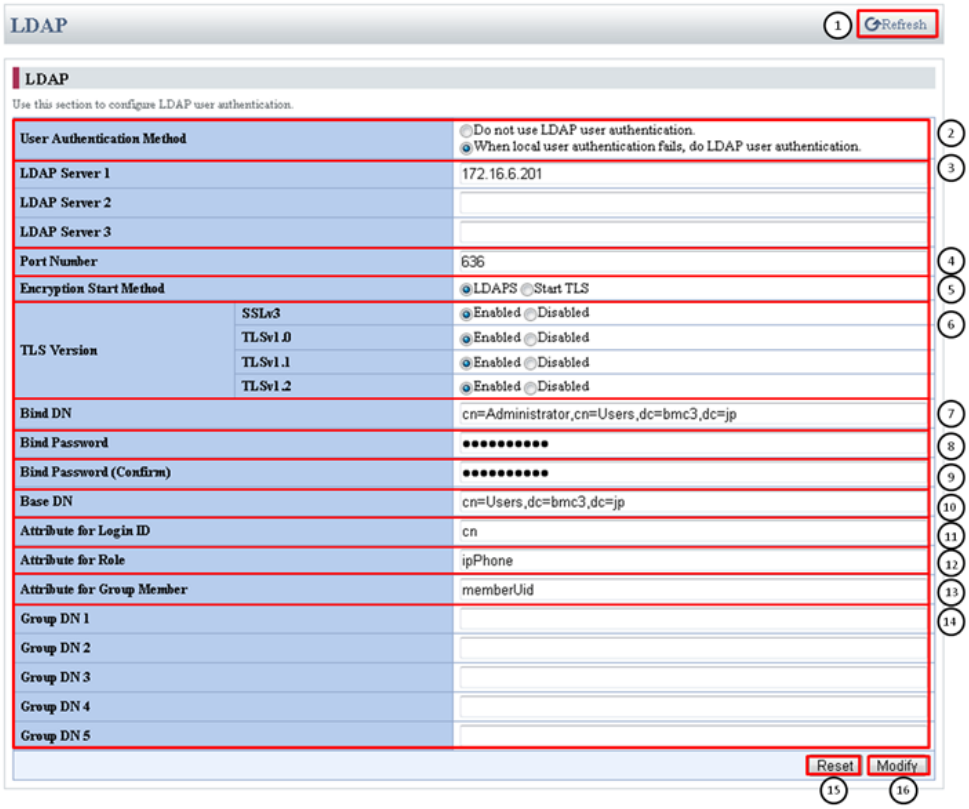
When you click **Modify** on the Edit IPMI Over LAN User Account screen, the following screen appears.



When clicking **Back**, you return to the Edit IPMI Over LAN User Account screen without saving the edits. When clicking **Confirm**, you return to the List of IPMI Over LAN User Accounts screen while saving the edits.

❑ LDAP

You can set user authentication with the LDAP. See “LDAP Server Linkage” in Chapter 13 for more information.



#	Item	Description
1	Refresh	Reloads the information.
2	User Authentication Method	Specifies a user authentication method. Do not use LDAP user authentication: Authenticates a user with user accounts registered in the server blade. When local user authentication fails, perform LDAP user authentication: Authenticates a user with user accounts registered in the server blade. If it fails, then authenticate the user with user accounts on the LDAP server.
3	LDAP 1-3	Specifies an LDAP with IP address (XXX.XXX.XXX.XXX) or FQDN: up to 255 characters.
4	Port Number	Specifies a destination port number with decimal numbers: 1 to 65535.
5	Encryption Start Method (*1)	Specifies a method to connect to the LDAP server. Generally, LDAP connection uses port 636, and Start TLS connection uses port 389. However, you may have to use another port depending on the environment. Check your environment and then set the port.

#	Item	Description
6	TLS Version(*2)	Enables a TLS version for connection to the LDAP server.
7	Bind DN	Specifies a DN used for binding to the LDAP server: up to 256 characters. If nothing is typed in this field, anonymous bind is used.
8	Bind Password	Specifies a password used for binding to the LDAP server: up to 32 characters. When nothing typed in this field, the password is none.
9	Bind Password (Confirm)	Type the password again for confirmation.
10	Base DN	Specifies a DN of the base entry for searching a user: up to 256 characters.
11	Attribute for Login ID	Specifies an attribute among attributes in user entry to use as Login ID: up to 64 characters.
12	Attribute for Role	Specifies an attribute containing a character string to show a role among attributes in user entry: up to 64 characters.
13	Attribute for Group Member	Specifies an attribute to show a member among attributes in group entry: up to 64 characters.
14	Group DN1-DN5	Specifies DNs of groups allowed to login: up to 256 characters. If nothing is typed in all fields, no group authentication is performed.
15	Reset	Cancels the edited settings.
16	Modify	Validates the edited settings and moves to the confirmation screen.

(*1) This item is available with the following BMC firmware versions or higher.

BMC: 07-07 on standard server blade: X55R3/X55S3/X55R4 model

BMC: 06-22 on standard server blade: X57A2 model

(*2) This item is available with the following BMC firmware versions or later.

BMC: 07-01 on standard server blade: X55R3/X55S3/X55R4 model

BMC: 06-01 on high-performance server blade: X57A2 model

❑ Syslog Transfer

You can set Syslog transfer on the following screen. See “Syslog Transfer” in Chapter 13 for details about the features.



#	Item	Description
1	Enable/Disable Syslog transfer	Enables or disables Syslog transfer.
2	Syslog Server	Specifies a syslog server using IP address in XXX.XXX.XXX.XXX, or FQDN using up to 127 characters.
3	Port Number	Shows the port number for syslog transfer destination.
4	[Reset] button	Disables the edit and returns to the state before editing.
5	[Modify] button	Enables the edit and goes to the confirmation screen.
6	[Send] button	Issues a test syslog for confirmation.

This function is available with the following BMC firmware versions or later.

BMC: 07-07 on standard server blade: X55R3/X55S3/X55R4 model

BMC: 06-22 on high-performance server blade: X57A2 model

Maintenance tab

Using the Maintenance tab, you can update the firmware, backup and restore the data managed on the firmware, and restart BMC.

❑ EFI Firmware Management

Only maintenance personnel can use this menu.

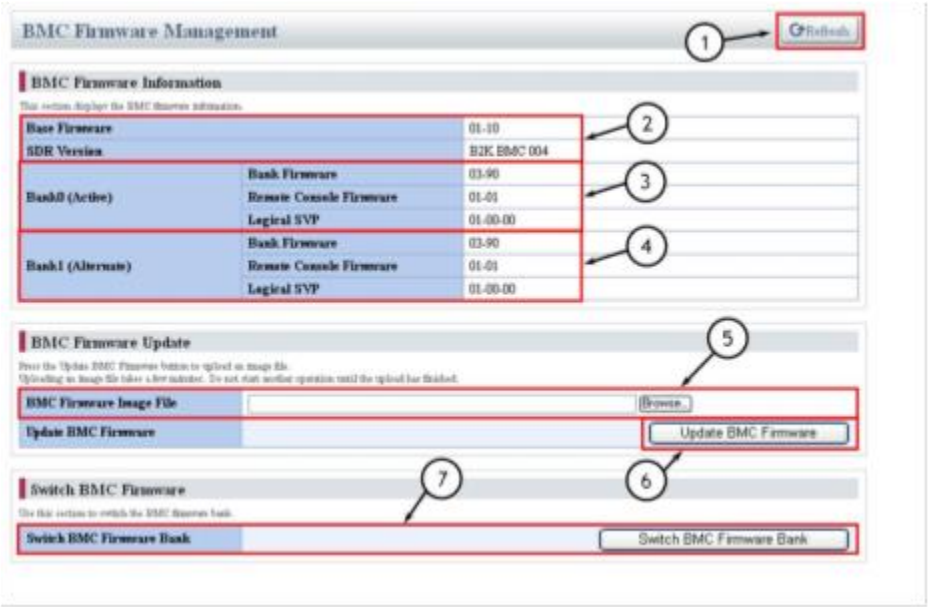
❑ BMC Firmware Management

You can update and switch BMC firmware on this screen.

The server blade has two banks (Bank0 and Bank1) of storage area for the BMC firmware. If one BMC firmware fails, you can boot BMC using the other bank.

You can update the BMC firmware on this screen. BMC firmware is updated by writing a new BMC firmware image to a bank (Alternate), which is not currently used, then switching banks, and restarting BMC.

You can also switch banks on this screen without updating the BMC firmware.



#	Item	Description
1	Refresh	Reloads the information.
2	Base Firmware SDR Version	Shows the information shared by Bank0 and Bank1. Base Firmware: shows the base firmware version SDR Version: shows the SDR version
3	Bank0	Shows the Bank0 information. Active: currently used. Alternate: currently not used. Bank Firmware: the firmware version written

#	Item	Description
		on this bank. Remote Console Firmware: the version of the remote console function. Logical SVP: the version of the logical SVP function.
4	Bank1	Shows the Bank1 information.
5	BMC Firmware Image File	Specifies the image file of BMC firmware to be uploaded.
6	Update BMC Firmware	Uploads the specified image file. It takes some minutes. When the uploading is complete, the confirmation screen is displayed.
7	Switch BMC Firmware Bank	Switches banks for use. When clicking Switch BMC Firmware Bank, the confirmation screen is displayed.



Only maintenance personnel can use **Update BMC Firmware** and **Switch BMC Firmware Bank**.

❑ Backup System Settings

Only maintenance personnel can use this menu.

❑ Restore System Settings

Only maintenance personnel can use this menu.

❑ Backup Server Management Settings

Only maintenance personnel can use this menu.

❑ Restore Server Management Settings

Only maintenance personnel can use this menu.

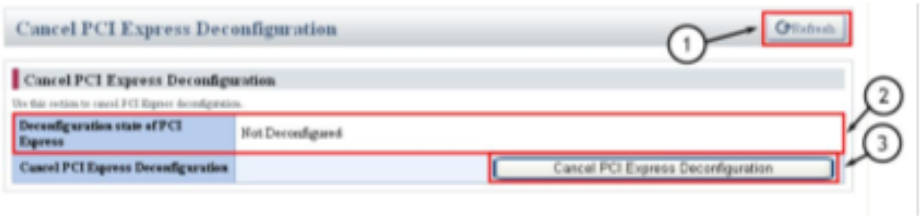
❑ Restart BMC

Only maintenance personnel can use this menu.

❑ Cancel PCI Express Deconfiguration

This screen shows the current deconfiguration state of PCI Express.

You can cancel PCI Express deconfiguration on this screen to make the deconfigured PCI Express devices enabled again.



#	Item	Description
1	Refresh	Reloads the information.
2	Deconfiguration state of PCI Express	Shows the current deconfiguration state of PCI Express. Not Deconfigured: In the server partition, no PCI Express device is deconfigured. Deconfigured: In the server partition, one or more PCI Express devices are deconfigured.
3	Cancel PCI Express Deconfiguration	Cancels PCI Express deconfiguration and makes the deconfigured PCI Express devices enabled again. When Cancel PCI Express Deconfiguration is pressed, the confirmation screen is displayed.

Tip

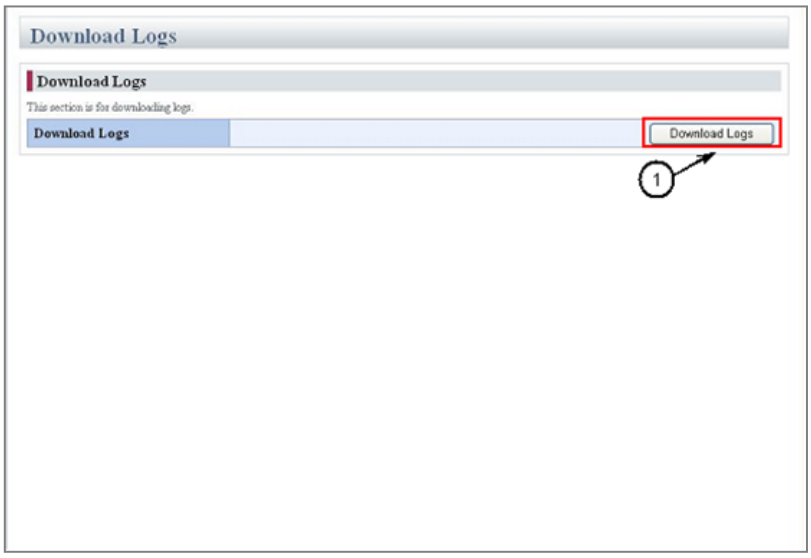
If PCI Express deconfiguration is canceled without carrying out required maintenance, a failure of PCI Express may be detected after next boot.

Logs tab

Using the Logs tab, you can download the logs collected by BMC, the blade management micro controller.

❑ Download Logs

You can download the log files corrected by the BMC on this screen.



#	Item	Description
1	Download Logs	Downloads the log files collected by BMC.

The log file contains the following logs.

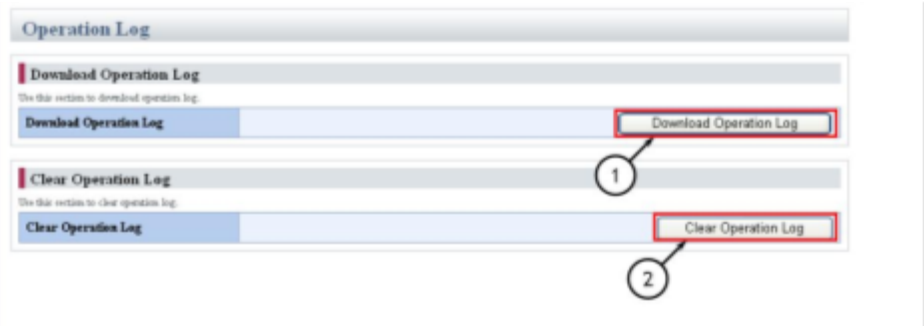
#	Item	Description
1	OS console log	Output of the serial console of the server blade. A log is collected when: 1 The server blade is powered off. 2 The server blade is reset. 3 BMC watchdog timer is expired. 4 The server blade Web console downloads logs. 64 kB of data is collected each time for conditions 1-3. Logs collected the last 5 times in above 1-3 will be stored in BMC and downloaded. In 4, only the latest log will be downloaded.
2	VFP (Virtual Front Panel) log	Logs collected by the VFP function The initialization codes are logged when the server blade is powered on.
3	Detailed log	Binary logs to analyze hardware failure.

Tip

- See “OS Console (Serial console redirection)” in Chapter 13 for information about the OS console.
- The OS console can be used by connecting to the BMC IP address of the server blade via Telnet or SSH.
- See “BMC Environment Setting Utility” – “Processing Failure” in the *Server Conductor/Blade Server Manager System Management Guide* for BMC WDT (Watch Dog Timer).

❑ Operation Log

You can download the operation logs and clear them on this screen.

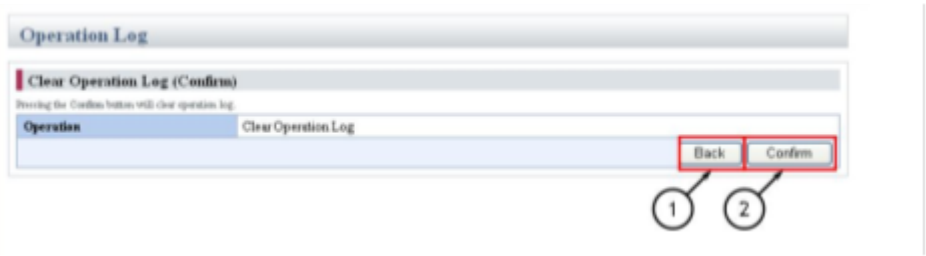


	Item	Description
1	Download Operation Log	Downloads the operation logs collected by BMC.
2	Clear Operation Log	Moves to the confirmation screen.

Note

When using the operation log with server blades X55A1/X55A2 model, you need to install BMC firmware 03-91 or later.

The confirmation screen is as follows.



	Item	Description
1	Back	Cancels the operation and returns to the previous screen.
2	Confirm	Clears the operation logs.

❑ VFP (Virtual Front Panel) Log Function

The VFP log function of a server blade captures the liquid crystal display (LCD) outputs of EFI and records them to the internal storage. The VFP function is used to store the initialization code at the power-on of a server blade.

The VFP log is recorded in the three-line format. The format includes Line1 (L1), Line2 (L2), and Line3 (L3), and each line consists of 40 characters.

#	Item	Description
1	Line1 (L1)	Records the time stamp at output.
2	Line2 (L2)	Records the EFI initialization code: power on self-test (POST) code.
3	Line3 (L3)	Records the front panel LED status for reference.

- VFP snapshot (file name: vfpSnapshot[0-3].log)

  When the blade is powered off or reset, a snapshot of VFP logs is copied to a log file. The latest four log files are stored in the server blade's internal storage.

```
# cd /var/hitachi
# ls
EFIDebug.log  EFITrace.log  vfp.log       vfpInfo.dat
# more vfp.log
L1:Aug 27 2020 11:28:44                 L2:EFI/BIOS:00 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:50                 L2:EFI/BIOS:E6 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:52                 L2:EFI/BIOS:47 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:55                 L2:EFI/BIOS:CC BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:56                 L2:EFI/BIOS:B0 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:57                 L2:EFI/BIOS:95 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:28:58                 L2:EFI/BIOS:6B BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:05                 L2:EFI/BIOS:6A BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:07                 L2:EFI/BIOS:69 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:10                 L2:EFI/BIOS:4D BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:14                 L2:EFI/BIOS:66 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:15                 L2:EFI/BIOS:67 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:17                 L2:EFI/BIOS:4B BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:18                 L2:EFI/BIOS:66 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:19                 L2:EFI/BIOS:4D BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:29:25                 L2:EFI/BIOS:52 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
L1:Aug 27 2020 11:33:03  01234          L2:EFI/BIOS:52 BMC:44                 L3:LID:off   PWR:on    ERR:off   CND:off
#
```

Example of VFP logs



Recovery procedure for server blade web console connection:

If you cannot connect to the server blade web console or the server blade web console does not respond for more than 1 minute when you click a menu item or a button, follow the recovery procedures described below.

Procedure1 (Check the network):

If there is failure in the network and the Transmission Checksum Protocol (TCP) connection between the web browser and the server blade does not operate normally, the web browser may not connect to the server blade web console, or the screens of the server blade web console may not be displayed in the web browser window.

Also, if the throughput of the network is low, it may take some time for the screens of the server blade web console to be displayed.

Check that there is no failure or problem in the network. If there is no problem or failure, continue to Procedure 2.

Procedure 2 (Restart the server blade BMC):

(1) Log in to the system console of the management module. See Chapter 6 for the usage of the system console for more information.

(2) Restart the server blade BMC using the following command on the system console:

`"PC command"-"P. Power control"-"R.Restart"`

See “PC command” in Chapter 6 for information about the PC command.

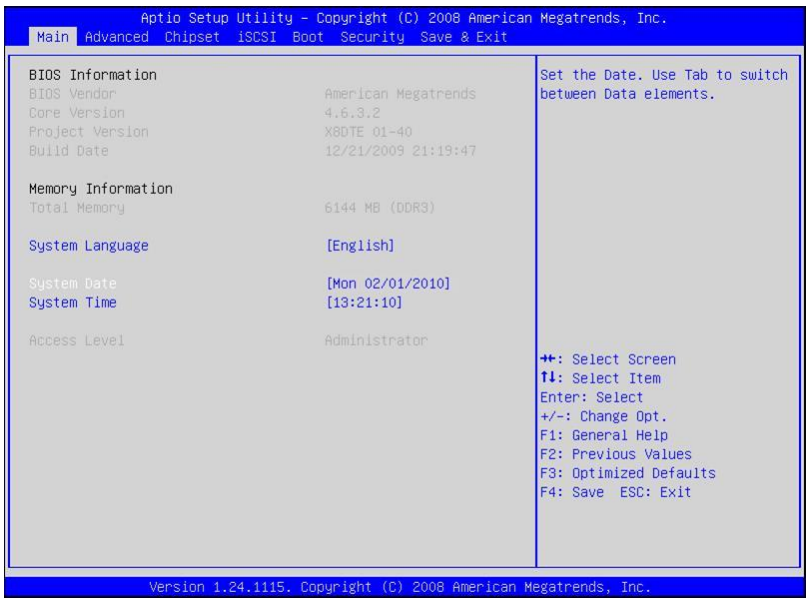
The BMC needs a few minutes to restart. Log in to the server blade web console after the BMC is restarted.

Standard server blade setup menu (X55A1/X55A2 models)

EFI Setup Screen

By entering the EFI Setup screen while the server blade is booting, you can halt the boot process and check or change the settings.

With the EFI startup screen open, press the **F2** key to display the EFI Setup screen.



The EFI Setup screen has six setup menus: Main, Advanced, Chipset, iSCSI, Boot, Security, and Save & Exit.

Main menu

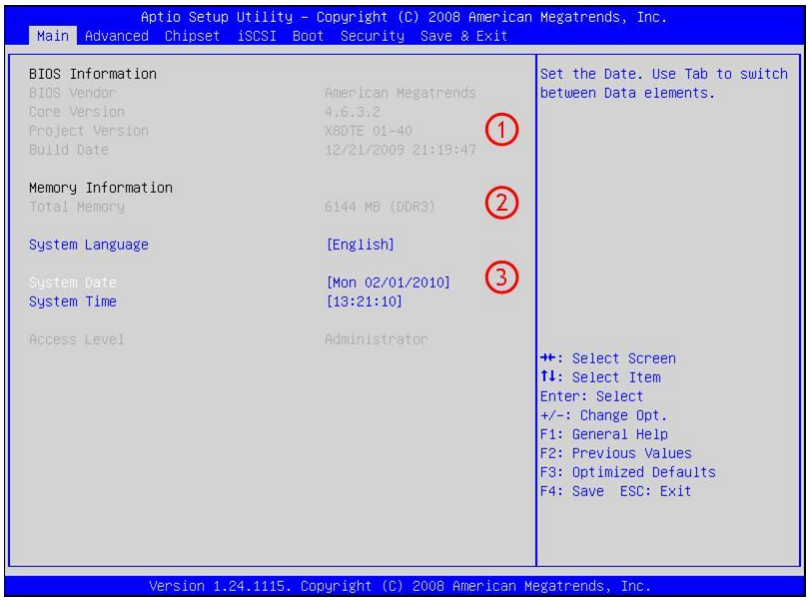


Figure 5-1 Main menu

On the Main menu, you can check the following items:

- EFI version: (1)
- Installed memory: (2)
- Server blade system time: (3)

Note: The keys used for operations in the EFI Setup menus are shown on the right side of the screen. Make sure not to use function keys F1 to F4 because you may unintentionally alter the settings with those keys.

❑ Checking the EFI version

The EFI version is the "XX.YY" part of "X8DTE XX.YY x64" in the "Project Version" field, where:

XX : Major Version

YY : Minor Version

In the following example, the EFI version is 01-40.



❑ Checking the installed memory

After increasing or replacing memory, you can check the amount of installed memory from the following item. Note that the displayed size is the total memory.*

In this example, 6144 MB of memory is installed.



*Note that when memory mirroring mode is enabled, the displayed size is one half of the total installed memory.

❑ Setting the server blade system time

You can check and set the date and time set in the server blade system.

Move the cursor to the item you want to change.



Use the **Tab** key to toggle between System Date and System Time. To change the setting, use the plus (+) and minus (-) keys.

Advanced menu

On the Advanced menu, you can enable or disable the PXE booting option.

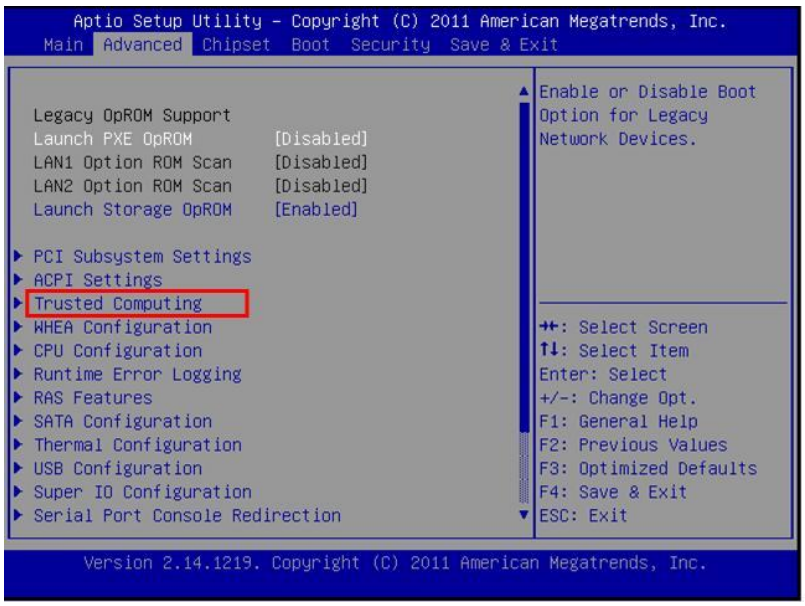


Figure 5-2: Advanced Menu

To enable PXE booting, move the cursor to **Launch PXE OpROM** and press **Enter**.

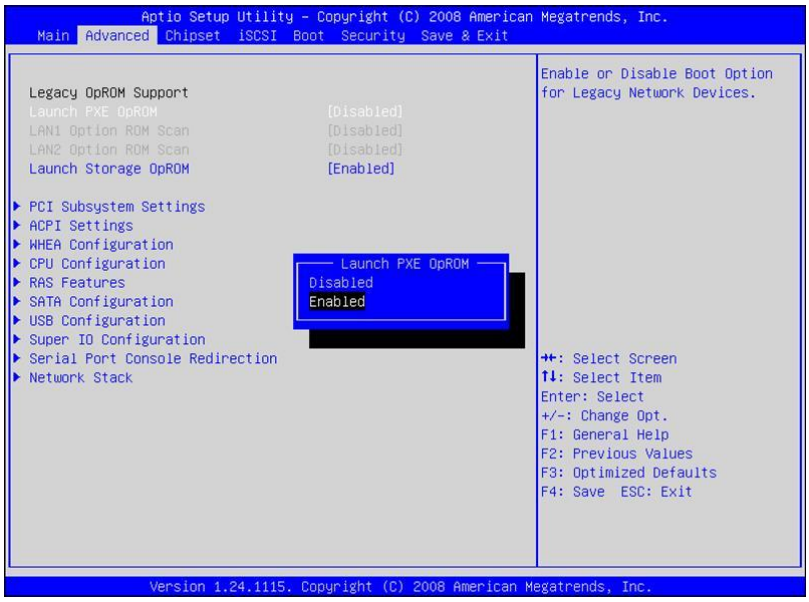


Figure 5-3: Setting PXE Enabled

The screen appears as shown in Figure 5-3. To specify Enabled, move the cursor to **Enabled** and press **Enter**.

Next, enable PXE booting for LAN1 in the same manner.

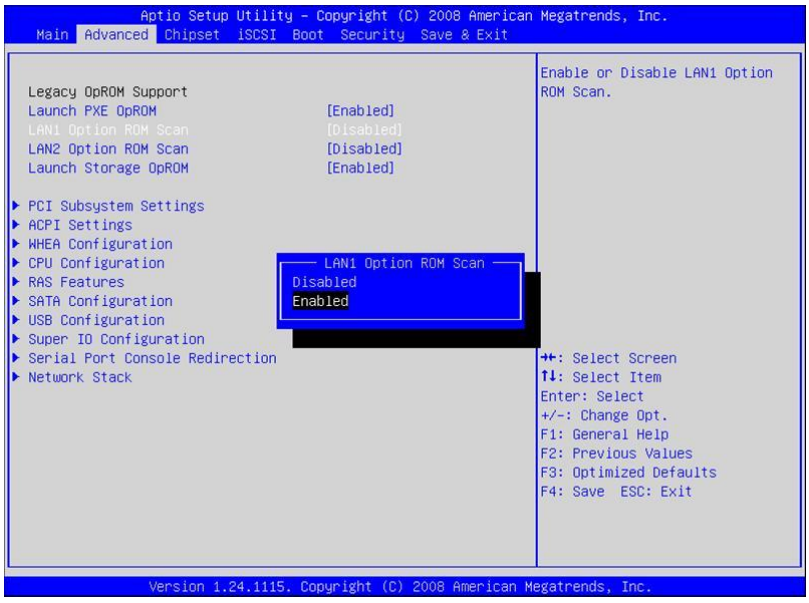


Figure 5-4: Setting LAN1 PXE Enabled

To enable PXE booting for LAN2, perform the setting in the same manner. You can enable PXE for LAN1 and LAN2 respectively or simultaneously.

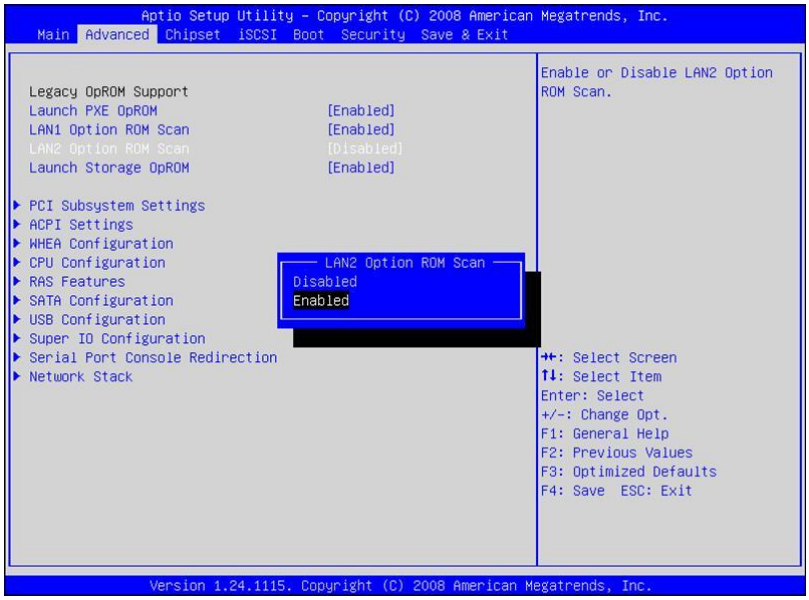


Figure 5-5: Setting LAN2 PXE Enabled

After changing settings, make sure to select Save Changes and Reset or Save Changes on the Save & Exit menu.

This is the last item that can be set on the Advanced menu.

Be sure not to change other settings. If you do, EFI may fail to restart.

Chipset menu

On the Chipset menu, you can check memory-related and Wake On Lan settings.

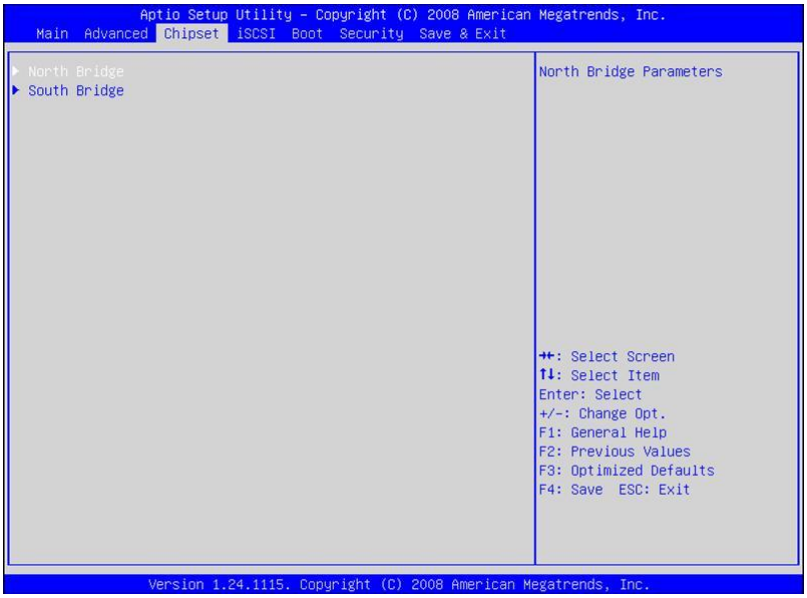


Figure 5-6: Chipset Menu

(1) Checking the Memory Mode and NUMA Settings

To check the Memory Mode and NUMA settings, select **North Bridge** on Figure 5-6 **Chipset** menu to show the following sub-menu.

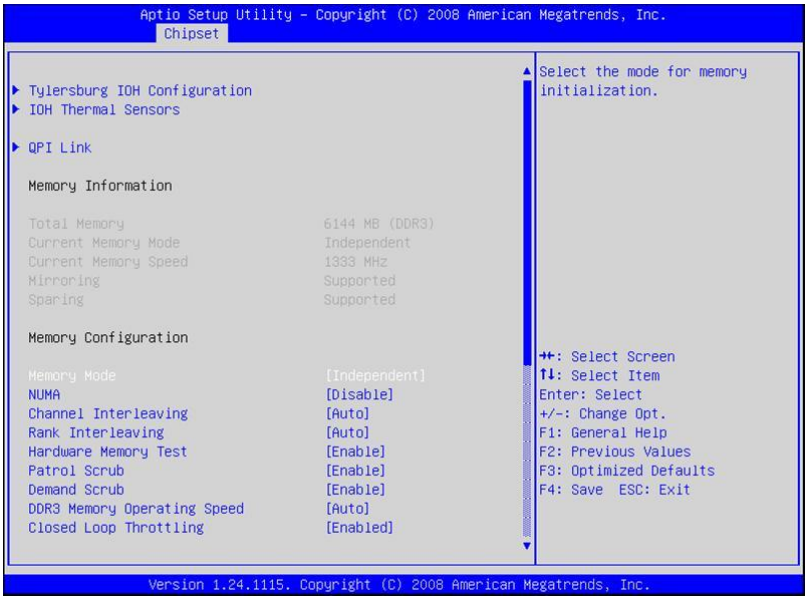


Figure 5-7: North Bridge Sub-Menu

Make sure that the settings for Memory Mode and NUMA are the same as the settings on the server blade web console.

See EFI setup in Server Blade Web Console Function for details about setting the memory mode on the server blade web console.

On the North Bridge sub-menu, you can check the Memory Mode and NUMA settings, but you must not attempt to change the settings.

Change the Memory Mode and NUMA settings, if necessary, only from the server blade Web console.

The settings on the North Bridge sub-menu can be viewed only. They must not be changed. Be careful because if a setting is changed inadvertently, the EFI may not start.

(2) Checking and Setting Wake On Lan

To check the Wake On Lan setting, select **South Bridge** on Figure 5-6: Chipset Menu to show the following sub-menu.

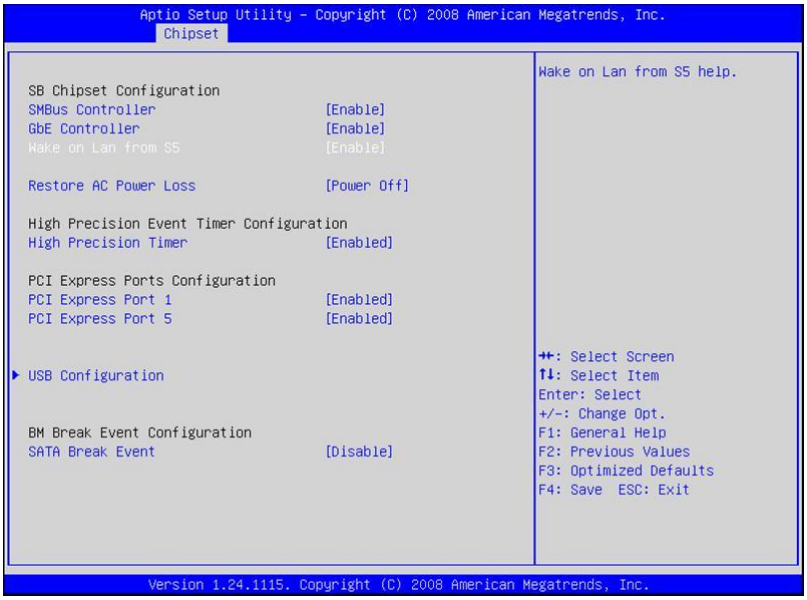


Figure 5-8: South Bridge Sub-Menu

Wake On Lan is always set to Enable.

If the setting appears as **Disable** for any reason, change it to **Enable**. On the South Bridge sub-menu, Wake On LAN is the only setting you can change. You must not change the other settings.

iSCSI menu

On the iSCSI menu, you can check the internet small computer system interface (iSCSI) settings.

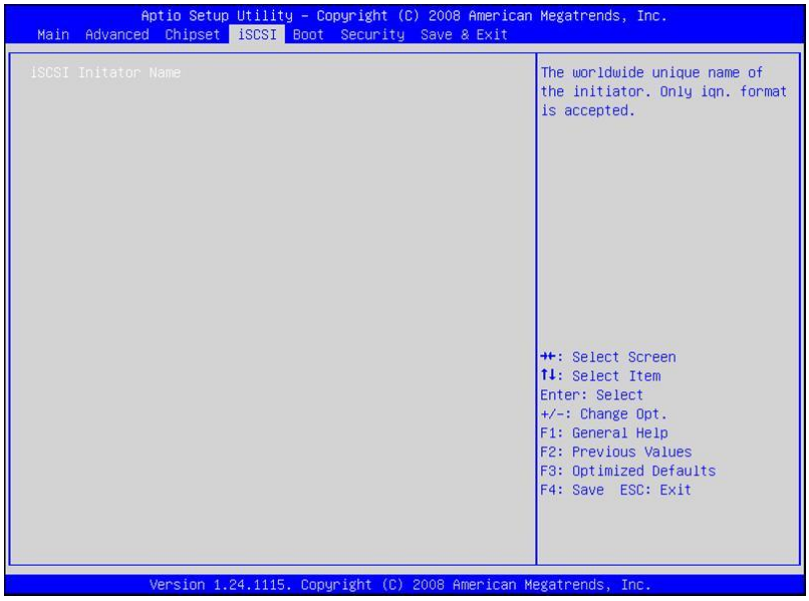


Figure 5-9: iSCSI Selection Menu

Boot menu

On the Boot menu, you can set the boot paths.

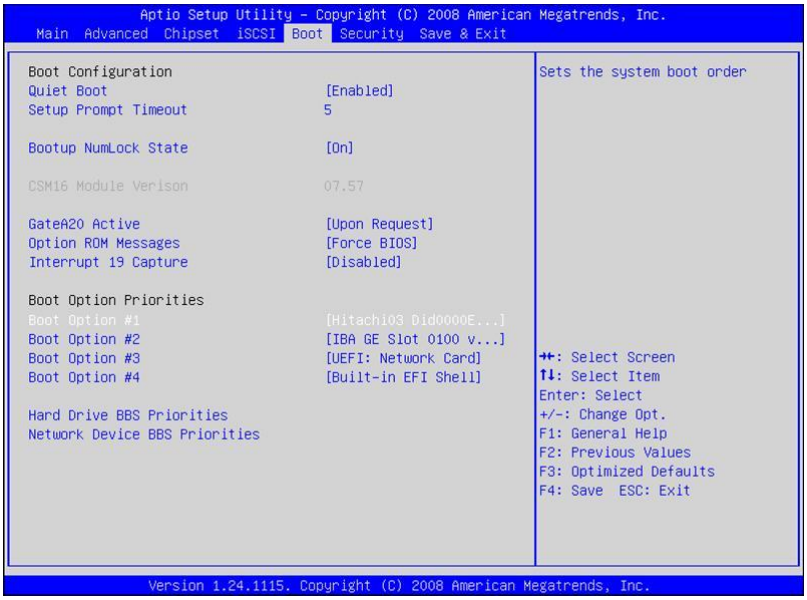


Figure 5-10: Boot Menu

EFI searches connection paths to peripheral devices in the order shown in the following table, and recognizes I/O devices at server blade startup. In Symmetric Multiprocessing (SMP) configuration, I/O devices are recognized in ascending order of server blade number.

Search order	Connection path to peripheral devices	Connection in the server blade	
	Device name	Location	Slot No.
1	Embedded HDD	-	-
2	Onboard NIC0 *1	Switch module slot	0
3	Onboard NIC1 *1		1
4	I/O board #1 *2	I/O board module slot	Odd number
5	I/O board #0 *2		Even number
6	Expansion card #0	Switch module slot	2
7			3
8	Expansion card #1		4
9			5

*1 In SMP configuration, PXE boot is supported only by onboard NIC of the primary blade.

*2 When an I/O slot expansion unit is connected, I/O devices are recognized in ascending order of the I/O board slot number.

The boot devices are booted in the order (#n) set in the Boot Option Priorities (where n: 1, 2, 3,...).

Up to four boot paths can be set. Items to be set in this screen depend on devices connected.

❑ About Boot Paths (Legacy Boot and EFI Boot)

Boot paths are categorized into two boot modes in the Compute Blade 2000. The implemented boot processing depends on which mode you select.

The two Compute Blade 2000 boot modes are:

- Legacy booting (conventional mode and boot method)
- EFI booting (newly supported mode and boot method)

The boot mode is determined automatically according to the boot device selected as Boot Option #1.

When Built-in Shell or UEFI:xxxxx is selected as Boot Option #1, EFI booting applies and the legacy boot path will be ignored.

Note that when a boot device other than Built-in Shell or UEFI:xxxxx is selected as Boot Option #1, the EFI boot path will be ignored.

❑ Selecting PXE booting

PXE booting can be specified in the boot path if Enabled is set for Launch PXE OpROM on the Advanced menu.

To specify PXE booting, set Boot Option #1 as follows:

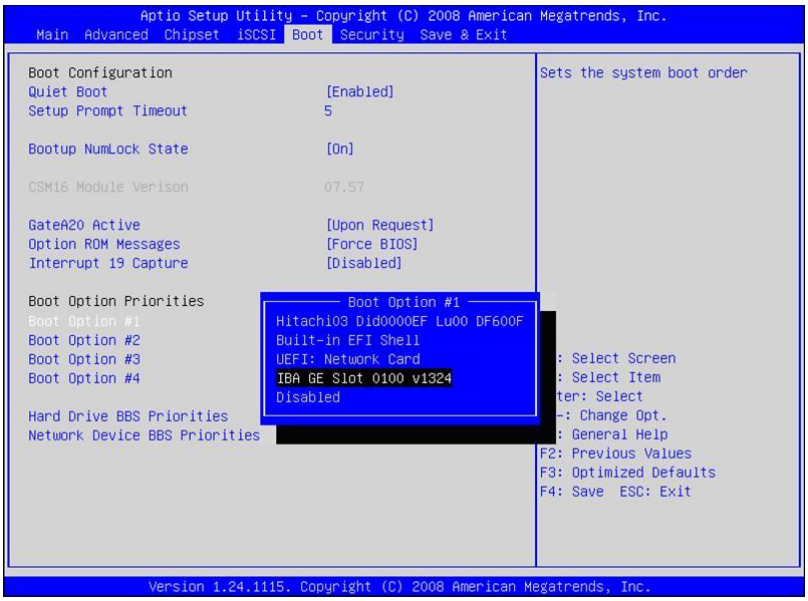


Figure 5-11: Setting the PXE Boot Path

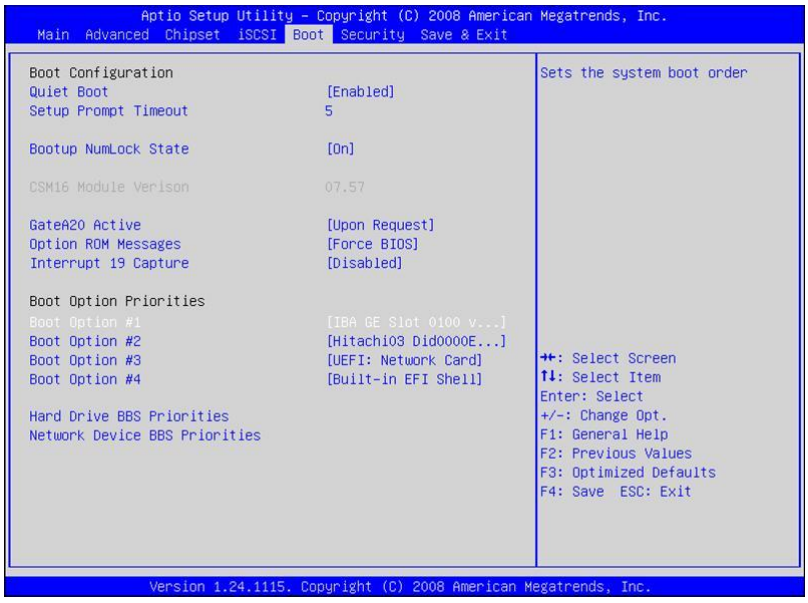


Figure 5-12: Screen with PXE Boot Path Specified

After changing the setting, remember to select Save Changes and Reset or Save Changes on the Save & Exit menu described later in this manual.

Security menu

The Security menu is for setting the administrator or user password.

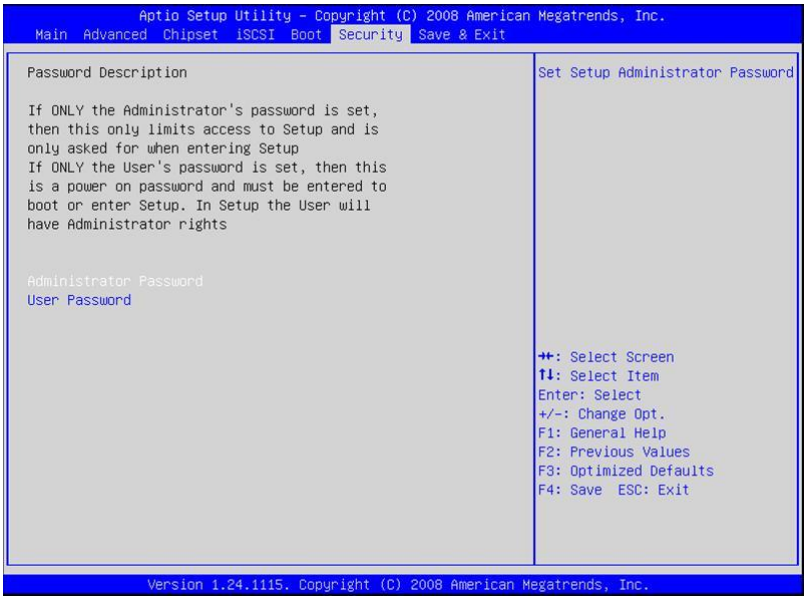


Figure 5-13: Security menu

You need to input a password, which you have set, at the timing shown in the following table.

#	Administrator password	User password	Request for password authentication
1	✓	✓	While a server blade is being booted *1
2	✓	-	When you enter the EFI Setup screen
3	-	✓	While a server blade is being booted *1

✓: The password is set; [-]: The password is not set.

*1 With EFI firmware version 01-61/02-61 or later , or 03-44/04-44 or later, you are not requested to input a password for authentication while a server blade is being booted.

Any password can be set for a user.

When you set a user password with EFI firmware version earlier than 01-61/02-61, or earlier than 03-44/04-44, it is always necessary to enter the password for authentication while a server blade is being booted.

When you set the N+M cold standby, high availability (HA), or automatic OS boot, do not set a password. Otherwise, the password authentication interrupts switching systems or booting modules.

Save & Exit menu

Use the Save & Exit menu to save changes or to restore changed settings to the Defaults.

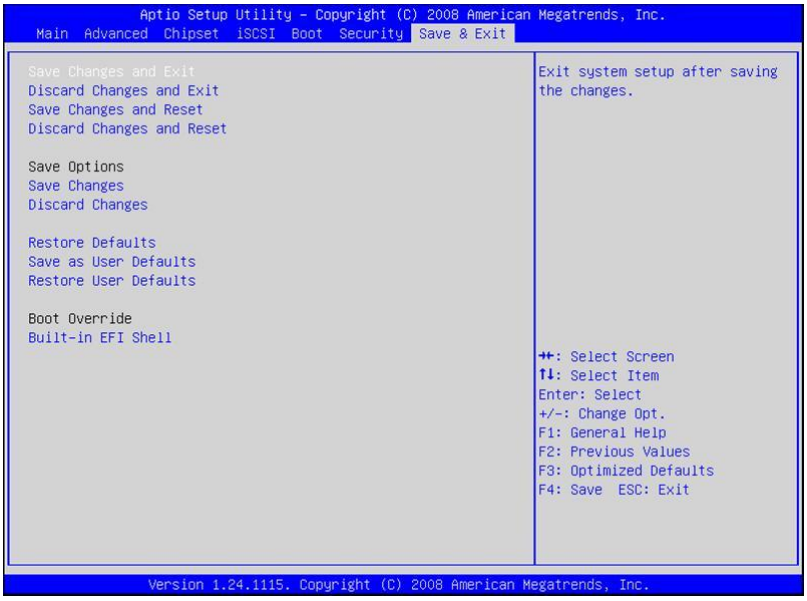


Figure 5-14: Save & Exit menu

Each item is described in the following table.

#	Item	Processing
1	Save Changes and Exit	Saves changes and exits the Setup utility. Boots the system from the device set in the boot path.
2	Discard Changes and Exit	Discards changes and exits the Setup utility. Boots the system from the device set in the boot path.
3	Save Changes and Reset	Saves changes and restarts the system.
4	Discard Changes and Reset	Discards changes and exits the Setup utility. Restarts the system.
5	Save Changes	Saves changes.
6	Discard Changes	Discards changes.
7	Restore Defaults	Restores settings to the system Defaults.
8	Save as User Defaults	Saves settings as user Defaults.
9	Restore User Defaults	Restores settings to the user Defaults.

❑ Boot Override

Boot Override on the Save & Exit menu allows you to boot the system from a specific device, disregarding the boot path set as Boot Option #1.

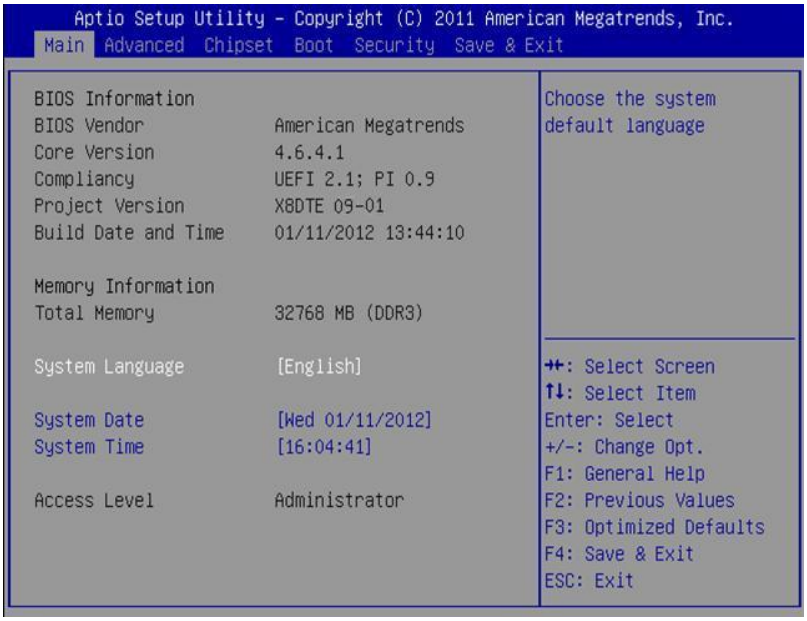
Unless otherwise specified, Boot Override would not normally be used.

Standard server blade setup menu (X55R3/X55S3/55R4 models)

EFI setup screen

By entering the EFI setup screen while the server blade is booting, you can halt the boot process and check or change the settings. With the EFI startup screen open, press one of the following keys to display the EFI Setup screen.

- X55R3/X55S3 model: F2 key
- X55R4 model: Delete key



The EFI Setup screen has six setup menus: Main, Advanced, Chipset, Boot, Security, and Save & Exit.

Main menu

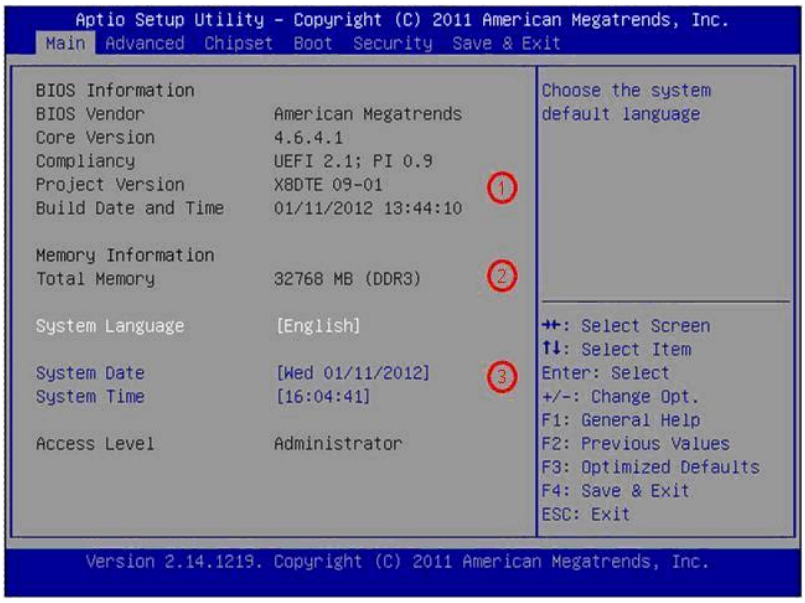


Figure 5-15 Main menu

On the Main menu, you can check the following items:

- EFI version: (1)
- Installed memory: (2)
- Server blade system time: (3)

Note: The keys used for operations in the EFI Setup menus are shown on the right side of the screen. Make sure not to use function keys F1 to F4 because you may unintentionally alter the settings with those keys.

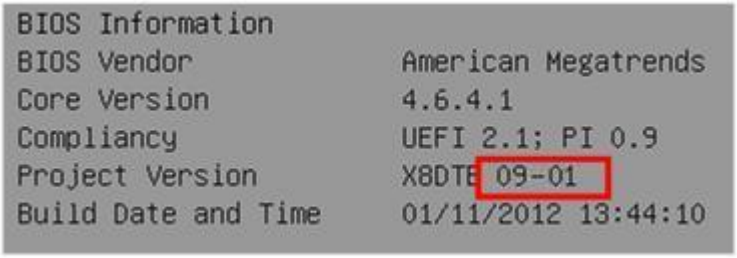
❑ Checking the EFI version

The EFI version is the `XX.YY`" part of `X8DTE XX.YY` in the **Project Version** field, where:

XX : Major Version

YY : Minor Version

In the example below, the EFI version is 09-01.



❑ Checking the installed memory

After increasing or replacing memory, you can check the amount of installed memory from the following item. Note that the displayed size is the total memory.*

In this example, 32 GB of memory is installed.



*When memory mirroring mode is enabled, the displayed size is one half of the total installed memory.

❑ Setting the server blade system time

You can check and set the date and time set in the server blade system.

Move the cursor to the item you want to change.



Use the Tab key to toggle between System Date and System Time.

To change the setting, use the plus (+) and minus (-) keys.

Advanced menu

On the Advanced menu, you can enable or disable the PXE booting option, show iSCSI settings, and set Trusted Platform Module (TPM) if TPM is installed.

For the X55R4 model, Launch PXE OpROM and Launch storage OpROM are not shown; see the EFI Setup screen in Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for the following settings.

- Launch PXE OpROM
- LAN1 Option ROM Scan
- LAN2 Option ROM Scan
- Launch storage OpROM

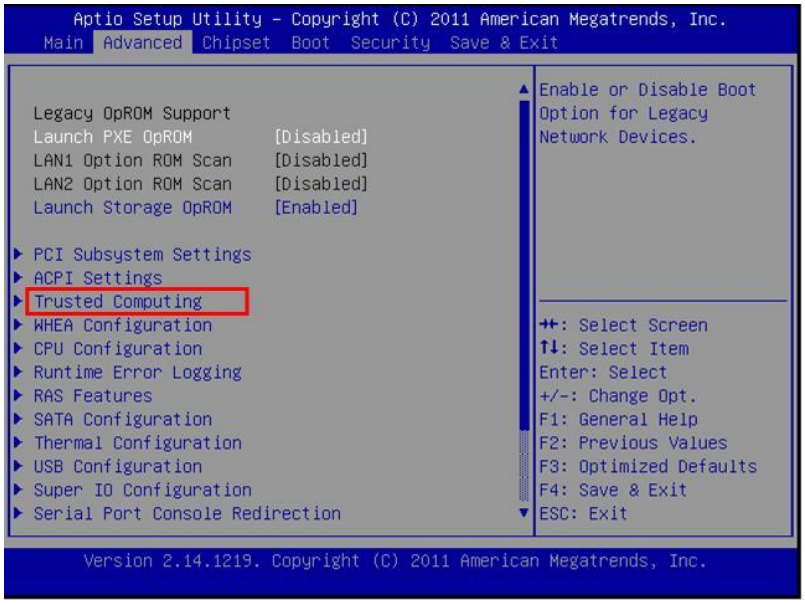


Figure 5-16: Advanced menu if TPM is installed

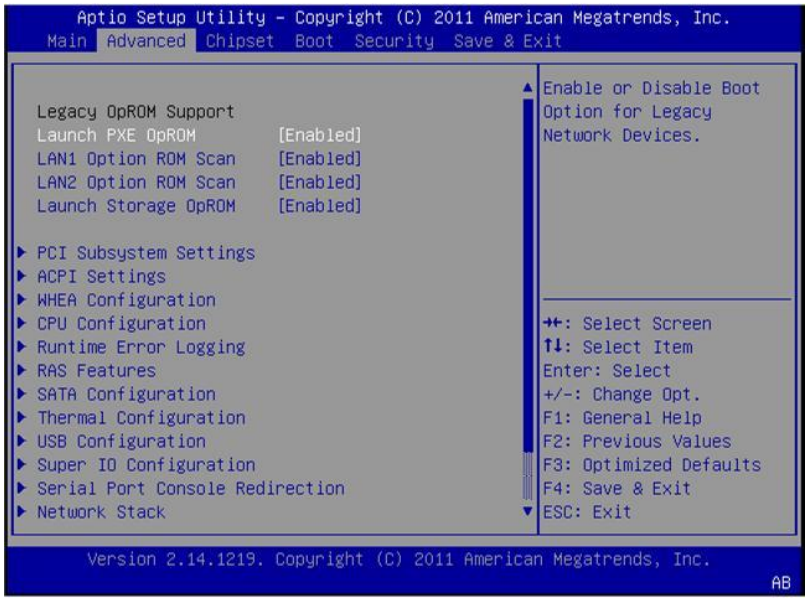


Figure 5-17: Advanced menu if TPM not installed

(1) Enabling/Disabling PXE booting

To enable PXE booting, move the cursor to **Launch PXE OpROM** and press **Enter**.

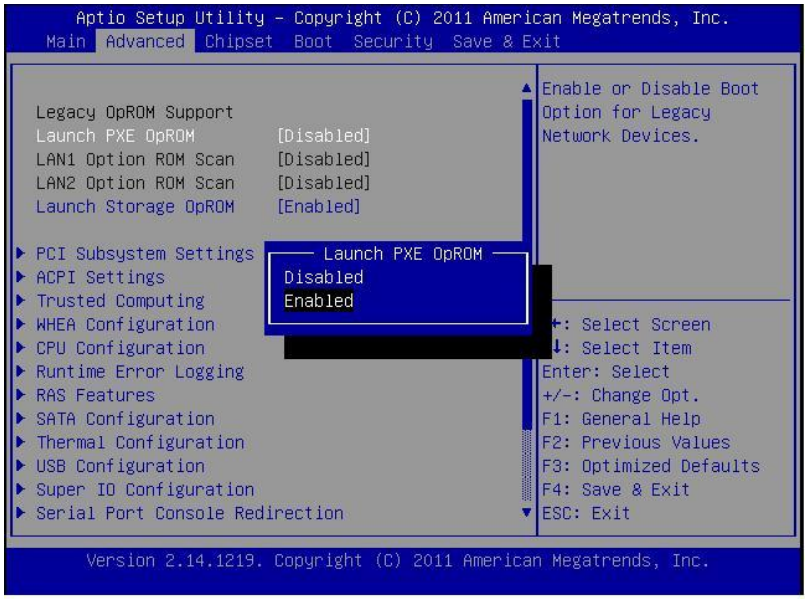


Figure 5-18: Setting PXE enabled

The screen appears as in Figure 5-18. To specify Enabled, move the cursor to **Enabled** and press **Enter**.

Next, enable PXE booting for LAN1 in the same manner.

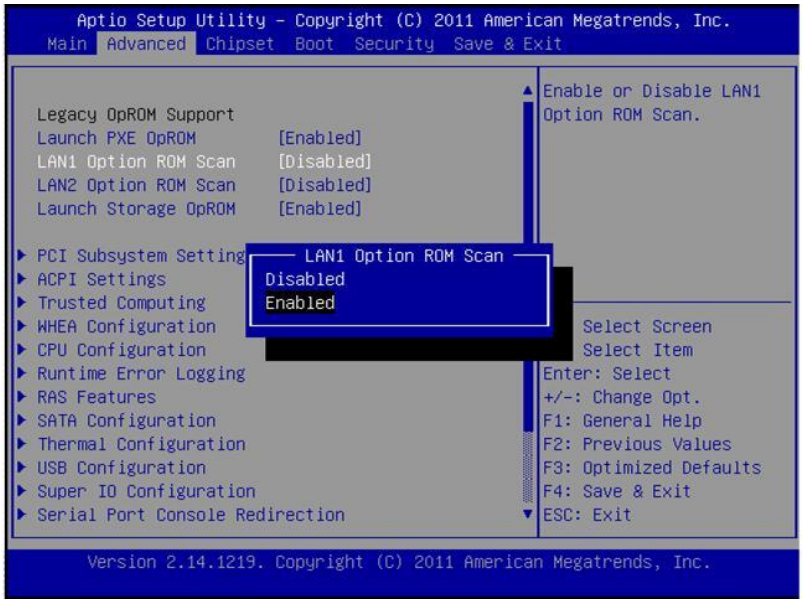


Figure 5-19: Setting LAN1 PXE enabled

To enable PXE booting for LAN2, perform the setting in the same manner. You can enable PXE for LAN1 and LAN2 respectively, or simultaneously.

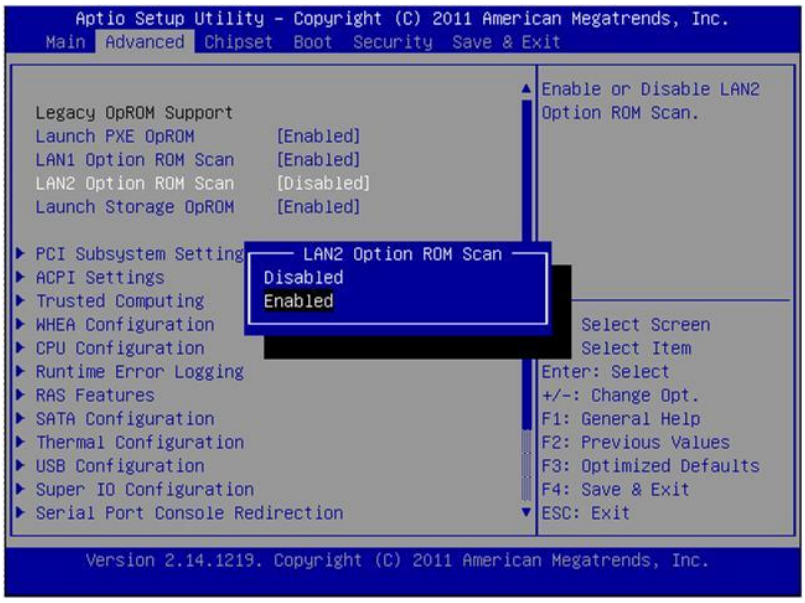


Figure 5-20: Setting LAN2 PXE enabled

(2) Viewing iSCSI

To show iSCSI settings, place the cursor on **iSCSI** and press **Enter**.

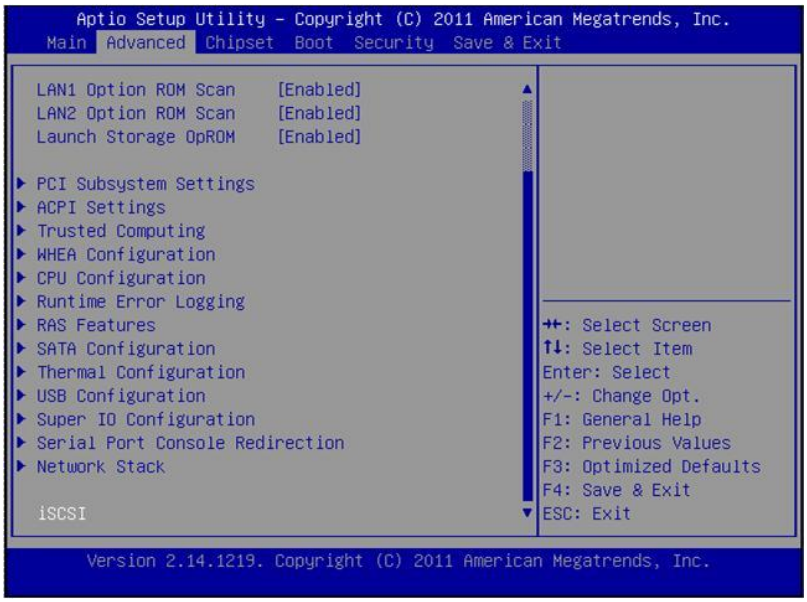


Figure 5-21 iSCSI setting to view or not

The following screen shows the iSCSI setting.

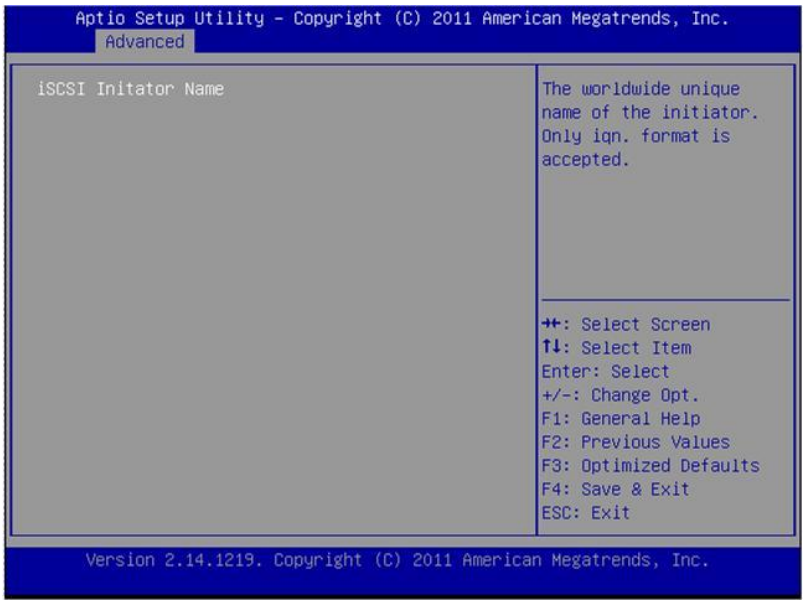


Figure 5-22: iSCSI setting shown

(3) TPM settings

To set TPM, place the cursor on **Trusted Computing** and press **Enter** to show the TPM setting screen.

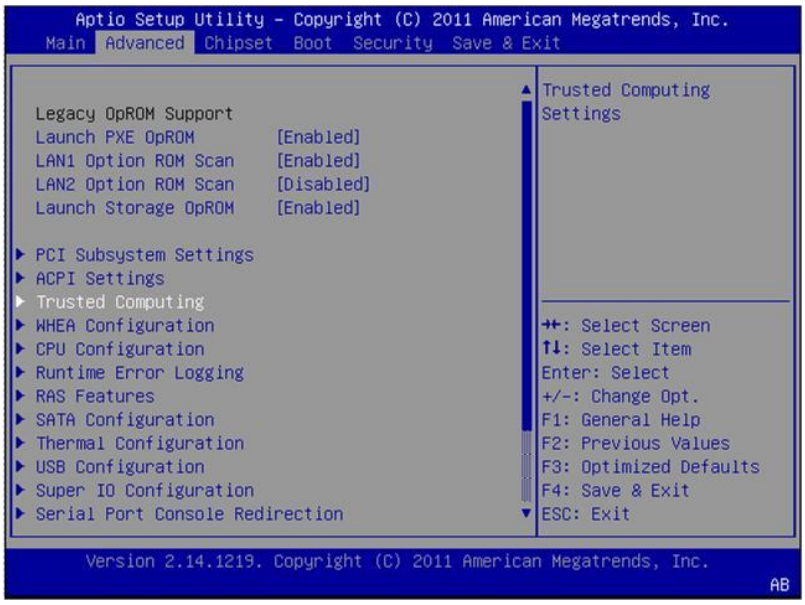


Figure 5-23 TPM to set or not

Do not disable TPM SUPPORT. If you do, BitLocker may not be installed. Just view other items and do not change their values.

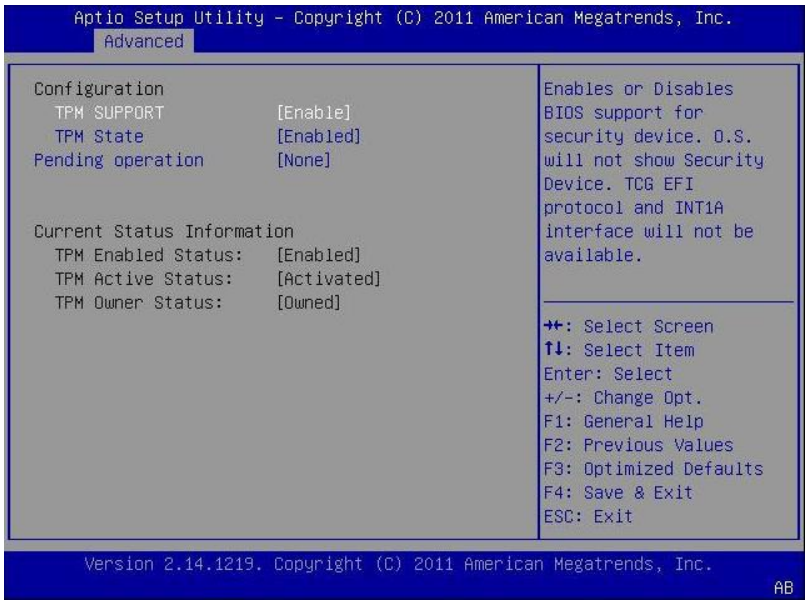


Figure 5-24: TPM to set



On Windows Server 2012 installed from EFI boot, do not execute BitLocker drive encryption using TPM due to it not being supported.

❑ Physical presence request

When you operate TPM using a program on the OS, the following Physical presence request may be displayed while booting the server blade next time. It requires user intervention to distinguish the TPM operation from that by a malicious program. Follow the directions shown on the screen. If you permit the TPM operation, press the F10 key; if not, press the Esc key. Press the F12 key instead of the F10 key depending on the operation.

Note that pressing the Esc key may display the Physical Presence request screen again. You do not need to press the Esc key again.

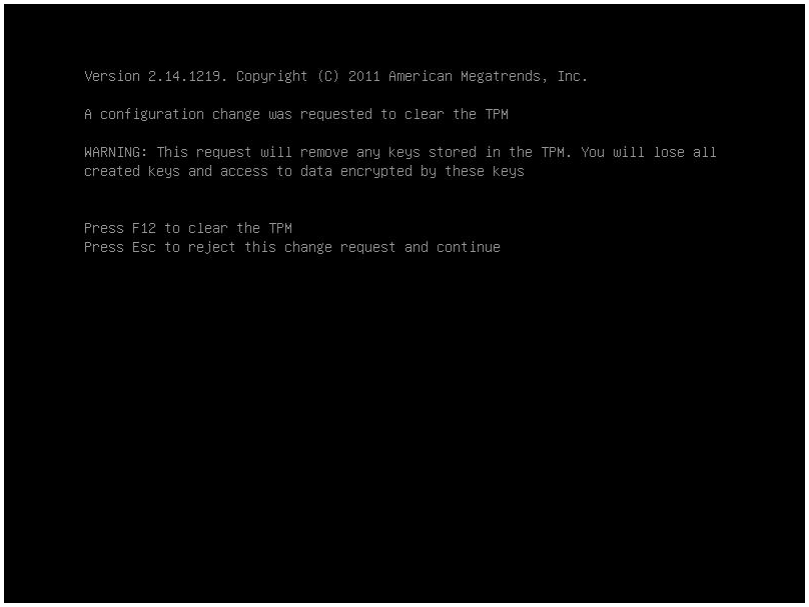


Figure 5-25: Physical presence request

After changing settings, make sure to select Save Changes and Reset or Save Changes on the Save & Exit menu. This is the last item that can be set on the Advanced menu.

Be sure not to change other settings because EFI may fail to restart.

Chipset menu

On the Chipset menu, you can check memory-related and Wake On Lan settings.

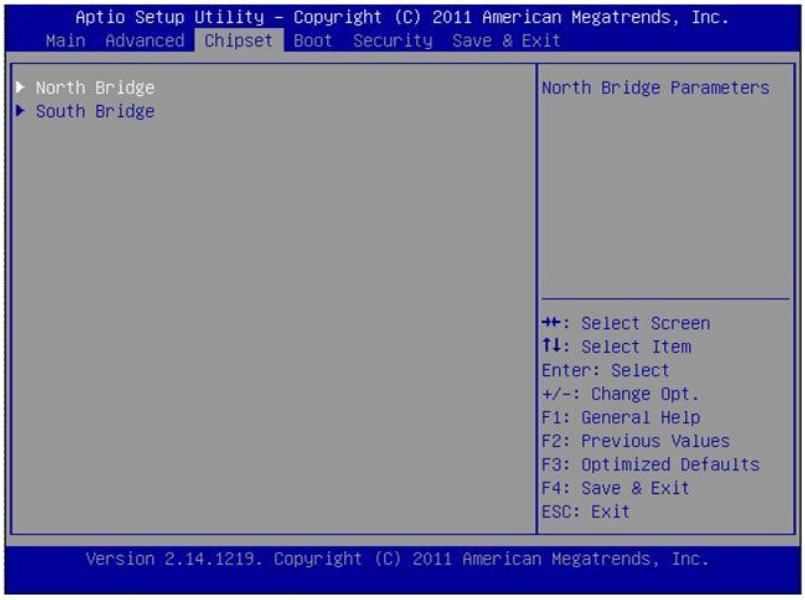


Figure 5-26: Chipset menu

(1) Checking the memory mode and NUMA settings

To check the Memory Mode and NUMA settings, select **North Bridge** on the Chipset menu.

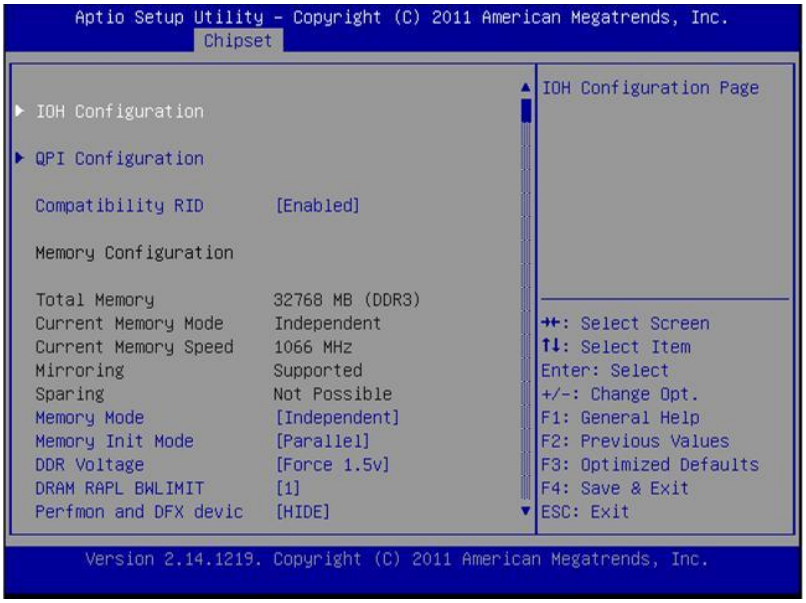


Figure 5-27: North Bridge sub-menu

Make sure that the settings for Memory Mode and NUMA are the same as those on the server blade web console.

See the BMC manual about setting the memory mode on the server blade Web console.

On the North Bridge sub-menu, you can check the Memory Mode and NUMA settings, but you must not attempt to change the settings.

Change the Memory Mode and NUMA settings, if necessary, only from the server blade web console.

The settings on the North Bridge sub-menu can be viewed only. They must not be changed. If a setting is changed inadvertently, the EFI might not start.

(2) Checking and setting Wake On Lan

To check the Wake On Lan setting, select **South Bridge** on the Chipset menu.

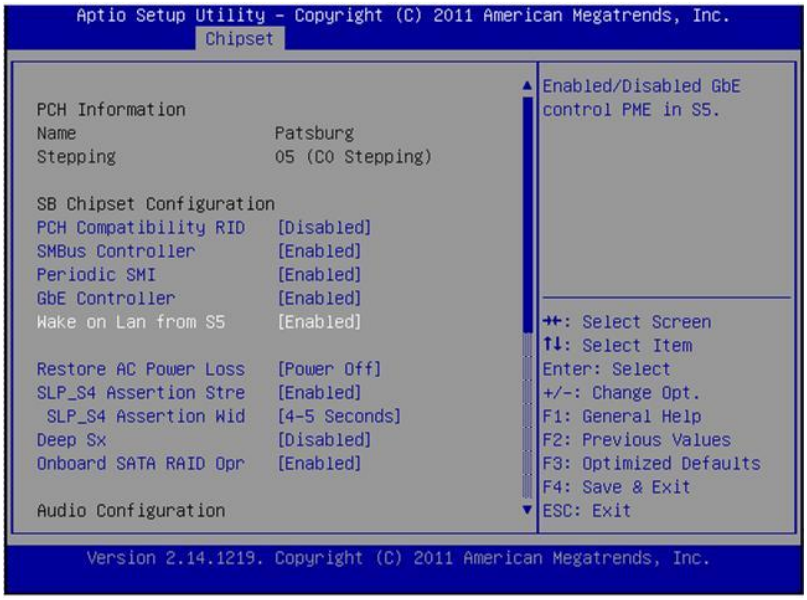


Figure 5-28: South Bridge to set WOL

Wake On Lan is always set to Enabled.

If the setting appears as Disable, change it to Enable. On the South Bridge sub-menu, Wake On LAN (WOL) is the only setting you can change. You must not change the other settings.

Boot menu

On the Boot menu, you can set the boot paths.

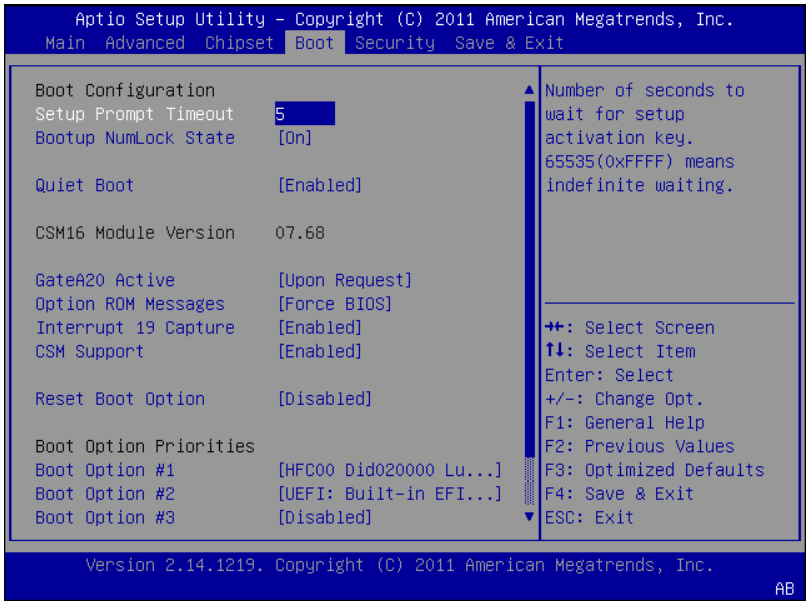


Figure 5-29: Boot menu

The boot devices are booted in the order (#n) set in the Boot Option (where n: 1, 2, 3).

Up to 4 boot paths can be set. Items to be set in this screen depend on the number of devices connected.



When a boot device is not connected to the server blade, built-in EFI Shell automatically starts. To return to the EFI setup screen from EFI Shell, you need to perform the exit command twice on EFI Shell. Once you perform the exit command, EFI Shell starts again. Then perform the exit command again.

❑ About boot paths (legacy boot and EFI boot)

Boot paths are categorized into two boot modes in the Compute Blade 2000. The implemented boot processing depends on which mode you select.

The two Compute Blade 2000 boot modes are:

- Legacy booting (conventional mode and boot method)
- EFI booting (newly supported mode and boot method)

The boot mode is determined automatically according to the boot device selected as Boot Option #1.

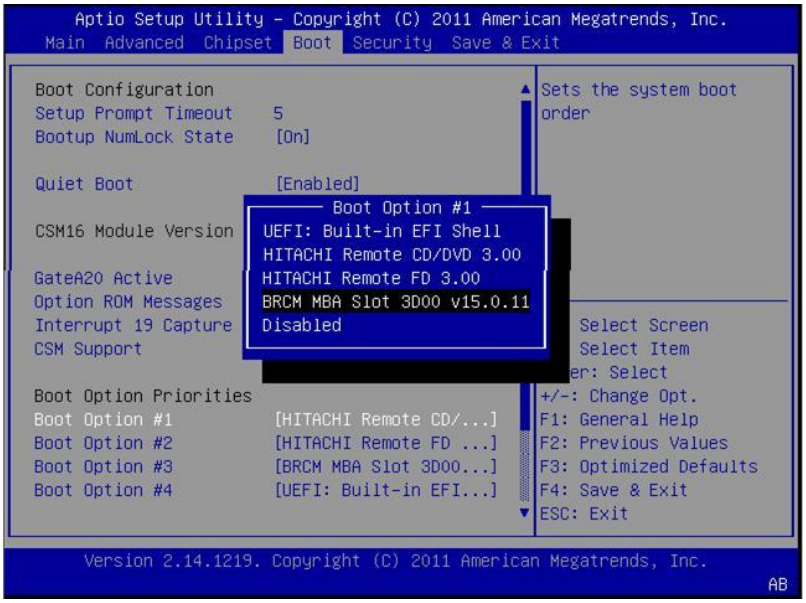
When Built-in Shell or UEFI:xxxxx is selected as Boot Option #1, EFI booting applies and the legacy boot path will be ignored.

Note that when a boot device other than Built-in Shell or UEFI:xxxxx is selected as Boot Option #1, the EFI boot path will be ignored.

❑ Selecting PXE booting

PXE booting can be specified in the boot path if Enabled is set for Launch PXE OpROM on the Advanced menu or on the Server Operation > EFI Setup of the server blade Web console. See Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for details of the server blade Web console.

To specify PXE booting, set **Boot Option #1** as follows:



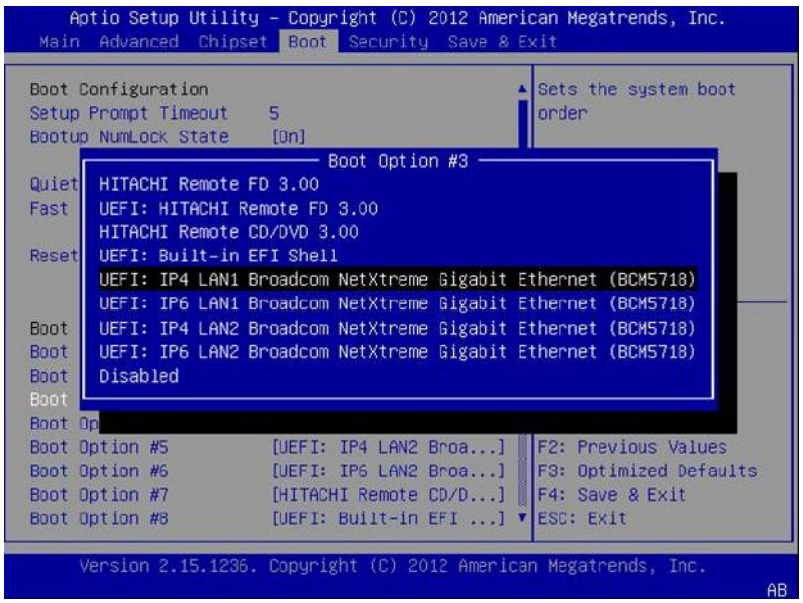


Figure 5-30: Setting the PXE boot path (Examples of Legacy boot)

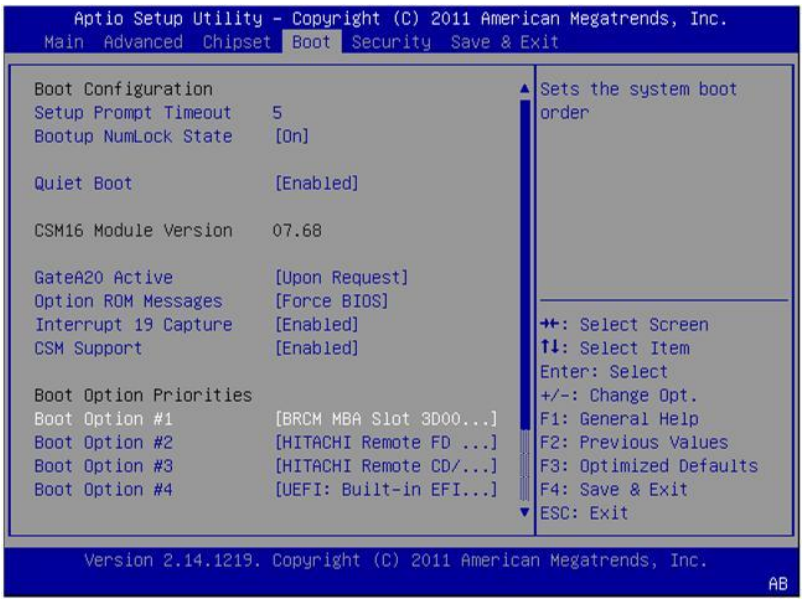


Figure 5-31: PXE boot path specified (Example of Legacy boot)

After changing the setting, remember to select Save Changes and Reset or Save Changes on the Save & Exit menu.

❑ Reset boot option

When you reboot a server blade with Reset Boot Option Enabled, Boot Option Priorities is initialized. Execute the following to initialize Boot Option Priorities.

- Remove the boot device and Built-in EFI shell to delete the boot option
- Initialize the boot priorities to the default.

Reset Boot Option is shown and available for EFI firmware version 09-42/10-42 or later for X55R3/X55S3 model, and for EFI firmware version 11-01/12-01 or later on X55R4 model. Make sure to execute Save Changes and Reset referring to Save & Exit menu before initializing Boot Option Priorities.



You cannot separately delete boot options and initialize boot priorities. Initialize Boot Option Priorities, and then reset boot options as necessary.

Security menu

The Security menu is for setting the administrator or user password.

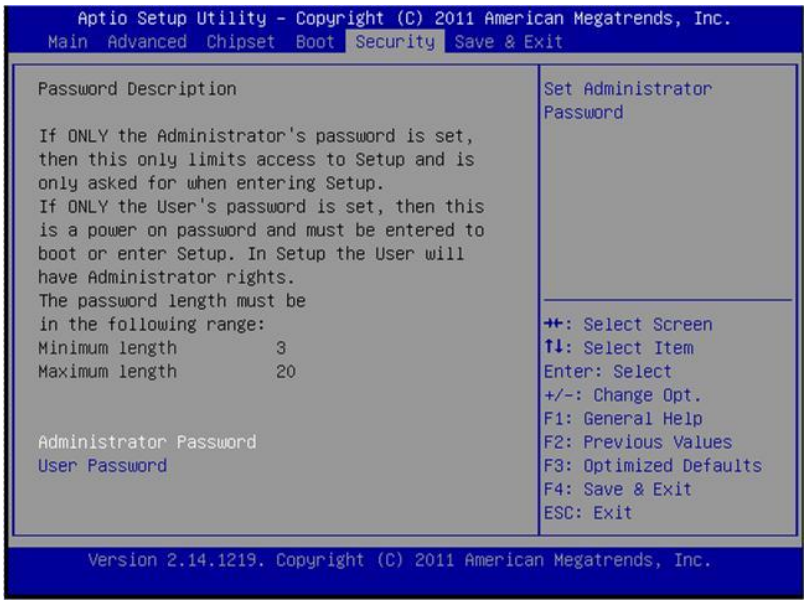


Figure 5-32: Security menu

You need to enter a password, which you have set, according to the table below.

#	Administrator password	User password	Request for password authentication
1	✓	✓	While a server blade is being booted
2	✓	-	When you enter the EFI Setup screen
3	-	✓	While a server blade is being booted

[✓]: The password is set; [-]: The password is not set.

Any password can be set for a user.

When you set a password, however, it is always necessary to enter the password for authentication when booting the server module.

When you set the N+M cold standby or automatic OS boot, do not set a password. Otherwise, the password authentication interrupts switching systems or booting modules.

Save & Exit menu

Use the Save & Exit menu to save changes or to restore changed settings to the defaults.

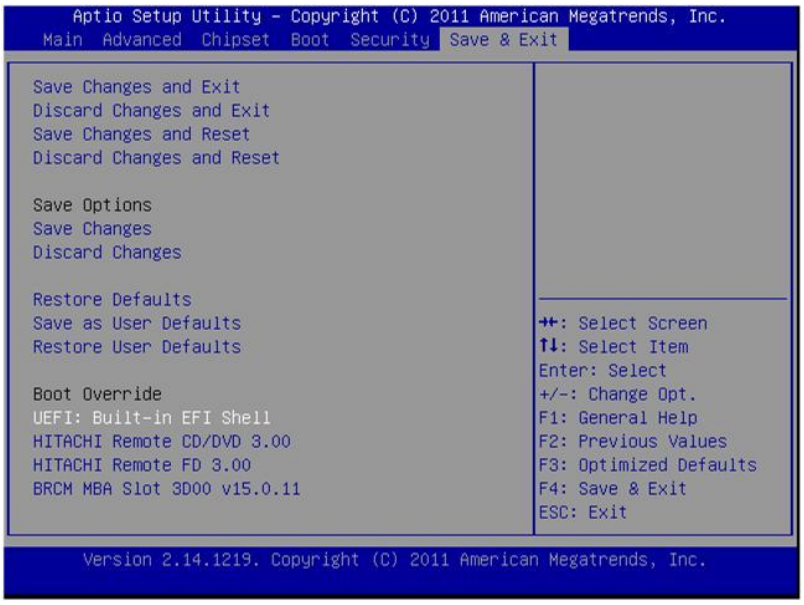


Figure 5-33: Save & Exit menu

Each item is described in the table below.

#	Item	Processing
1	Save Changes and Exit	Saves changes and exits the Setup utility. Boots the system from the device set in the boot path.
2	Discard Changes and Exit	Discards changes and exits the Setup utility. Boots the system from the device set in the boot path.
3	Save Changes and Reset	Saves changes and restarts the system.
4	Discard Changes and Reset	Discards changes and exits the Setup utility. Restarts the system.
5	Save Changes	Saves changes.
6	Discard Changes	Discards changes.
7	Restore Defaults	Restores settings to the system defaults.
8	Save as User Defaults	Saves settings as user defaults.
9	Restore User Defaults	Restores settings to the user defaults.

❑ Boot Override

Boot Override on the Save & Exit menu allows you to boot the system from a specific device, disregarding the boot path set as Boot Option #1.

Unless otherwise specified, Boot Override would not normally be used.

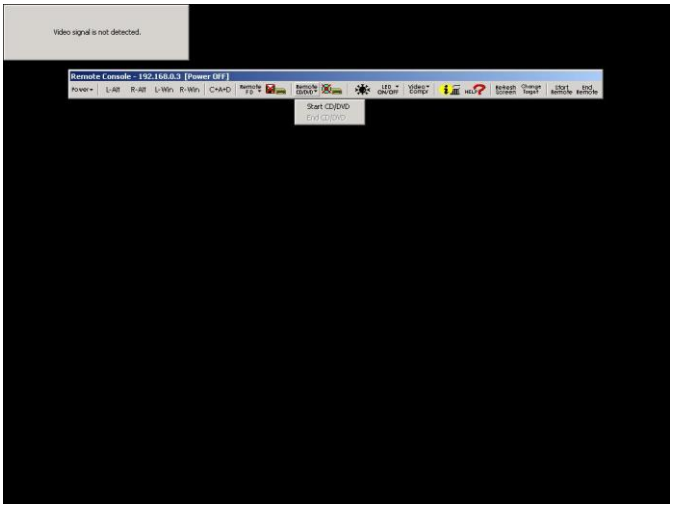
Remote CD/DVD boot procedure

To boot the server blade from the remote CD/DVD or to install the OS using the remote CD/DVD function, follow the procedure mentioned below. Steps may be different depending on your remote console application.

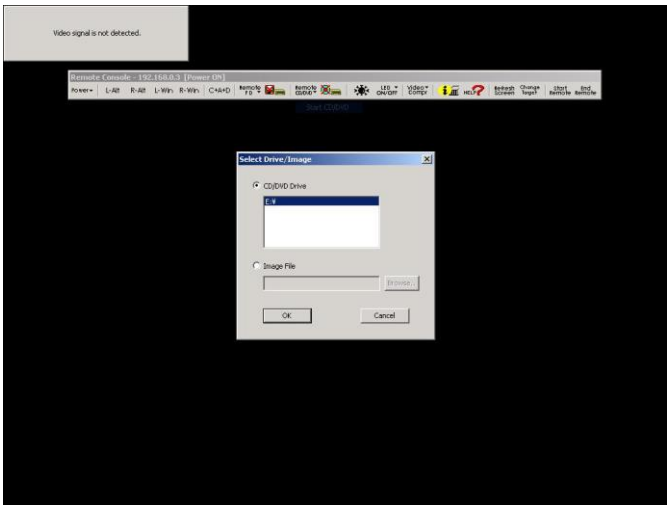
Remote Console Application (Reclient)

1 Insert the CD/DVD media into the console terminal's CD/DVD drive.

2 Start the **Remote Console Application (Reclient)**, and then select **Remote CD/DVD** on the toolbar and **Start CD/DVD**. If the toolbar is not visible, press **Alt + G** to display it.



3 Select the console terminal's CD/DVD drive, and then click **OK**.



Tip

Steps 1 to 3 must be performed before powering on or resetting the server blade; otherwise, the server blade will not recognize the remote CD/DVD.

If you want to install an OS or perform some other task using a remote FD, complete steps 1 to 3 and then select the **Remote FD menu** and **Start FD**.

4 Power on or reset the server blade, and start the EFI, and then press the **F2** key to display the EFI Setup menus.



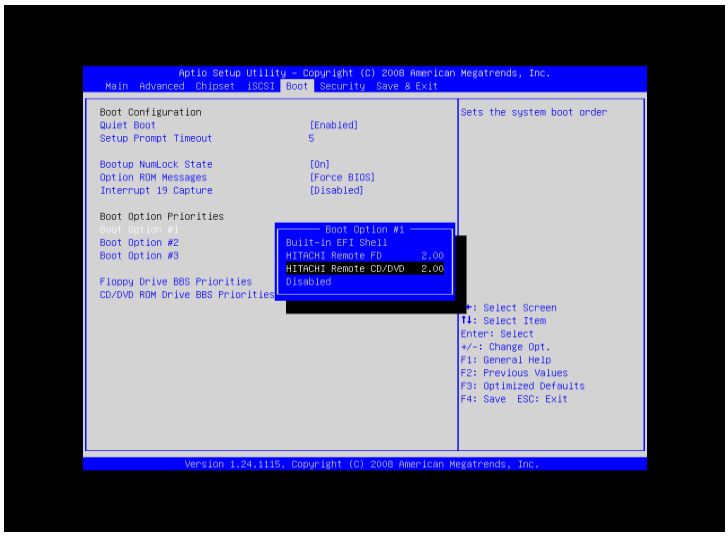
5 Select the **Boot** menu using the arrow keys. Make sure that **HITACHI Remote FD** is set in **Boot Option #1** and **HITACHI Remote CD/DVD** is set in **Boot Option #2**, as shown in the following figure.

Tip

Depending on the types of devices installed in or connected to the server blade, the display may differ from the following screen.



If the boot order differs from the order shown in the previous screen, set the correct boot devices in Boot Option #1 and Boot Option #2. The following screen shows the sub-menu for setting Boot Option #1. Boot Option #2 can be set similarly.



6 If you made no changes, select **Save & Exit** menu -- **Discard Changes and Exit** to restart the server blade. If you changed any settings, select **Save & Exit** menu -- **Save Changes and Exit** to restart the server blade. After the server blade has restarted, the system will automatically start booting from the remote CD/DVD.

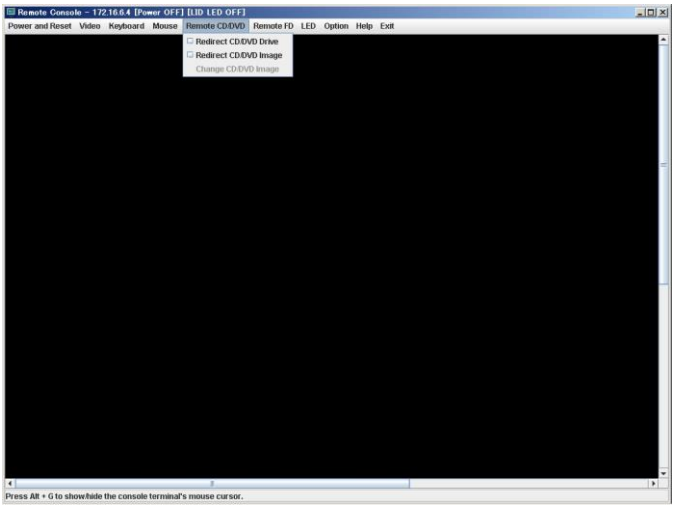
Tip

- Booting from a remote CD/DVD may fail if a floppy disk has been inserted in the console terminal's floppy disk drive. In this case, remove the floppy disk and then restart the server blade.
- Remove the CD/DVD driver media from the console terminal after installation. When using the remote console application (Reclient), select **Remote CD/DVD > End CD/DVD**. When using the remote FD, remove the media from the console terminal FD drive and select **Remote FD > End FD** on the remote console toolbar.

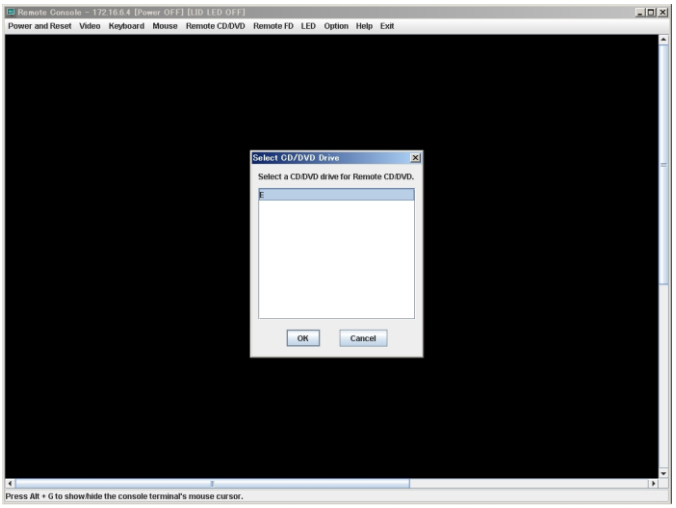
Remote Console Application (Java application)

1 Insert the CD/DVD media into the console terminal's CD/DVD drive.

2 Start the **Remote Console Application** (Java application), and then select **Remote CD/DVD** on the toolbar and **Redirect CD/DVD**.



3 Select a CD/DVD drive, then click **OK**.

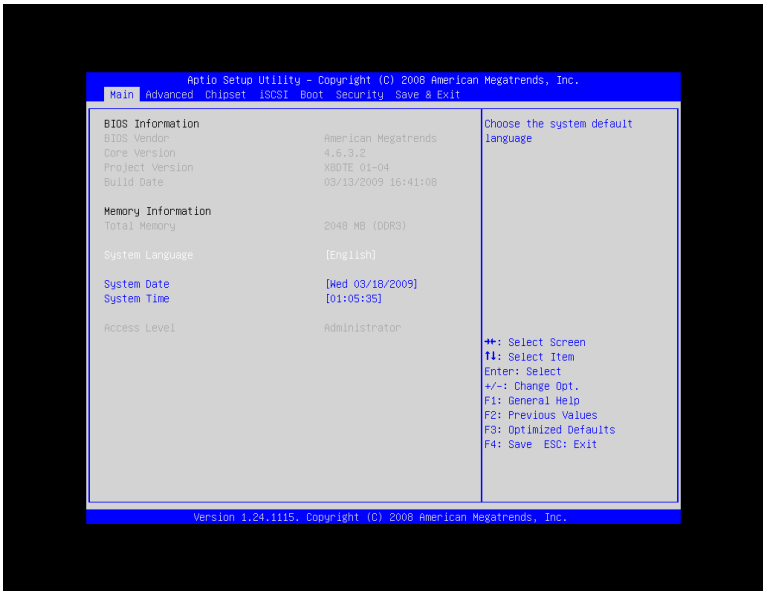


Tip

Steps 1 to 3 must be performed before powering on or resetting the server blade; otherwise, the server blade will not recognize the remote CD/DVD.

If you want to install an OS or perform some other task using a remote FD, complete steps 1 to 3 and then choose the **Remote FD** menu and **Start FD**.

4 Power on or reset the server blade, and start the EFI. Press the **F2** key to display the **EFI Setup** menus.



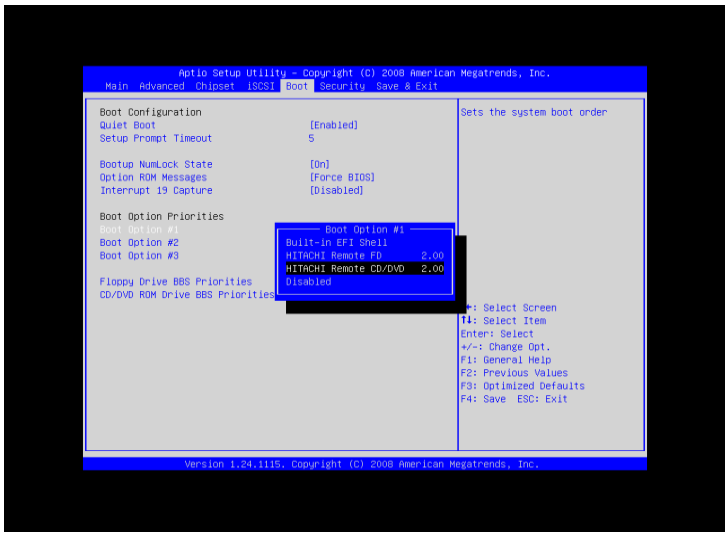
5 Select the **Boot** menu using the arrow keys. Make sure that **HITACHI Remote FD** is set in **Boot Option #1**, and **HITACHI Remote CD/DVD** is set in **Boot Option #2**, as shown in the following figure.

Tip

Depending on the types of devices installed in or connected to the server blade, the display may differ from the screenshot below.



If the boot order differs from the order shown in the previous screen, set the correct boot devices in **Boot Option #1** and **Boot Option #2**. The following screen shows the sub-menu for setting **Boot Option #1**. **Boot Option #2** can be set similarly.



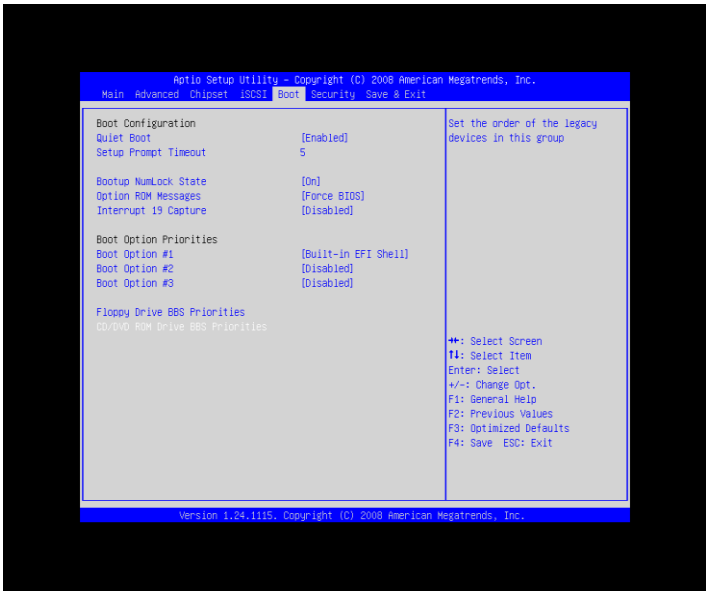
6 If you made no changes, select **Save & Exit** menu -- **Discard Changes and Exit** to restart the server blade. If you changed any settings, select **Save & Exit** menu -- **Save Changes and Exit** to restart the server blade. After the server blade has restarted, the system will automatically start booting from the remote CD/DVD.

Tip

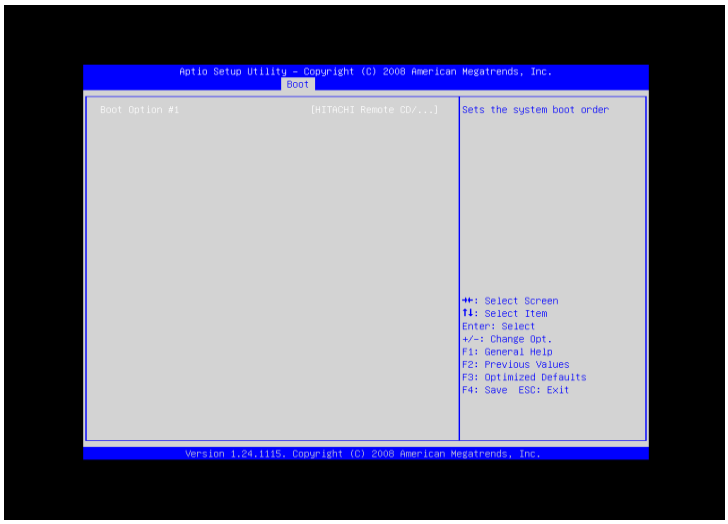
- Booting from a remote CD/DVD may fail if a floppy disk has been inserted in the console terminal's floppy disk drive. In this case, remove the floppy disk and then restart the server blade.
- Remove the CD/DVD drive media from the console terminal after installation.

If HITACHI Remote CD/DVD or HITACHI Remote FD is not listed in the boot options, change the settings as follows. Use of a remote CD/DVD is assumed here:

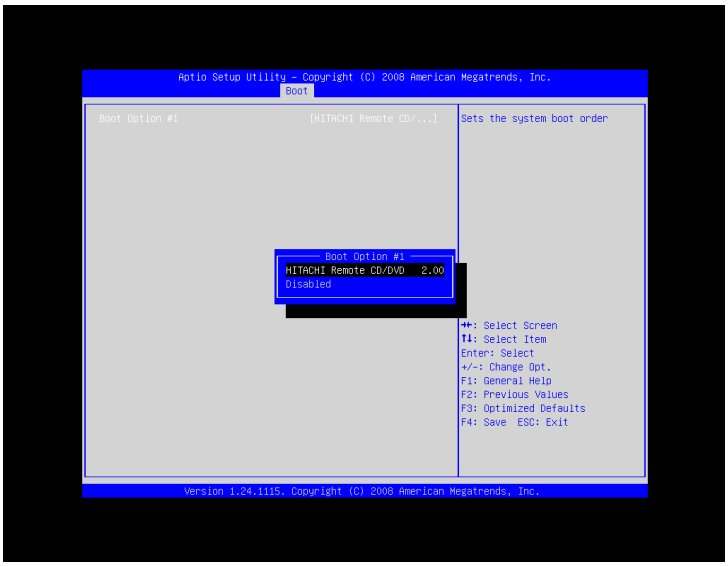
1 On the **Boot** menu, select **CD/DVD ROM Driver BBS Priorities**.



2 The following screen appears. Press **Enter**, and then select **HITACHI Remote CD/DVD**.



Sub-Menu 1



Sub-Menu 2

3 After enabling HITACHI Remote CD/DVD, press **ESC** to return to the **Boot** menu. On the **Boot** menu, set **HITACHI Remote CD/DVD** in **Boot Option #2**.

To boot from a remote FD, select **Floppy Driver BBS Priorities** on the **Boot** menu and then perform the same procedure as above.



After installation is completed, remove the CD/DVD media from the console terminal's CD/DVD drive. Then, choose the **Remote CD/DVD** on the toolbar of the Remote Console Application and **End CD/DVD**. If you use a remote FD, remove the floppy disk from the console terminal's floppy drive, and then choose the **Remote FD** on the toolbar and **End FD**.

Hardware memory dump

Hardware memory dump allows you to collect snapshots from the main memory, CPU registers, and PCI configuration headers without using dump functionalities of operating systems. Correcting dump images is started manually by users. Users can specify a storage device to store collected dump images.

This feature is disabled by default. Users should enable this feature before collecting dump images.



When hardware memory dump is enabled, EFI occupies about 400 MB of main memory.



- When hardware memory dump is enabled, EFI occupies about 400 MB more of main memory than usual (disabled).
- This feature is available with X57A1, X57A2, X55A1(*1), X55A2, X55S3/X55R3(*2), and X55R4 models.

  (*1): X55A1 model needs to have EFI version 03-xx/04-xx applied.
  (*2): X55S3/X55R3 models need to have EFI version 09-32/10-32 or later applied.
- You can usually use this feature only on Redhat Enterprise Linux 5.4 or later without using KVM (Kernel-based Virtual Machine).. If asked to collect hardware memory dump by your reseller, however, you can use the feature on other OSs. On VMware, the feature is available only at VMware startup, when Loading VMware xxxx is displayed or earlier.
- When tboot package is installed, the feature will not work. Change the setting value to the one *described in the Hitachi Compute Blade 2000 Software Guide*.

How to set hardware memory dump

1 Create a dump partition.

Create a disk partition that the server blade can access. The partition, `dump partition`, needs to satisfy the following requirements. Use tools running on the OS, such as fdisk and parted, for creating the dump partition.

#	Item	Requirements
1	Storage device	The storage device needs to support an EFI driver. The storage device needs to be an HDD connected to one of the following mezzanine cards or I/O adapters. Mezzanine card: Hitachi 8 Gb 2-port Fibre-channel mezzanine card Hitachi 8 Gb 2-port Fibre-channel mezzanine card I/O adapter: Hitachi 8 Gb 1-port Fibre-channel adapter Hitachi 8 Gb 2-port Fibre-channel adapter Hitachi 16Gb 1-port fibre channel adapter(*) Hitachi 16Gb 2-port fibre channel adapter(*)
2	File system	FAT 32
3	Partition size	Any size is available. Recommended partition size is about 102% of the physical memory size installed.

(*) For Hitachi 16 Gb fibre channel, the following EFI firmware version is required. Version 11-40/12-40 or higher for standard server blade model, X55R4 Version 07-65/08-65 or higher for high-performance server blade model, X57A2

Create a dump partition with RHEL 5

(1) Create a partition using fdisk,

```
fdisk /dev/sdx
```

Steps:

(d) Delete the area.

(n) Create a new area (primary partition 1).

(t) Change the area system ID to `W95 FAT32 (LBA).`

(w) Write the table in the disk to end.

(2) Format the partition with FAT32.

```
mkdosfs -n LABEL -F 32 /dev/sdx1
```

LABEL: any volume label (up to 11 American Standard Code for Information Interchange (ASCII) characters)



- The size of disk partitions available is 1.9 TB or less due to the restriction on the FAT32 supported by the EFI firmware.
- Create a dump partition on a dedicated logical unit (LU). Do not create any other partition on the same LU.
- With both Linux Tough Dump and a dump partition, re-perform the command mkdosfs to format the partition and set a volume label even if the dump partition has already been formatted. If a volume label is set with a command other than the command above, the volume label may not be correctly displayed in the EFI setup menu described later.



- Note that if the dump partition does not have enough free space for the dump file, the part of the dump file beyond the free space size is discarded. Since dump files are not automatically deleted, the user needs to properly delete some for maintenance.
- An area, where memory pages are the default value (all: 0x0) at hardware memory dump, is not saved in the dump file.
- We recommend that you set a distinguishable name on the volume label of a dump partition.
- It is recommended that a dump partition be connected to a path different from the boot path.
- When there are multiple dump partitions or multiple paths are connected to a dump partition, a device that is recognized first at the EFI boot will be a dump partition.

2 Create a file for identifying the dump partition.

You need to place a file on the root directory of the dump partition so that the system can identify the dump partition. Only one partition among partitions connected to the system is available as a dump partition. Create and place a file for identification according to the table below.

File name	DumpSignature.dat
Size	16 bytes
Data (in binary format)	B4 91 61 32 6E C0 A4 23 C3 75 55 15 37 55 A6 1D

3 Check the host bus adapter (HBA**)** BIOS settings.

Check the following when an HBA port is connected to an LU that contains a dump partition..

- HBA BIOS is Enabled.

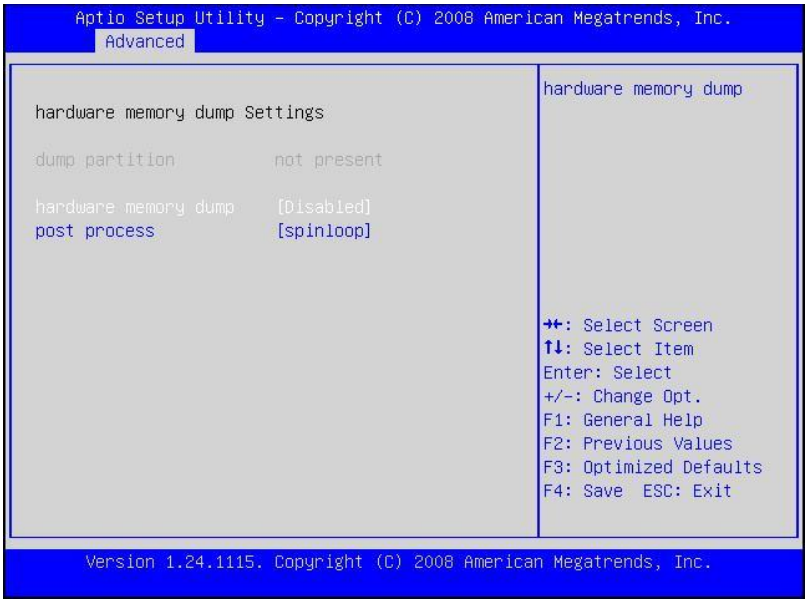
  See “Procedure to set a HBA-BIOS to Enable” in the *Hitachi Gigagbit Fibre Channel Adapter User’s Guide (BIOS/EFI Edition)* for detailed procedures .

- The LU with a dump partition is registered in Boot Priority.

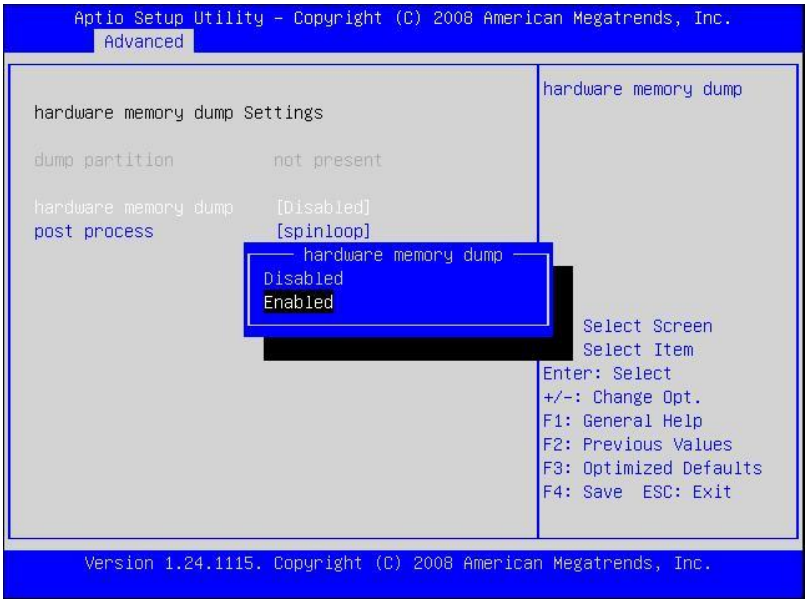
  See “Procedure to set a Boot Priority” or “Procedure to set a Boot Priority manually” in the *Hitachi Gigagbit Fibre Channel Adapter User’s Guide (BIOS/EFI Edition)* for detailed procedures.

4 Enable the hardware memory dump.

Enter the EFI setup menu and select **hardware memory dump Settings** to display the setting screen.



Select **hardware memory dump** and then select **Enabled** in the subscreen.

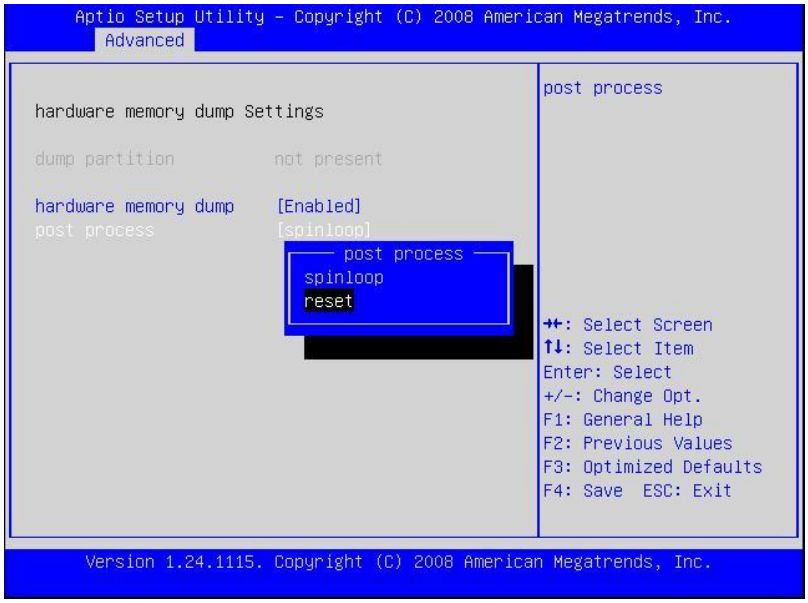


5 Specify the post process of the hardware memory dump.

Select **post process** and specify a setting suitable for your environment.

Spin Loop: Halts after the dump.

Reset: Resets automatically and reboots the server blade after the dump.



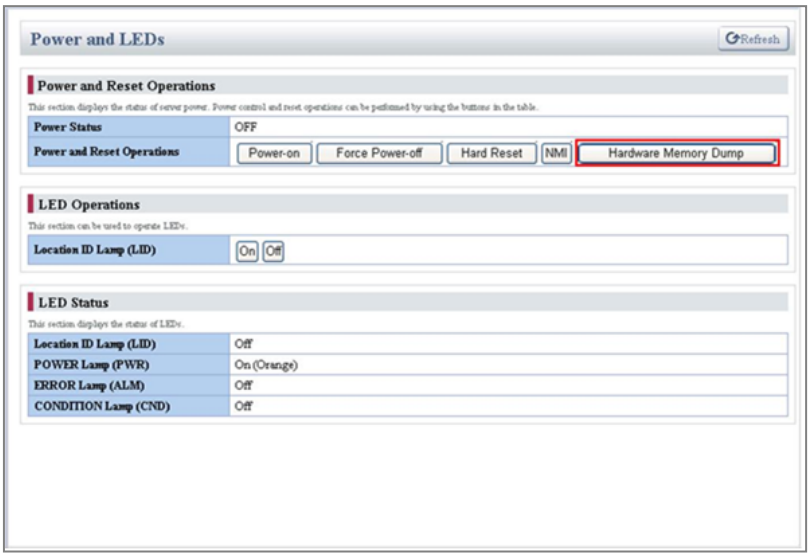
6 Save the settings and reboot the server blade.

To check if the dump partition is properly identified: Select **hardware memory dump Settings** under the **Advanced** tab in the EFI setup menu after rebooting the server blade. Check that the volume label of the target dump partition is displayed in **dump partition**.

How to start hardware memory dump

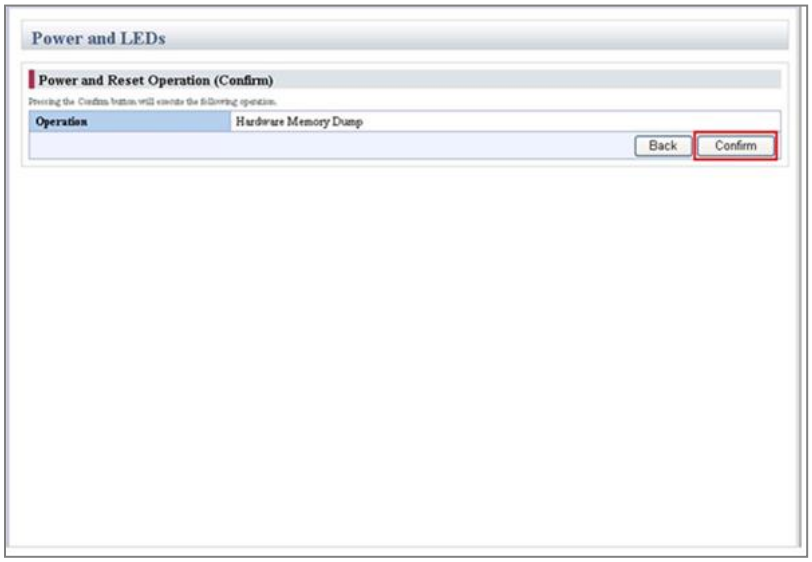
Hardware memory dump is performed in the Power and LEDs screen under the server operation tab of the server blade web console.

1 In the **Power and LEDs** screen, click **Hardware Memory Dump**.



2 In the **Power and LEDs (Confirm)** screen, click **Confirm**.

Hardware memory dump will start.





- This operation only gives a command to start hardware memory dump. Then the server blade Web console responds and returns to the Power and LEDs screen before the dump is complete.
- To check the dump progress, use the OS console to the target server blade for X55R3/X55S3 models; use the remote console to the target server blade for other models.

3 Check the progress and completion of the hardware memory dump.

When the hardware memory dump is started, the following screen is displayed in the remote console or OS console.

```
hardware memory dump Entry.
Dump partition found.
Cpu registers dump Done.
Pci registers dump Done.
Memory manifest dump Done.
Memory data dump Start.
   2752512 pages /  134182815 pages (  2%)
```

The following is a rough estimated time required for a dump:

About 4 minutes per 2 GB dump file size.

Required time for dump depends on the write performance of the storage.

When the dump is successfully completed, “hardware dump complete” is displayed. After the dump is complete, the operation set in **Post process** of the EFI setup menu is executed.



- When the dump partition does not have enough free space for the dump file, a message appears and the dump is stopped when free space runs out.
  Once the dump is stopped, it cannot be resumed.
- If hardware memory dump process has aborted, data on the dumped images might be corrupted.
- When executed in the virtual environment, hardware memory dump may not work properly. Check system event logs about whether hardware memory dump has been executed or not. If “IPMI WDT Timeout (BIOS)” is displayed after “Issue INIT for HardwareDump” or if “HardwareDump Start” is not displayed in the system event log, the hardware memory dump might not have worked properly.
-

Where hardware memory dump is stored

Hardware memory dump data will be stored as a file in the directory on the dump partition.

Directory structure		Content
/HDUMP_YYMMDD_hhmm/	register.dat	Processor Registers
	pci.dat	PCI Config Header
	manifest.dat	Memory Manifest
	memory_[1st page address].dat (*) (*) Address in hex; in the unit of 4 Kbyte	Memory Data



Dump files are not be automatically deleted. Delete them manually if necessary.

MegaRAID WebBIOS

The system equipment with serial attached SCSI (SAS) internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y can set a disk array using the MegaRAID WebBIOS utility.

Under normal operation, you do not need to change the settings.

Setting is required only if you need to change the system configuration, for example, when you have changed hard disks. It is not necessary for the system configuration to be changed for usual operation.

Make sure to operate MegaRAID WebBIOS in accordance with descriptions in this manual, because it might not work properly. Do not execute the operation other than described in this manual.



When using a mouse in MegaRAID WebBIOS operations, change the setting for the mouse of the remote console to Relative mode.

Change the mode to Relative mode referring to Mouse mode settings for the remote console before starting MegaRAID WebBIOS.



When using the boot from an external storage, disable the boot from MegaRAID WebBIOS.

Referring to BIOS settings for SAS internal RAID board, change the controller BIOS setting to Disabled.



- When booting from an external storage, disable the boot from MegaRAID WebBIOS.
  See the following to change the Controller BIOS to Disabled:
  With MegaRAID SAS 1078, see BIOS settings for SAS internal RAID board.
  With MegaRAID SAS 2108, see BIOS settings for SAS internal RAID board.
  With MegaRAID SAS 2208, see BIOS settings for SAS internal RAID .
- Connect a mouse to the remote console before starting MegaRAID.

SAS RAID controller

The following three types of SAS RAID controllers can be installed in the system unit.

- MegaRAID SAS 1078 (model: GVX-CA2SRD2X1)
- MegaRAID SAS 2108 (model: GVX-CA2SRD4X1)
- MegaRAID SAS 2208 (CB2000 standard server blade: X55R3 model)

This section describes MegaRAID WebBIOS per SAS RAID controller type.

See one of the two that are installed on your system.

MegaRAID SAS 1078

❑ Starting and ending MegaRAID WebBIOS

Use the following procedure to start the MegaRAID WebBIOS.

1 Turn on the power supply to the system equipment.

2 When the following screen appears, press and hold the **Ctrl** key and press the **H** key.

The MegaRAID WebBIOS is started.

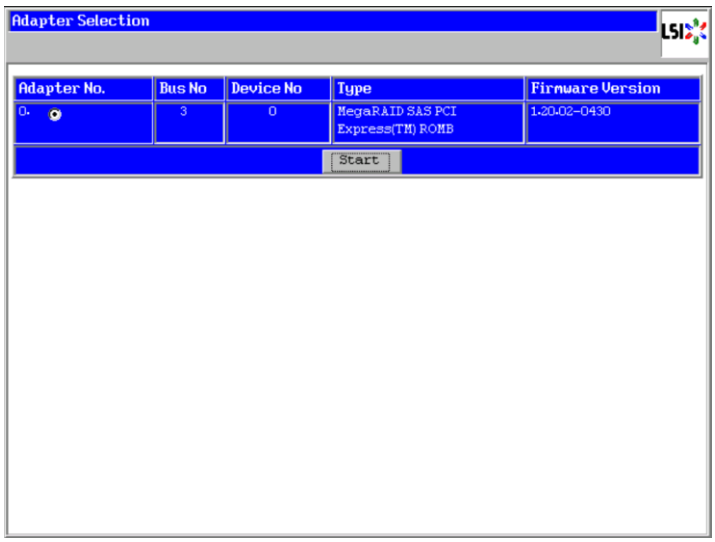
```
LSI MegaRAID SAS-MFI BIOS
Version x.xx.xx (Build xxx xx, xxxx)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus x Dev x) MegaRAID SAS PCI Express(TM) ROMB
FW package: x.x.x-xxxx


x Virtual Drive(s) found on the host adapter.

x Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS
```

If the operating system has been started before you press the keys, shutdown the operating system and then restart the system equipment. Check the manual for ending your operating system because some operating systems, such as Windows, require shutdown and other special operations when the particular operating system is terminated.

3 The MegaRAID WebBIOS is started and the **Adapter Selection** menu appears.



4 Press the **Ctrl** key once.

Note

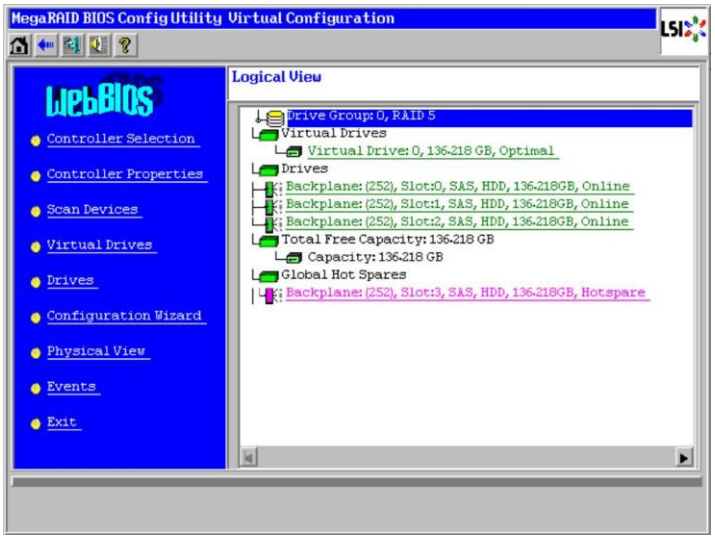
If you do not press the **Ctrl** key, your keyboard and mouse may not operate properly.

If the keyboard or mouse is not available when you operate MegaRAID WebBIOS, press the **Ctrl** key once.

5 Press **Enter** once.

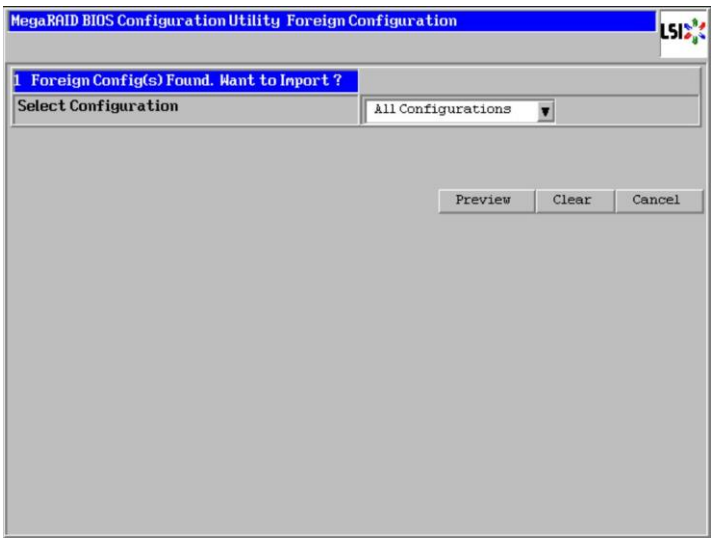
Without pressing **Enter**, the mouse will not work properly.

The main menu is displayed.



Tip

If a hard disk which has different disk array configuration coming from the record in the disk array controller board exists, the following screen is displayed. See Disk with a foreign configuration for more details.



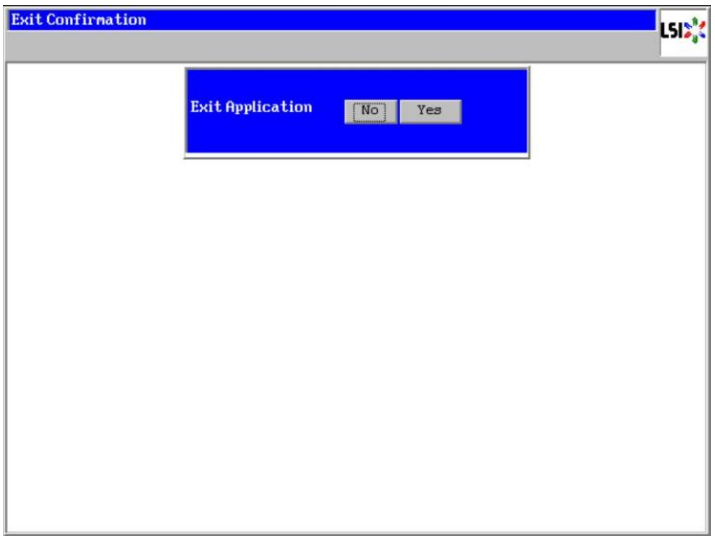
Use the following procedure to end the MegaRAID WebBIOS.

1 From the main menu, click **Exit**.

The exit confirmation screen appears.



When you want to return to the main menu, click Home or  .



2 Click **Yes**.

Clicking **No** returns you to the main menu.

3 When the following message appears, power off the system equipment or with the remote console application (Reclient), click the **C+A+D** button in the toolbar of the system console; with the remote console application (Java application), click **Keyboard > (Ctrl+Alt+Del)** in the toolbar or press the **Alt+L** keys to restart the system equipment.



Tip

For the remote console (Reclient), see the *Hitachi Compute Blade 2000 Remote Console Application User's Guide* contained in the remote console application CD attached to the system equipment.

For the remote console (Java application), see "Remote Console Application (Java Application)" in Chapter 3.

❑ Operation for MegaRAID WebBIOS

For MegaRAID WebBIOS, you can set individual items by using the following keys.

Connect a mouse to the remote console before starting MegaRAID WebBIOS.

Key/mouse	Operation
Mouse	Moves the mouse cursor.
Mouse - left button	- Selects an item that the mouse cursor is placed on. - Moves the cursor to an item to which the mouse cursor points. - Selects a disk array or physical hard disk.
0 to 9	Enables you to enter numerical values.
Ctrl	Selects multiple disk arrays or hard disks.
Del, Back Space	Deletes an entered value.

❑ Key operation for MegaRAID WebBIOS

This section describes how to operate the MegaRAID WebBIOS using only the keyboard.

Operating MegaRAID WebBIOS with keyboard

You can set the following items for MegaRAID WebBIOS using the keyboard.

Key	Operation
Tab	Moves the cursor in order. *1
Shift + Tab *2	Moves the cursor in reverse order.
Enter, Space	- Selects the item that the cursor is put on. - Determines an item setting. - Determines a disk array or physical hard disk.
[↑], [↓]	- Selects a disk array or physical hard disk. - Selects a setting value.
Shift	Selects multiple disk arrays or hard disks.
0 to 9	Inputs a numerical value.
Del, Back Space	Deletes an entered value.

*1 The item selected by the cursor is encircled by the dotted line.

*2 **Shift + Tab** is to press the **Tab** key while pressing the **Shift** key.



It may be hard to find the cursor on some screens. In this case, press the **Tab** key or **Shift + Tab** keys to move the cursor to a position where you can find it, and then move the cursor to the position for the operation to perform.

Screen composition for MegaRAID WebBIOS

The main menu of the MegaRAID WebBIOS utility includes the Menu Icon, which is not used in operation with the keyboard.

Operation in MegaRAID WebBIOS setting/disk array configuration

When operating MegaRAID WebBIOS only with the keyboard, replace the mouse with the keyboard as follows:

- Click (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.
- Put a check mark in (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.

Execute a specific operation when setting or configuring a disk array, as follows:

- Select **Menu > Logical View > Physical View** in the main menu:

  Press the **Tab** key or press the **Tab** key while pressing the **Shift** key to move the cursor among **Menu**, **Logical View**, and **Physical View**.
  - When displaying the main menu, press the **Tab** key once to move the cursor to **Controller Selection** that is selected.
  - Move the cursor to **Exit** using the **Tab** key. With the cursor on **Exit**, press the **Tab** key once. The cursor moves to **Logical View** or **Physical View**.
  - With the cursor on **Logical View** or **Physical View**, press the **Tab** key twice. The cursor moves to **Controller Selection**.

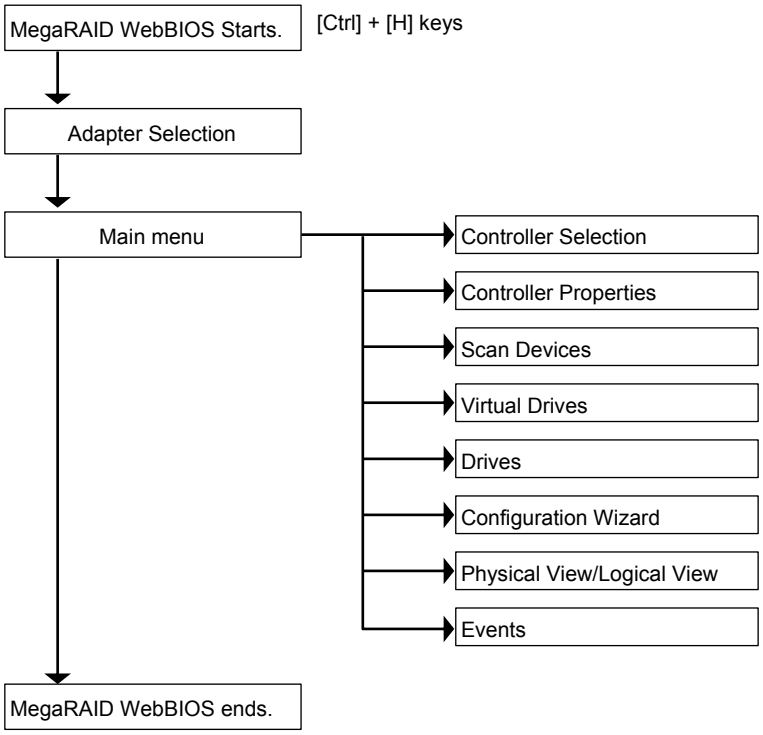


You can select a hard disk or disk array using the [↑] and [↓] keys on the selection screen of Logical View or Physical View.

- Setting items in each menu.
  To change a setting value, put the cursor on the setting item box and select a new setting value using the [↑] and [↓] keys or enter the setting value using the numerical keys.
- Selecting multiple hard disks in disk array configuration.
  Press and hold the **Shift** key and select hard disks using [↑] and [↓] keys, and then press **Enter** or **Space** key.

❑ Configuration of MegaRAID WebBIOS

The MegaRAID WebBIOS is configured as shown below.

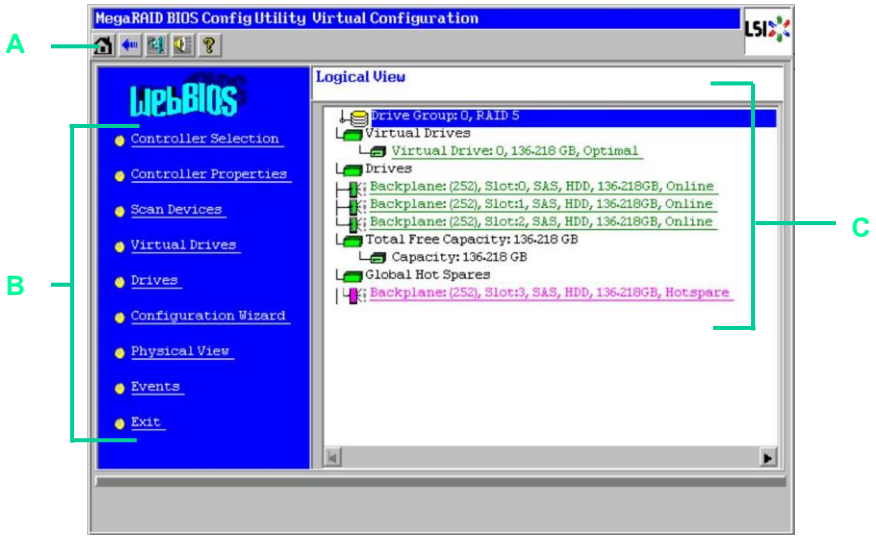


Tip

Adapter Selection is displayed on the Controller Selection window.

❑ Screen configuration of MegaRAID WebBIOS

The MegaRAID WebBIOS screen configuration is shown below.



A Menu icon

The following icons are available.

Icon at the upper left on the screen	Operation from an icon click
	Return to the main menu.
	Return to the previous screen
	End the utility.
	Temporarily stop ringing the buzzer on the disk array controller board. *1
	Display the version of MegaRAID WebBIOS,

*1 This function is not supported.

B Menu

Menu items for MegaRAID WebBIOS are displayed. Click each item to go to the respective menu screen.

C Logical View/Physical View

Hard disks or disk arrays connected to the disk array controller are displayed.



Click a hard disk from disks displayed in Logical View or Physical View. The same screen is displayed as when you select Virtual Drives > Properties from the menu.

Select a disk array from disks displayed in Logical View. The same screen is displayed as when you select Drives > Properties from the menu.

❑ Setting items for MegaRAID WebBIOS

This section describes the setting items and values for MegaRAID WebBIOS.

- The same alphanumeric characters are used to associate the setup screen and each of the items.
- In the table, the underlined values are Default values. Those in brackets [ ] are recommended values.

  Example:

  [Enabled (valid)]/Disabled (invalid): "Enabled" is the Default and also the recommended value.

  [Enabled (valid)]/Disabled (invalid): "Disabled" is the Default value; and "Enabled" is the recommended value, which requires a setting change.

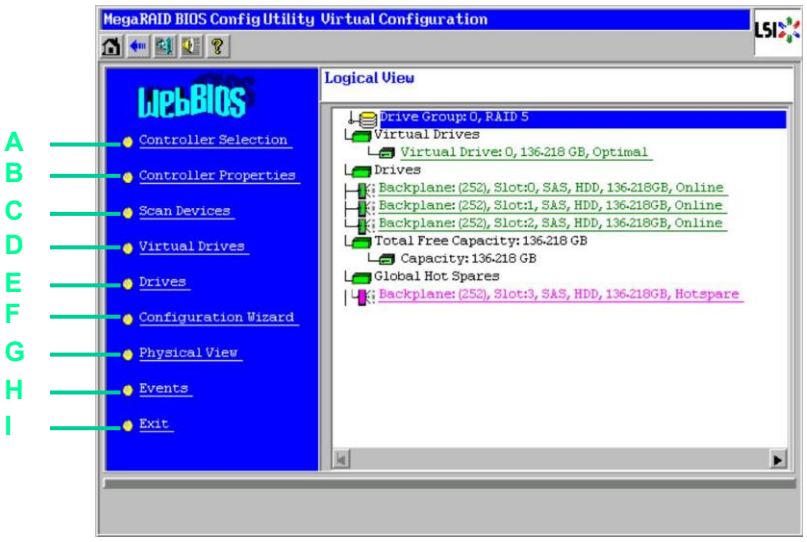
  When you need to change the setting from the Default to the recommended value, the recommended value is emphasized in red.



Unless otherwise specified, use the recommended values for all setting items. If you set non-recommended values, the equipment would not be supported and might not operate properly.

Main menu

Start MegaRAID WebBIOS. The following main menu appears.



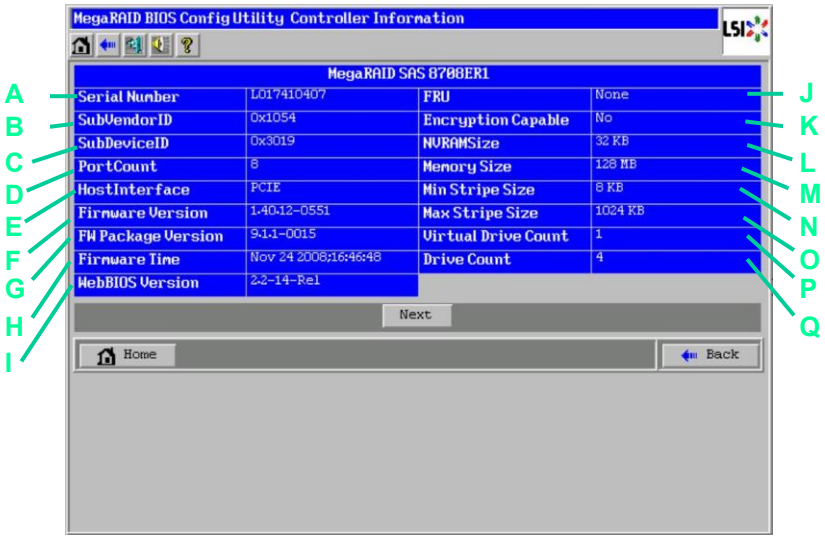
Menu		Content	Setting/display value
A	Controller Selection	Selecting the disk array controller to be operated	-
B	Controller Properties	Viewing and setting the hardware information on the disk array controller board	See Controller properties: menu for setting the disk array controller board.
C	Scan Devices	Scanning the installed devices	-
D	Virtual Drives	Viewing and setting the disk array (logical drive) information	See Virtual Drives: Viewing and setting disk array information.
E	Drives	Viewing and setting the hard disk (physical drive) information	See Drives: Viewing physical hard disk information.
F	Configuration Wizard	Building or formatting disk arrays	See Building disk arrays.
G	Physical View/Logical View	Switching display modes	See Switching the display mode.
H	Events	Displaying events	-
I	Exit	Ending the MegaRAID WebBIOS	See Ending procedure in Starting and ending MegaRAID WebBIOS.

Tip Do not use Events because Event is not supported.

Controller properties: menu for setting the disk array controller board

You can display and set the hardware information about the disk array controller board.

Select **Controller Properties** from the main menu, and the following screen appears.



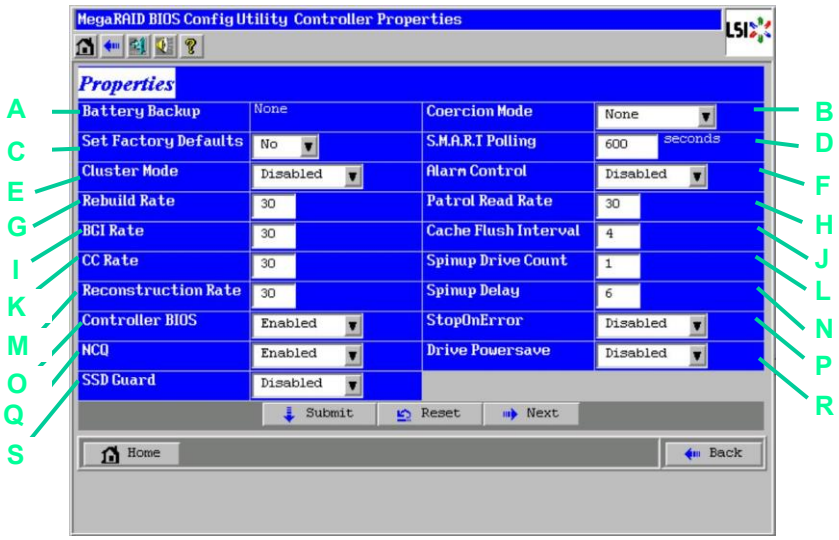
Display item		What is displayed
A	Serial Number	Serial number
B	SubVendorID	Sub-vendor ID
C	SubDeviceID	Sub-device ID
D	PortCount	Number of ports installed
E	HostInterface	Host interface
F	Firmware Version	Firmware version
G	FW Package Version	Firmware package version
H	Firmware Time	Current time at which firmware is acquired
I	WebBIOS Version	MegaRAID WebBIOS version
J	FRU	Board names per maintenance
K	Encryption Capable	Encryption function: Enable or Disable
L	NVRAM Size	Size of NVRAM installed
M	Memory Size	Size of memory installed
N	Min Stripe Size	Minimum stripe size
O	Max Stripe Size	Maximum stripe size
P	Virtual Disk Count	Exisiting number of array configurations (logical devices)
Q	Physical Disk Count	Number of physical devices installed

Tip

You cannot change the settings for those items displayed here.

Properties: Controller properties submenu 1

Click **Next** in the **Controller Properties** screen, and the following screen appears.



Display item		Display/content	Setting/display value **
A	Battery Backup	Battery backup unit mount status.	None
B	Coercion Mode *1	Setting the capacity control for the physical hard disk used for disk array building	[None (using the entire capacity)] / 128 MB way (using a capacity as a multiple of 128 MB) / 1 GB way (using a capacity as a multiple of 1 GB)
C	Set Factory Defaults *2	Returning all the settings to their Default values	—
D	S.M.A.R.T Polling *4	Setting the interval of Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T.) reporting	0 to 65535 / 300 / [600]
E	Cluster Mode *3	Setting the cluster mode	[Disabled (invalid)] / Enabled (valid)
F	Alarm Control	Sounding the buzzer on the controller in the event of a fault at a connected device	[Disabled (not sounding)] / Enabled (sounding) / Silence (stop sounding temporarily)
G	Rebuild Rate *3	Priority of rebuilding	0 to 100 / [30]
H	Patrol Read Rate *3	Priority of patrol reading	0 to 100 / [30]
I	BGI Rate *3	Priority of background initializing	0 to 100 / [30]
J	Cache Flush Interval *3	Flash timing for write-cache data	1 to 255 / [4]
K	CC Rate *3	Priority of integrity inspection	0 to 100 / [30]
L	Spinup Drive Count *4	Number of hard disk motors started at system startup	0 to 8 / [1]
M	Reconstruction Rate *3	Priority of capacity expansion	0 to 100 / [30]
N	Spinup Delay *4	Timing for hard disk motors started at system startup	0 to xxx / [6]
O	Controller BIOS *3	Validating the BIOS for the disk array controller	[Enabled (valid)] / Disabled (invalid)

Display item		Display/content	Setting/display value **
P	StopOnError *3	Setting whether to start the operating system in the event of a fault at system startup	[Disabled (booting)] / Enabled (not booting)
Q	NCQ *3	Enabling or disabling the native command queuing (NCQ) command	[Enabled (valid)] / Disabled (invalid)
R	Drive Powersave *3	Setting the saving mode to a hard disk	[Disabled (invalid)] / Enabled (valid)
S	SSD Guard *4	Setting the solid state drive (SSD) Guard function	[Disabled (invalid)] / Enabled (valid)

*1 This can be changed only when no disk arrays have been set.

*2 Do not use **Set Factory Defaults**. This setting must be changed to the recommended values.

*3 Always use the Default setting.

*4 Always use the recommended values.

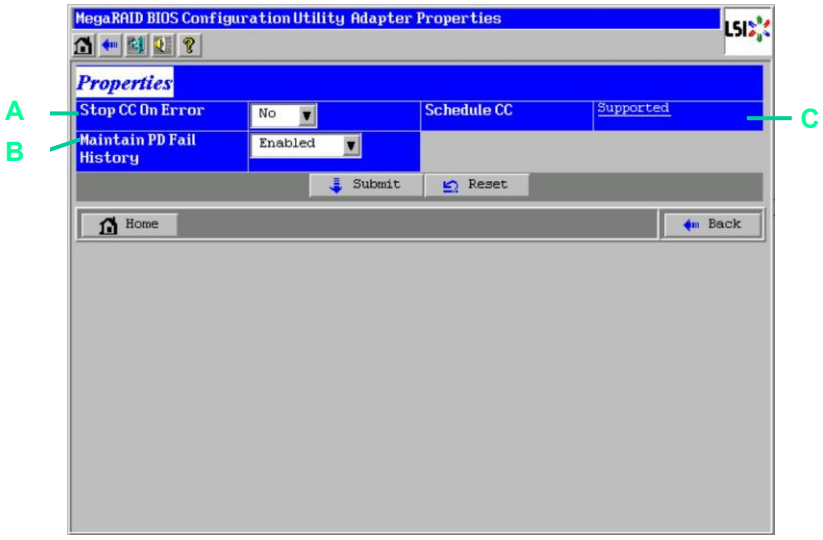


Place the mouse cursor on a setting item and left-click the mouse to change the setting values. Or, left-click the mouse to move the cursor and enter a value from the keyboard. Click **Submit** after making the setting.

Properties: Controller properties submenu 2

Click **Next** in the **Properties: Controller properties submenu 1** screen and the following screen appears.

> ***Notice***
>
> This setting item is not supported. Do not use this setting.

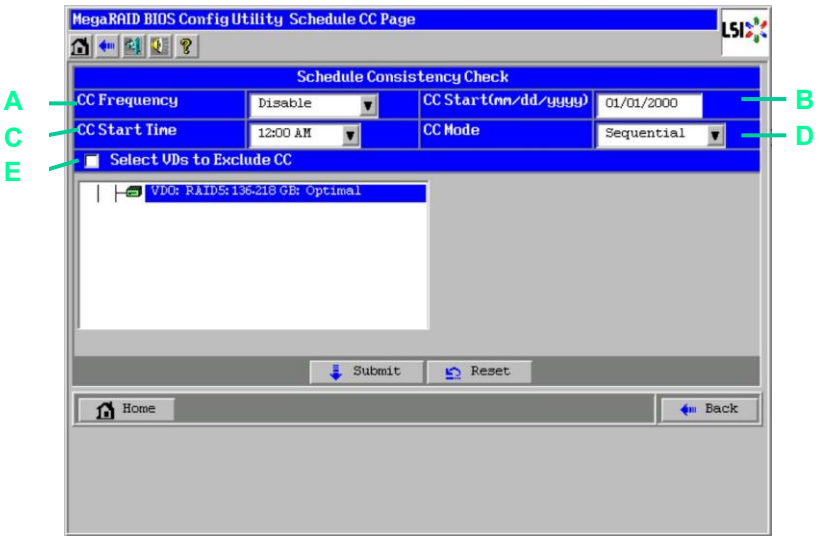


Setting item		Description	Setting/display value **
A	Stop CC On Error	Sets an operation when an error is detected at the consistency check (CC).	[No (continuous operation)] / Yes (stops the consistency check.)
B	Maintain PD Fail History	Sets whether or not a failed hard disk can be used.	[Enabled (Registers failed hard disk information.)] / Disabled (Not register failed hard disk information.)
C	Schedule CC	Sets a consistency check schedule.	When clicking [Supported], the screen moves to “Schedule CC Page: Schedule Consistency Check setting submenu”.

Schedule CC Page: Schedule consistency check setting submenu

Click **Supported** of Schedule CC in the **Properties: Controller Properties submenu 2** screen, and the following screen appears.

> ***Notice***
>
> This setting item is not supported. Do not use this setting.

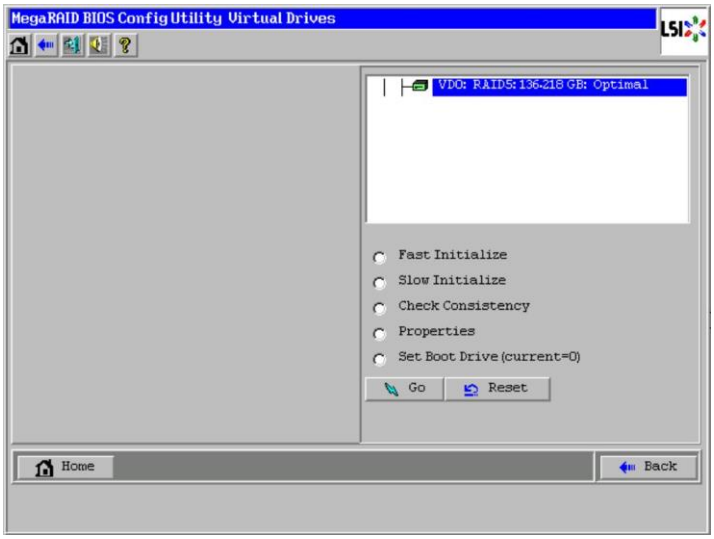


Setting item		Description	Setting/display value **
A	CC Frequency	Sets the consistency check schedule function: Enable or Disable	[Disable (invalid schedule)] / Enabled (valid schedule)
B	CC Start (mm/dd/yyyy)	Sets on what date the consistency check starts.	Choose any date.
C	CC Start Time	Sets on what time the consistency check starts.	12:00 AM. to 11:00 PM. / [The nearest to the present time]
D	CC Mode	Sets if the consistency check is executed on multiple disk arrays.	[Sequential (a consistency check per array)] / Concurrent (a consistency check on multiple arrays)
E	Select Virtual Drives (VDs) to Execute CC	Specifies a disk array on which the consistency check is executed.	Choose any array configuration.

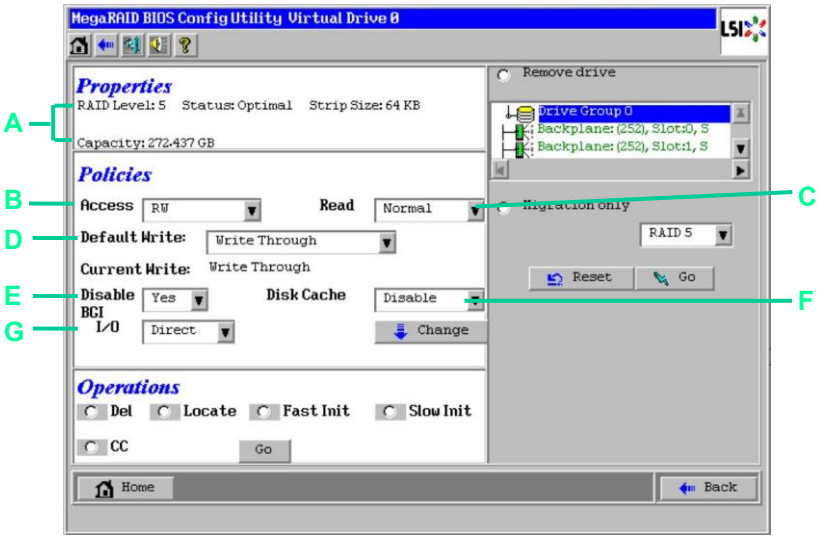
Virtual Drives: Viewing and setting disk array information

You can display and change the information on the disk array (logical drive) that is already set.

Select **Virtual Drives** in the main menu, and the following screen appears:



Select a disk array for viewing information and changing the setting from the list on the upper right of the screen. Check **Properties** and then click **Go**, and the disk array properties screen appears.



Display item		What is displayed	Setting/display value **
A	RAID Level	RAID level	-
	Status	Status of the disk array	-
	Capacity	Size of the disk array	-
	Strip Size	Stripe size of the disk array	-
B	Access *1	Access mode	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
C	Read	Read policy	[Normal (no advance reading)] / Ahead (always advance reading) / Adaptive (advance reading only in the event of sequential access)
D	Default Write *2 *3	Setting the write cache	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)
E	Disable BGI *1	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
F	Disk Cache *1	Setting the cache installed in a physical hard disk	[Disable (cache: not used)] / [Enable (cache: used) / No change (based on the hard disk setting)]
G	I/O *1	Setting the read-cache operation	[Direct (reading from the cache at a cache hit)] / [Cached (always reading from the cache)]

*1 Make sure to set the default value or recommended value to use this item.

*2 Default Write supports setting in Always Write Back only when the system equipment is connected to an uninterruptible power supply (UPS). Even so, set **Write through** when installing OS because the installation might not finish properly.

*3 Do not select **Write Back with BBU**.

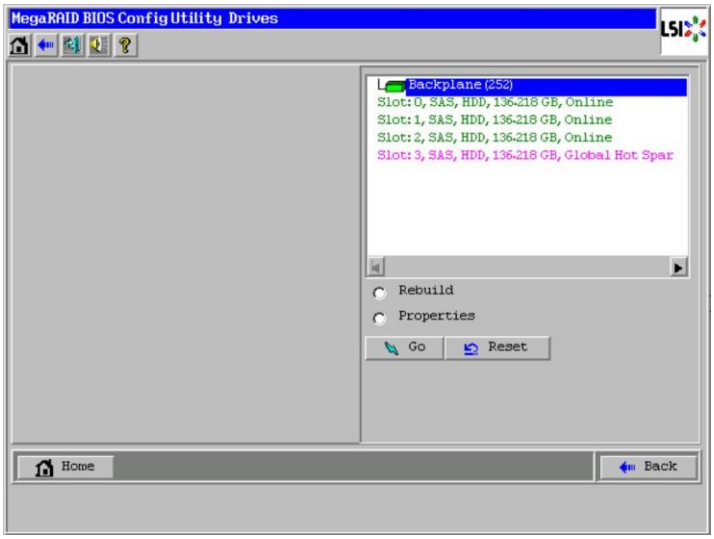
NOTICE

When enabling the write cache of the disk array, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Drives: Viewing physical hard disk information

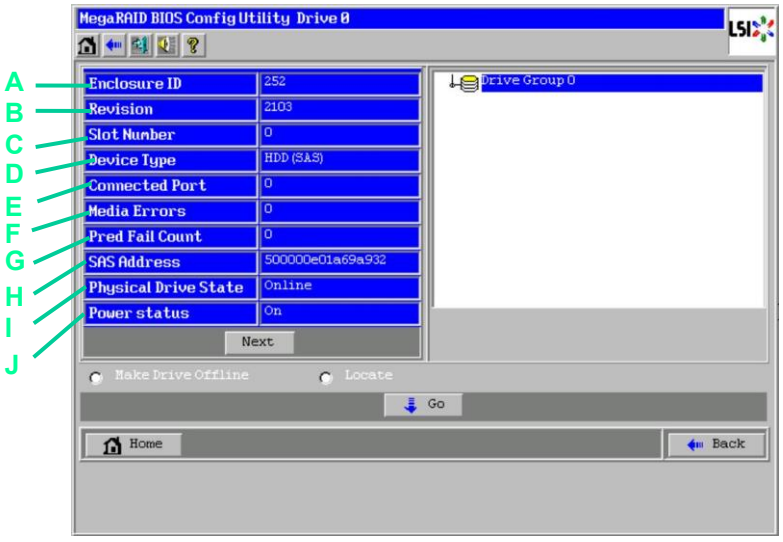
Here you display the information on the physical hard disk in the physical drive connected to the disk array controller.

Select **Drives** in the main menu and the following screen appears:



Select a disk array for viewing and setting information from the list on the upper right of the screen. Check **Properties** and then click **Go**. The following screen appears.

Hard disk property menu 1



Display item		What is displayed
A	Enclosure ID	ID number of the enclosure device connected
B	Revision	Firmware version
C	Slot Number	Number of the slot installed
D	Device Type	Device type
E	Connected Port	Port number of the disk array controller board connected
F	Media Errors	Number of media errors detected
G	Pred Fail Count	Number of S.M.A.R.T. warnings reported
H	SAS Address	SAS address
I	Physical Drive Status	Physical hard disk status
J	Power Status	Power Status

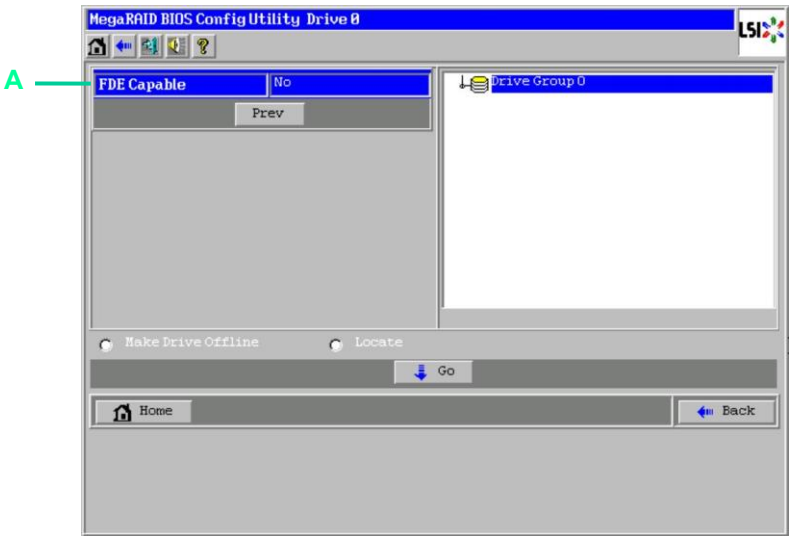
Tip

Items described in the table above cannot be changed.

For the status of the physical hard disk, see Status.

Media Errors and Pred Fail Count are cleared when the system power is turned off.

Hard disk property menu 2



Display item		What is displayed
A	FDE Capable	Full Disk Encryption: Capable or No

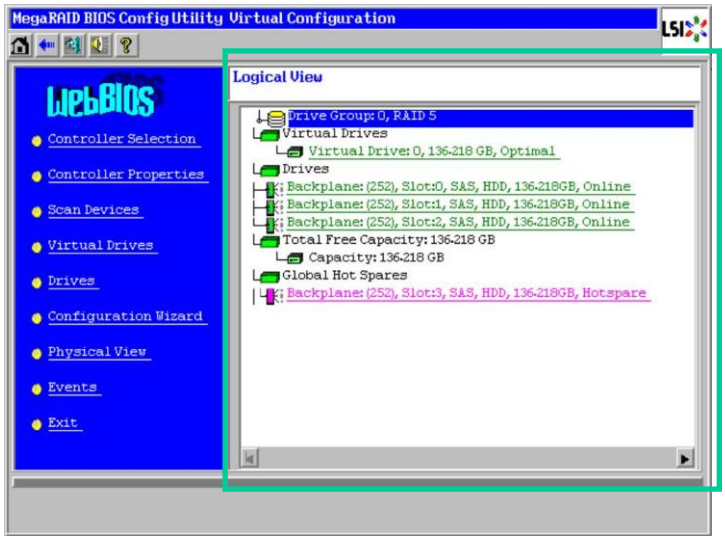
Tip

Items in the table above cannot be changed.

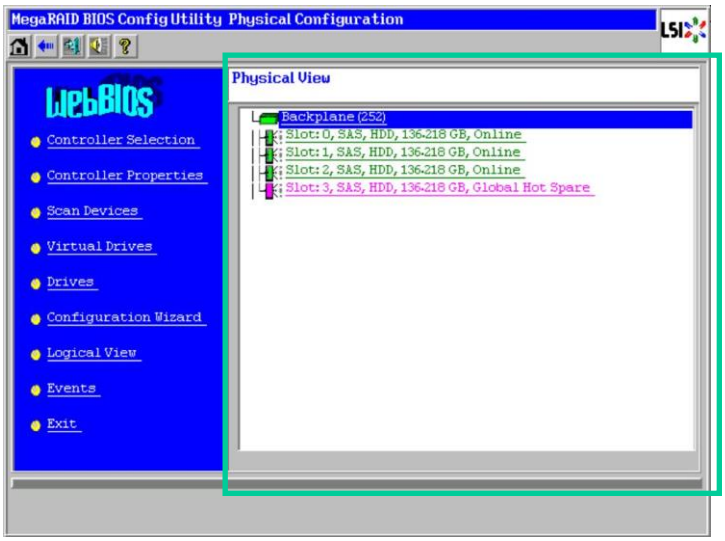
❑ Switching the display mode

This section describes switching disk array display modes in the main menu.

There are two types of display mode: Logical View and Physical View.
Logical View mode displays a list of disk array configurations that are already set.
Physical View mode displays a list of physical hard disks comprising of a disk array configuration.



Logical View mode:
Disk array configuration



Physical View mode:
Disk array configuration

Tip

- The Logical View mode is applied when the MegaRAID WebBIOS is started.
- To switch to the physical view mode, click **Physical View** in the Logical View mode from the main menu.
- To switch to the logical view mode, click **Logical View** in the Physical View mode from the main menu.

Building disk arrays

This section describes the procedure for building disk arrays.

The building of disk arrays should be entirely performed from the Configuration Wizard.

> ***NOTICE***
>
> You must not change the disk array during system operations. If you do, all data will be lost from those disks due to change in the disk array.

Note

Make sure to set each item in the recommended value unless other specific directions are given. Otherwise, the system may not properly operate. Hitachi Data System is not responsibile for a malfunction due to changed settings other than our recommended values.

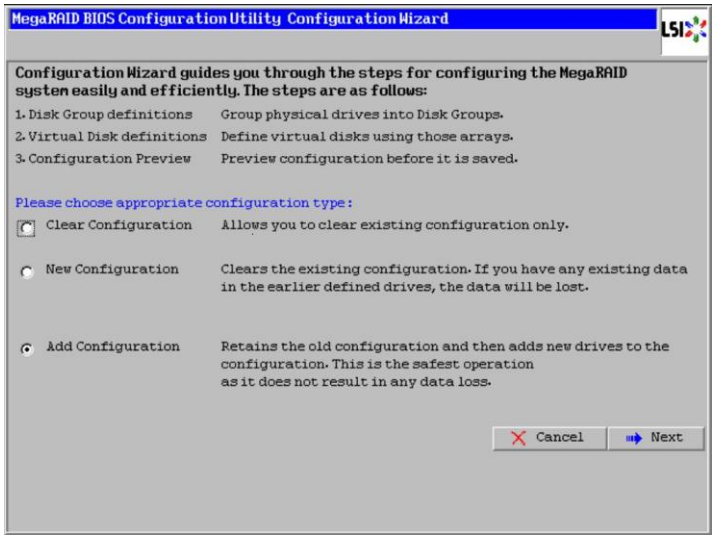
Building disk arrays for RAID 0, 1, 5, and 6

This section describes the procedure for building new disk arrays for Redundant Arrays of Independent Disks (RAID) 0, 1, 5, and 6.

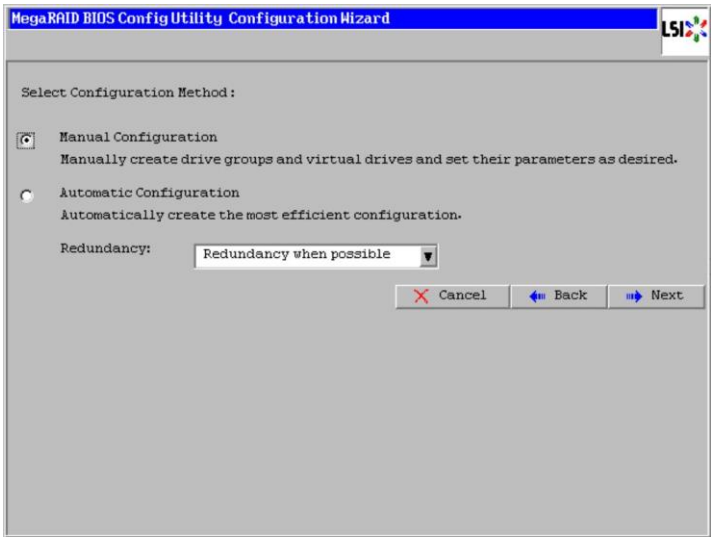
Tip

To build RAID 10, see Building disk arrays for RAID 10. For information about how to set hotspare, see Setting hotspares.

1 Select **Configuration Wizard** from the main menu. The following screen appears.



2 Check **New Configuration** or **Add Configuration**, and click **Next**. The following screen appears:



> ***NOTICE***
>
> If you select New Configuration, all data in those hard disks including the disk array information will be lost. Backup your required data before selecting New Configuration.

Tip

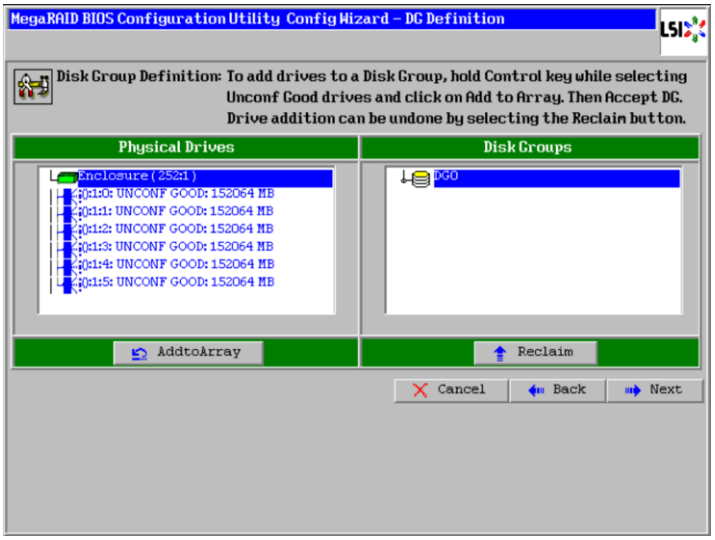
The existing disk arrays will remain when you select **Add Configuration**. Add Configuration should be selected when you want to keep the existing disk arrays, and to build disk arrays using additional hard disks.

If you select **New Configuration**, you lose the existing disk arrays. This should be selected when you discard the existing disk array and build a new one.

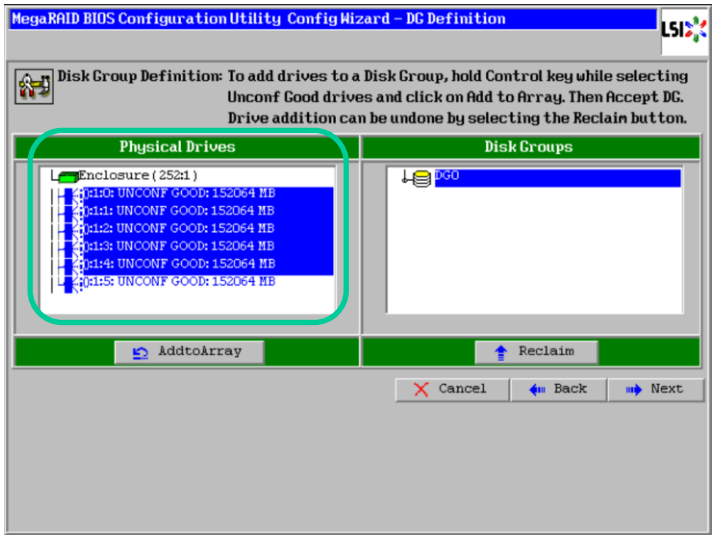
If you select **New Configuration**, the following screen appears first. Clicking **Yes** allows you to build a disk array.



3 Check **Custom Configuration**, and click **Next**. The following screen appears:



4 Select a hard disk to be used for building a disk array.



The number of hard disks required varies depending on the RAID level to be set. The following table summarizes the number of hard disks required.

RAID level	Number of hard disks required
RAID 0	1 or more
RAID 1	2
RAID 5	3 or more
RAID 6	4 or more

Note

RAID 6 with three hard disks is not supported because the system may not operate properly.

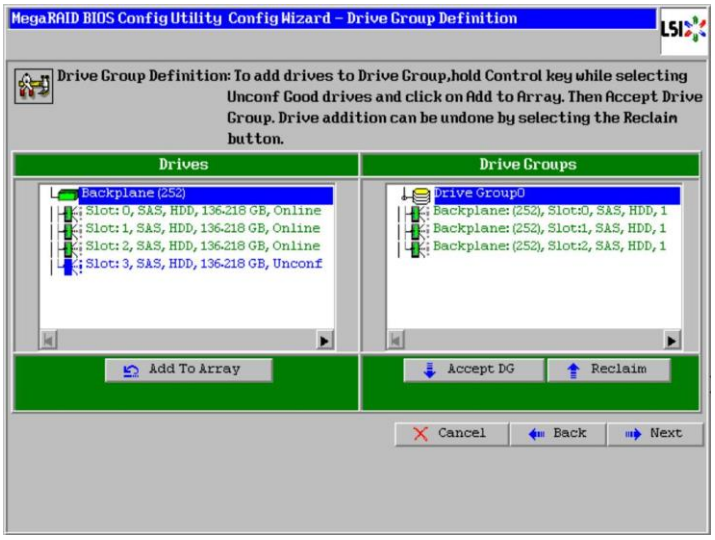
Tip

You can select only a hard disk whose status is Unconfigured Good (unused).

To select multiple hard disks, click them while pressing the **Ctrl** key.

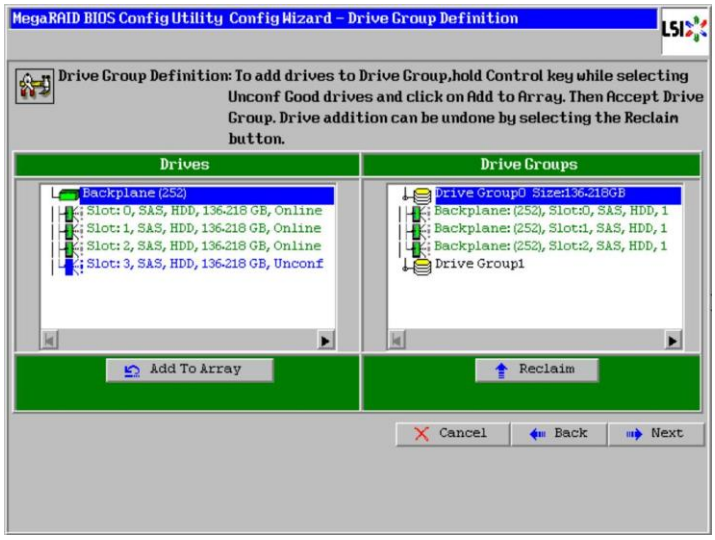
5 After selecting all hard disks for building a disk array, click **Add to Array**.

Status of those selected hard disks is **Online** as shown in the **Drives** pane.

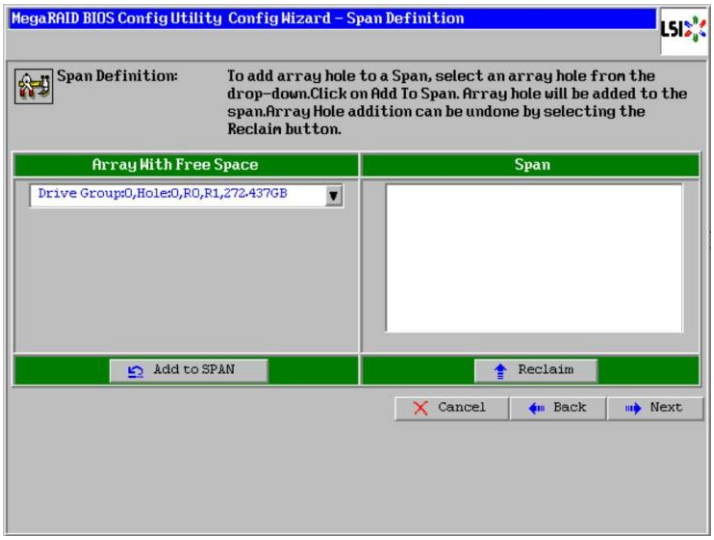


To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

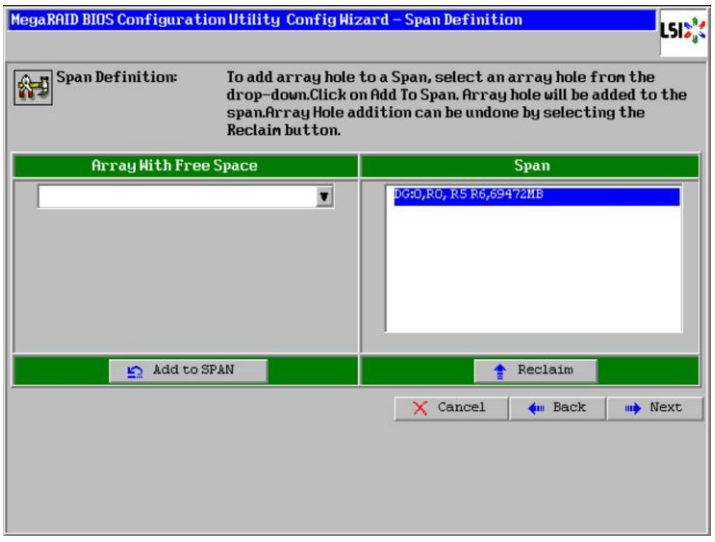
6 Click **Accept DG**. The following screen appears:



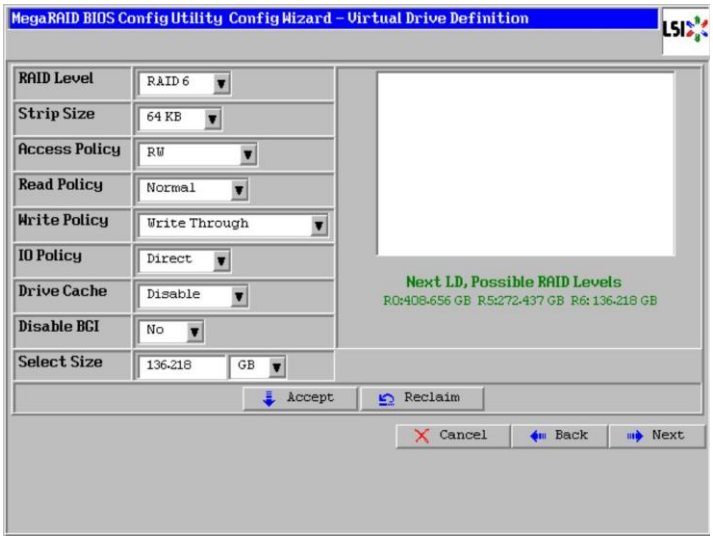
7 Click **Next**. The following screen appears:



8 Click **Add to SPAN.** The following screen appears:



9 Click **Next**. The following screen appears:



10 Specify the RAID level, stripe size, read policy, write policy, and disk array size. Set each item to the correct value in the following table.

Item	Content	Setting value
RAID Level *1	RAID Level	Specify any level.
Stripe Size *2	Stripe size (only RAID 0 and 5)	2 KB / 4 KB / 8 KB / 16 KB / 32 KB / [64KB] / 128 KB
Access Policy *3	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advance reading)] / Ahead (always advance reading) / Adaptive (advance reading only in the event of sequential access)
Write Policy *4 *5	Write policy	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)
IO Policy *3	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)
Drive Cache *3	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)
Disable BGI *3 *6	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *7 *8	Size of a disk array	Enter the maximum capacity value.

*1 RAID 6 with three hard disks is not supported.

*2 For RAID 1, set 64 KB by Default.

*3 Always use the Default or recommended value for Access Policy.

*4 In Write Policy, Write Back can be set only when the system equipment is already connected to the UPS (uninterruptible power supply). Confirm that the checkmark is removed from **Wrthru for BAD BBU** at that time. Even in this case, set **Write Through** when the operating system is installed. Otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays.

*5 Do not select **Write Back with BBU**.

*6 Change from the Default value to the recommended value.

*7 Maximum capacity size that can be set is shown under **Next LD, Possible RAID Levels** at the right of the screen. Change the maximum capacity value for your RAID level.



Maximum capacity value under the RAID 0 setting: 408.656 GB
Maximum capacity value under the RAID 5 setting: 272.437 GB
Maximum capacity value under the RAID 6 setting: 136.218 GB

*8 Do not change the unit of **Select Size: always GB by Default**.

NOTICE

When enabling the write cache of the disk array, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Tip

If you specify a larger disk array size than the maximum capacity, “Unacceptable size” appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

11 Click **Accept**.
One of the following screens appears.

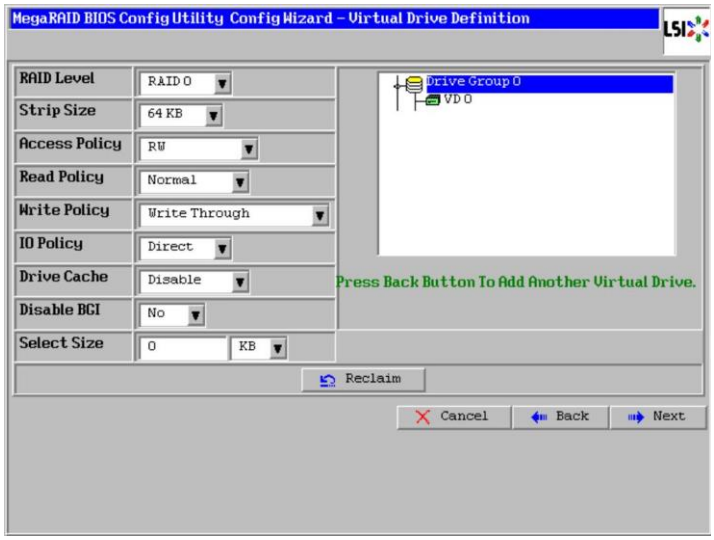
◆ When selecting **Write Through** in the write policy setting:



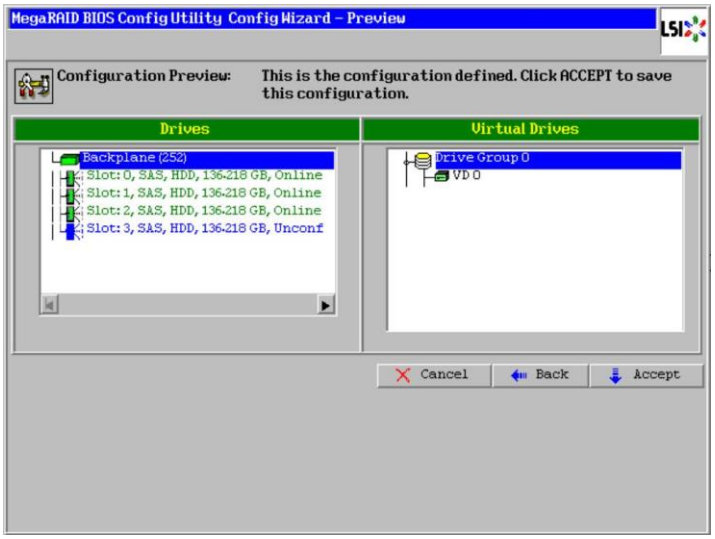
◆ When selecting **Always Write Back** in the write policy setting:



12 Click **Yes**. The following screen appears:



13 Click **Next.** The following screen appears**:**



14 Click **Accept**. The following screen appears:



15 Click **Yes**. The following screen appears:



16 Click **No**. The screen returns to the main menu.

17 Initialize the disk array that you have built referring to Initializing disk arrays.

Building disk arrays for RAID 10

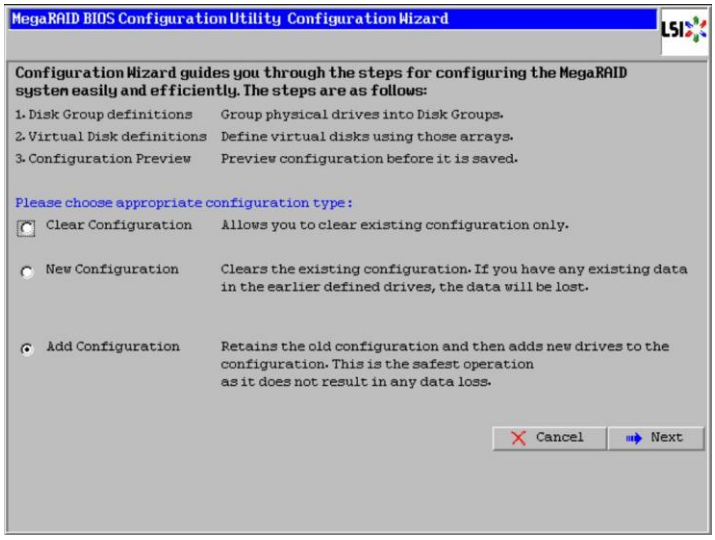
The following procedure describes building disk arrays for RAID 10.

The following table summarizes the number of hard disks required for building RAID 10.

RAID level	Number of hard disks required
RAID 10	4

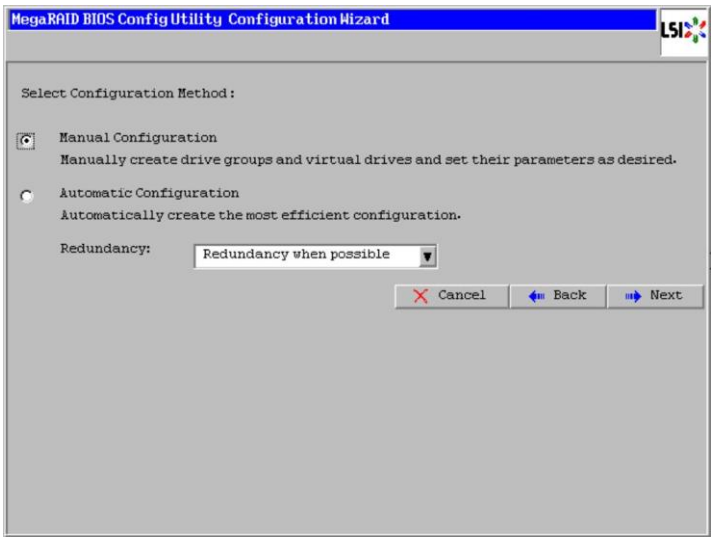
1 Select **Configuration Wizard** from the main menu.

The following screen appears:



2 Check **New Configuration** or **Add Configuration**, and click **Next**.

The following screen appears:



NOTICE

If you select New Configuration, all data in those hard disks including the disk array information will be lost. Backup your required data before selecting New Configuration.

Tip

The existing disk arrays will remain when you select Add Configuration. Add Configuration should be selected when you want to keep the existing disk arrays, and to build disk arrays through an additional hard disk.

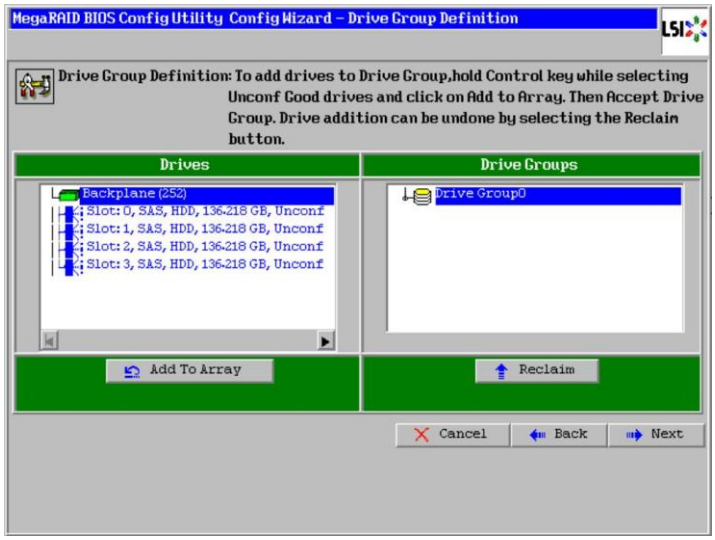
If you select New Configuration, you lose the existing disk arrays. This should be selected when you discard the existing disk array and build a new one.

If you select New Configuration, the following screen appears first. Clicking **Yes** allows you to build a disk array.

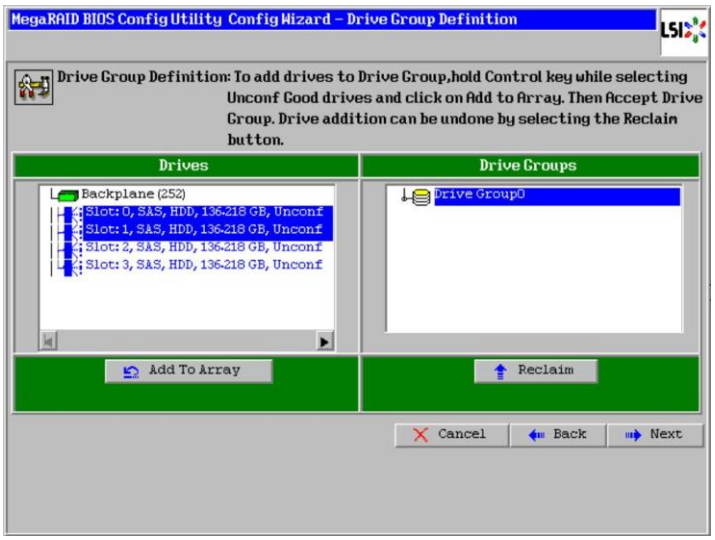


3 Check **Custom Configuration** and click **Next**.

The following screen appears:



4 Select two hard disks to be used for building a disk array.

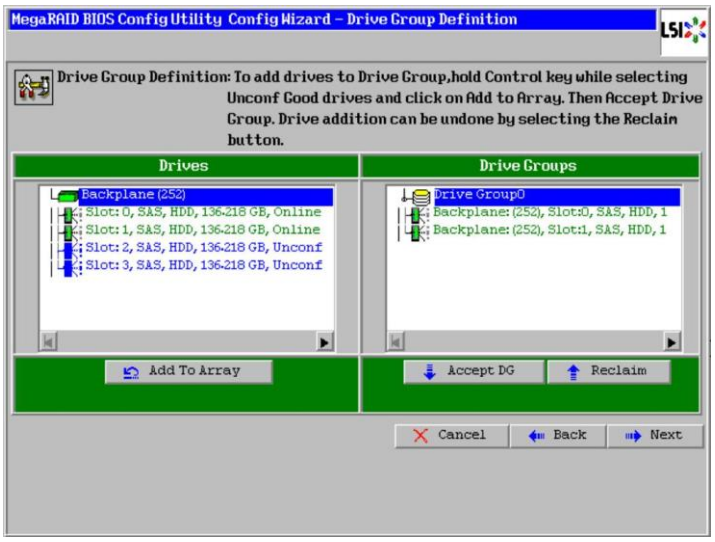


Tip

You can select only a hard disk whose status is Unconfigured Good (unused).

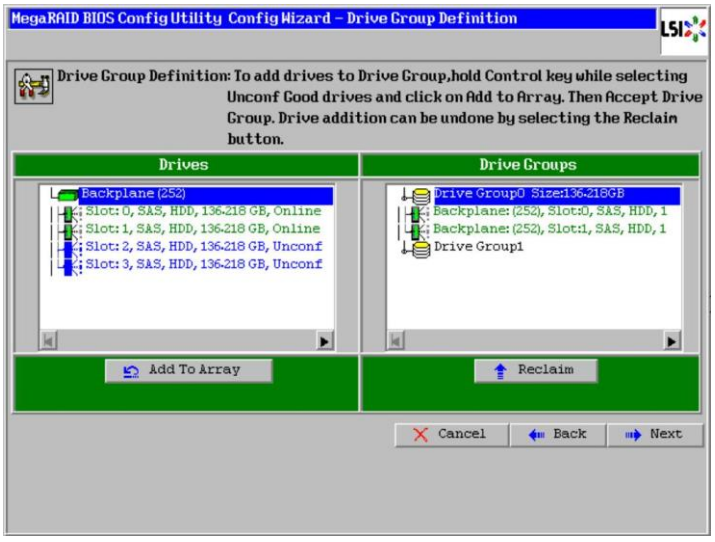
To select multiple hard disks, click them while pressing the **Ctrl** key.

5 After selecting two hard disks for building a disk array, click **Add to Array**.
Status of those selected hard disks is **Online** as shown in the **Drives** pane.



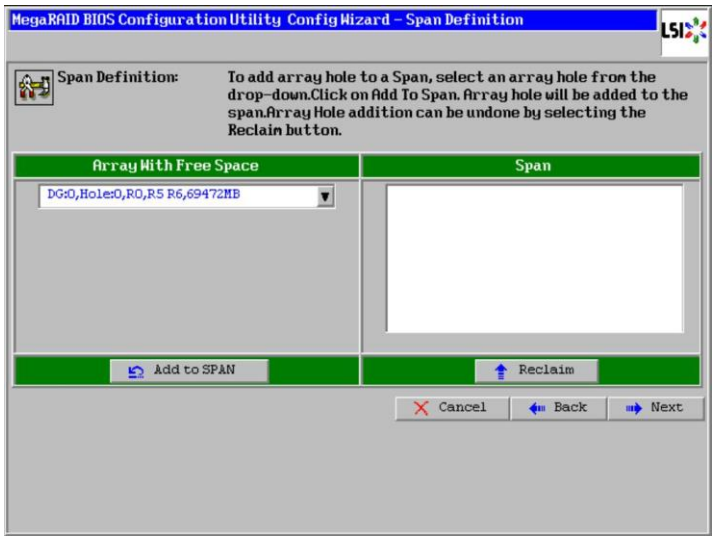
Tip To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

6 Click **Accept DG**.
The following screen appears:



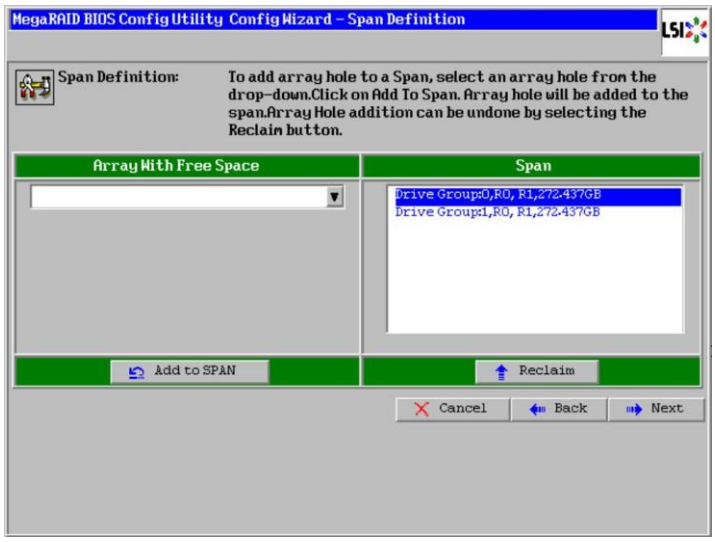
7 Repeat steps 4, 5, and 6 until you have selected all hard disks used for RAID 10, and then click **Next**.

The following screen appears:



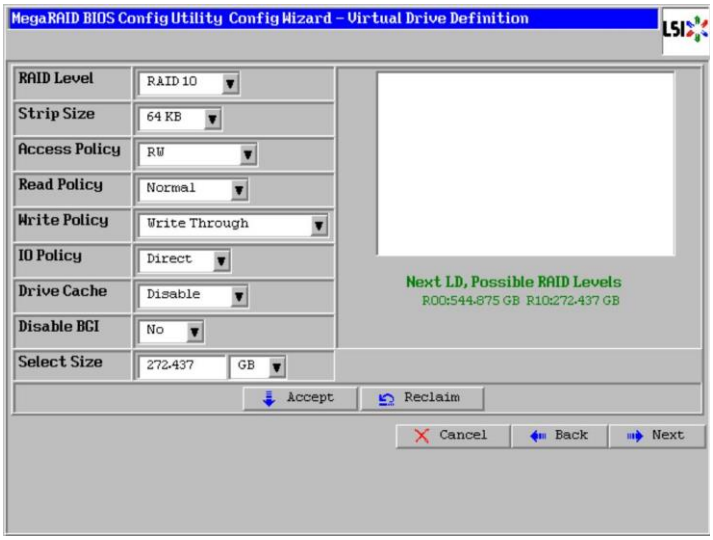
8 Click **Add to SPAN** as many times as repeated in steps 4, 5, and 6 in step 7.

Click it until the following display under **Array With Free Space** disappears.



9 Click **Next**.

The following screen appears:



10 Specify the RAID level, stripe size, read policy, write policy, and disk array size.

Set the values for each item in the following table.

Item	Content	Setting value **
RAID Level	RAID Level	[RAID 10]
Stripe Size *1	Stripe size	2 KB / 4 KB/ 8 KB / 16 KB / 32 KB / [64 KB] / 128 KB
Access Policy *1	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advanced reading)] / Ahead (always advanced reading) / Adaptive (advanced reading only in the event of sequential access)
Write Policy *2 *3	Write policy	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)
IO Policy *1	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)
Drive Cache *1	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)
Disable BGI *1 *4	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *5 *6	Size of a disk array	Entering the maximum capacity value.

*1 Always use it in the default or recommended value.

*2 In Write Policy, Always Write Back can be set only when the system equipment is already connected to the UPS (uninterruptible power supply). Even in this case, set **Write Through** when the operating system is installed. Otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays.

*3 Do not select **Write Back with BBU**.

*4 Change from the default value to the recommended value.

*5 Keep the existing maximum capacity value in **Select Size**.

*6 Do not change the unit of **Select Size: always [GB] by Default**.

NOTICE

When enabling the write cache of the disk array, connect the system equipment to a UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.



If you specify a larger disk array size than the maximum capacity, “Unacceptable size” appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

11 Click **Accept**.
One of the following screens appears.

◆ When selecting **Write Through** in the write policy setting:

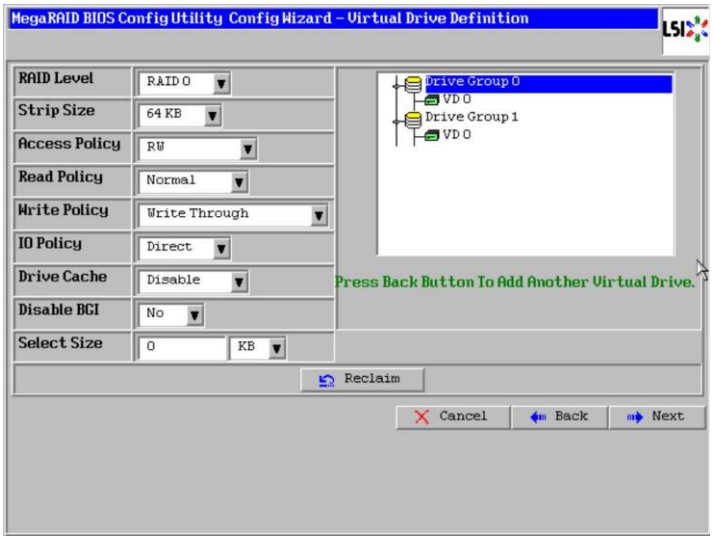


◆ When selecting **Always Write Back** in the write policy setting:



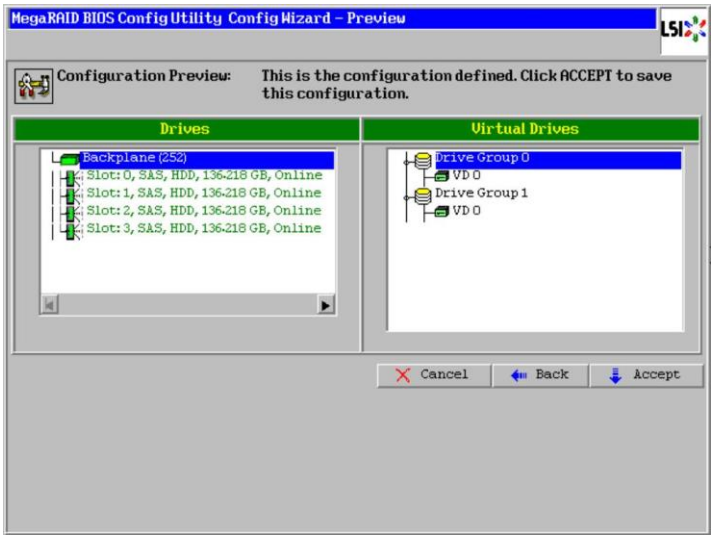
12 Click **Yes**.

The following screen appears:



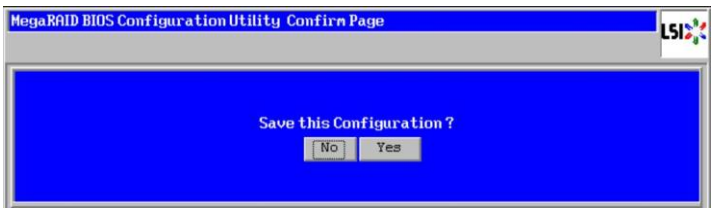
13 Click **Next**.

The following screen appears:



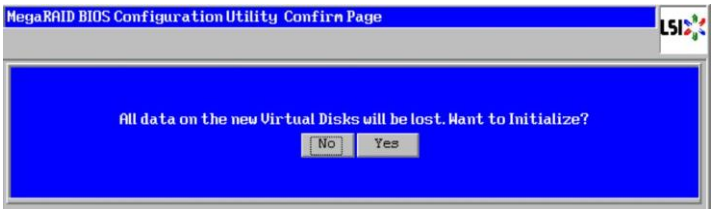
14 Click **Accept**.

The following screen appears:



15 Click **Yes**.

The following screen appears:



16 Click **No**.

The screen returns to the main menu.

17 Initialize the disk array that you have built, referring to Initializing disk arrays.

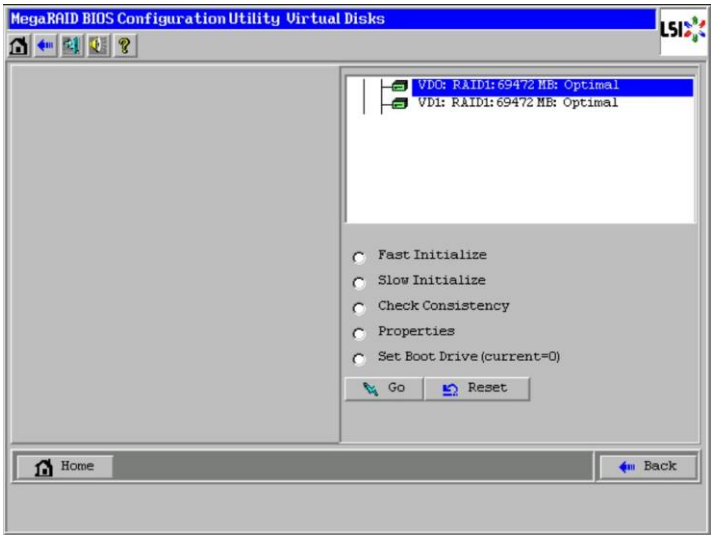
Initializing disk arrays

This section describes the procedure for initializing disk arrays

> **NOTICE**
>
> When a disk array is initialized, all data in those hard disks including the disk array information will be lost. Backup your required data before initializing a disk array.

1 Select **Virtual Drives** from the main menu.

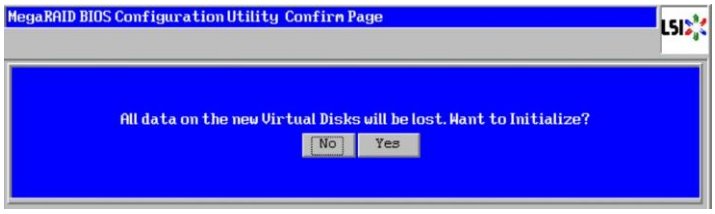
The following screen appears:



2 From the list of disk arrays displayed in the frame at the upper right, select a disk array configuration to initialize.

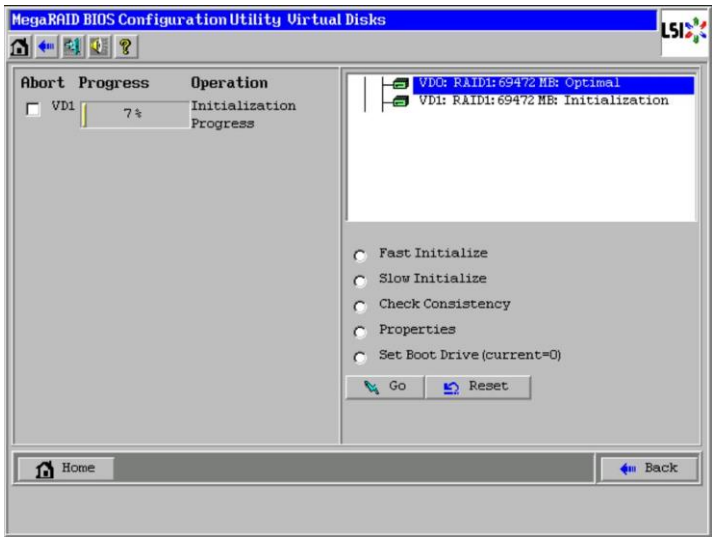
3 Check **Slow Initialize** and click **Go**.

The following screen appears:



4 Click **Yes**.

The initialization progress is displayed.



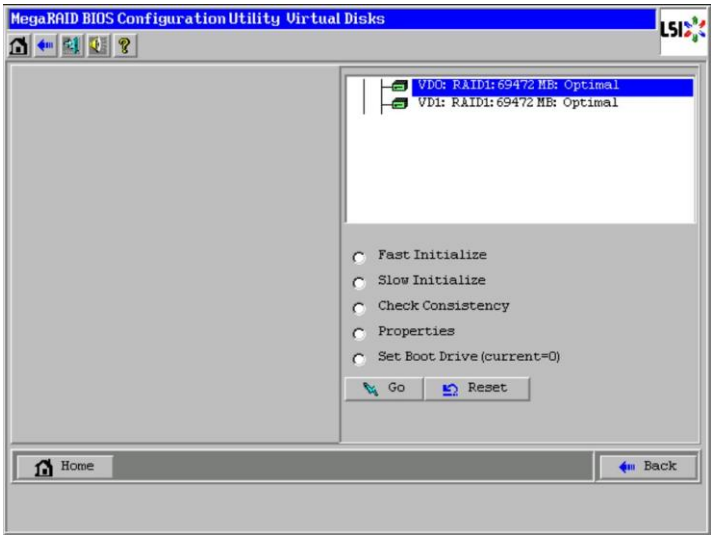
5 Wait until the process is completed 100%.

A guideline of initialization time is shown in the table below.

Single hard disk capacity	Initialization time
147 GB (SAS type)	Approximately 50 minutes
300 GB (SAS type)	Approximately 100 minutes
600 GB (SAS type)	Approximately 200 minutes

Tip The initialization time varies depending on the single hard disk capacity regardless of the RAID level or disk array capacity.

6 When initialization is completed 100%, click **Home** to return to the main menu.



Deleting disk arrays

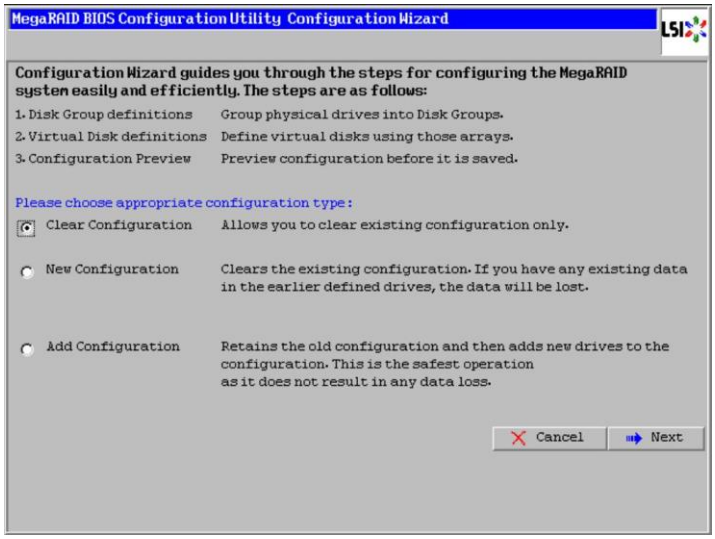
This section describes the procedure for deleting disk arrays.

> ***NOTICE***
>
> When a disk array is deleted, all data in those hard disks including the disk array information will be lost. Backup your required data before deleting a disk array.

Deleting all disk arrays simultaneously

1 Select **Configuration Wizard** from the main menu.

The following screen appears:



2 Check **Clear Configuration** and click **Next**.

The following screen appears:

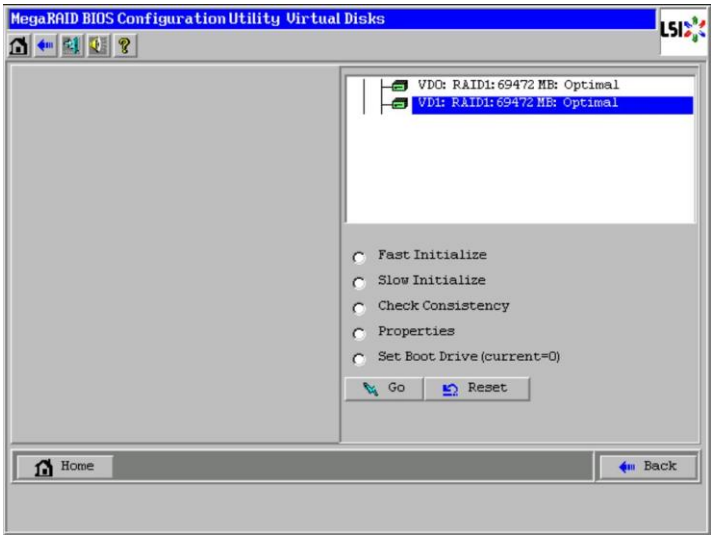


3 Click **Yes**.

Deleting disk arrays selectively

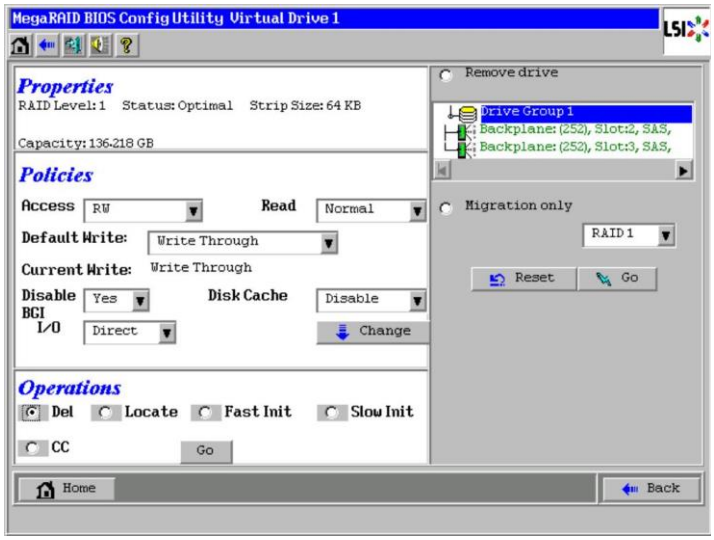
1 Select **Virtual Drives** from the main menu.

The following screen appears:

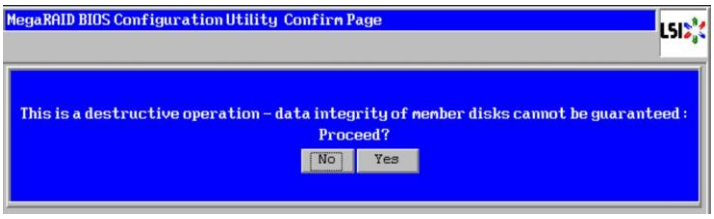


2 From the list displayed at the upper right of the screen, select a disk array that you want to delete. Then check **Properties** and click **Go**.

The following screen appears:



3 Check **Del** and click **Go**.
The following screen appears:



4 Click **Yes**.

Checking disk arrays for consistency

This section describes how to check the consistency of disk arrays.

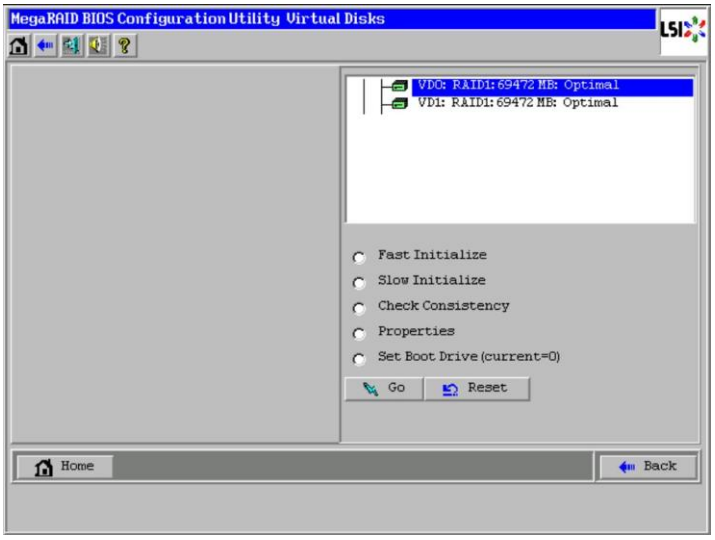
Consistency check can be done from MegaRAID Storage Manager. See the *MegaRAID Storage Manager* manual in the DriverKit CD-ROM for how to check consistency from the MegaRAID Storage Manager.

Tip

Consistency check on disk arrays can be executed only for RAID 1, 5, 6, and 10.

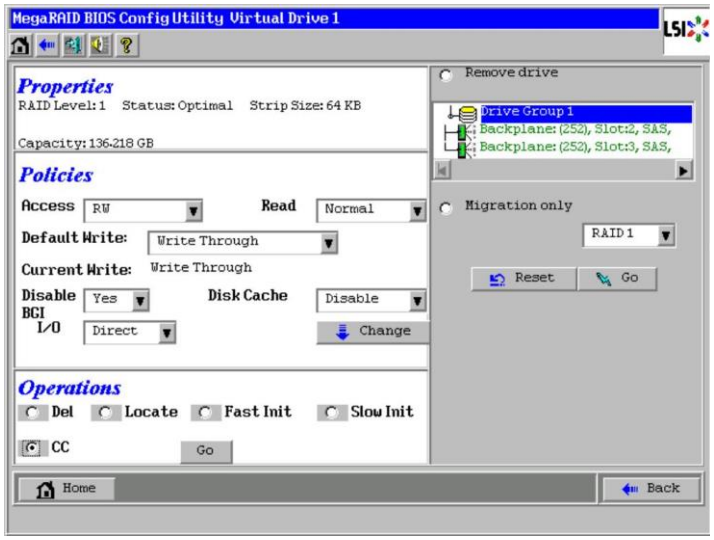
1 Select **Virtual Drives** from the main menu.

The following screen appears:



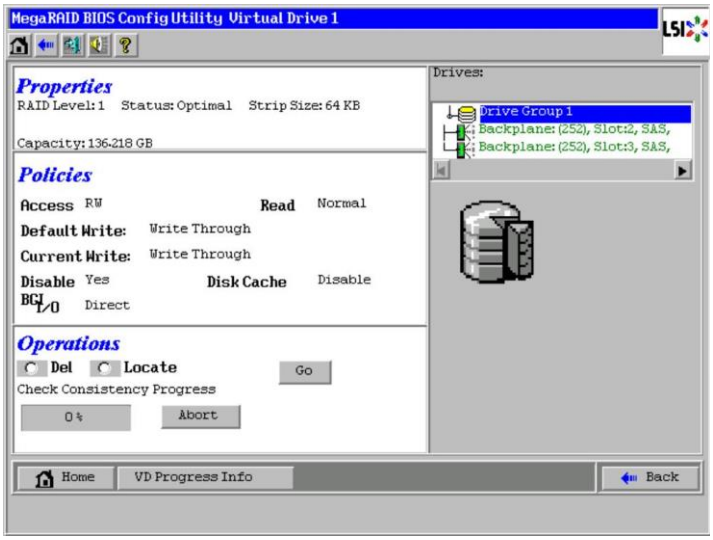
2 From the list displayed at the upper right of the screen, select a disk array that you want to check the consistency. Then check **Properties** and click **Go**.

The following screen appears:



3 Check **CC** and click **Go**.

The progress of consistency check is displayed.



4 Wait until the process is completed 100%.

5 When the consistency check is completed 100%, click **Home** to return to the main menu.

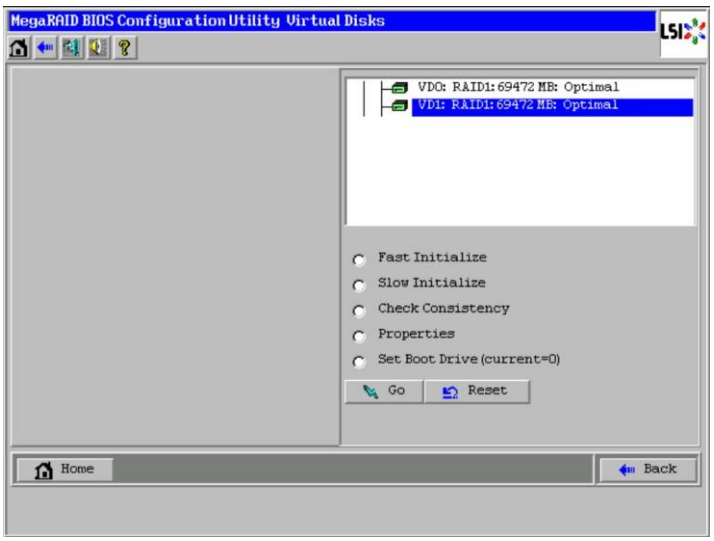
Changing the order of booting disk arrays

This section describes the procedure for changing the booting order in an environment in which multiple disk arrays are set.

Normally, the highest order of booting is assigned to the disk array that was set first. You can assign a disk array that has been built later, however, to the highest in the boot order.

1 Select **Virtual Drives** from the main menu.

The following screen appears:



Tip **Set Boot Drive** is followed by the number of the current disk array being booted.

2 From the list displayed at the upper right of the screen, select a disk array for which you want to set a boot device. Next, check **Set Boot Drive** and click **Go**.

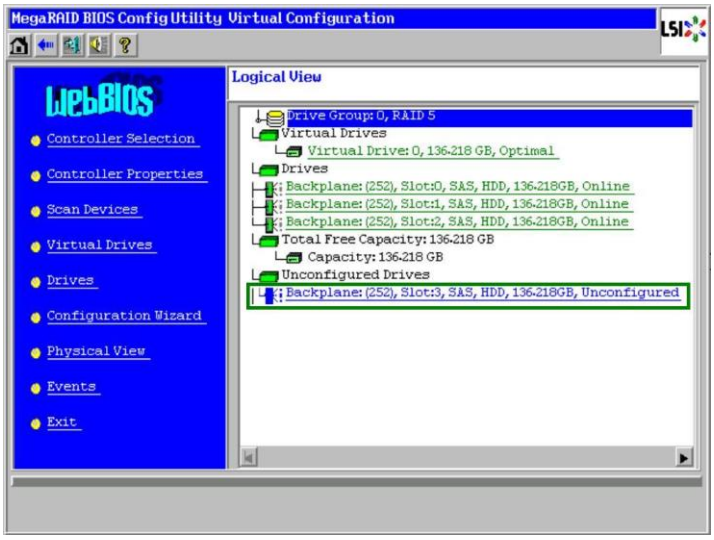
Setting hotspares

This section describes the procedure for setting hotspares.

Note

Be sure to configure redundant disk arrays, RAID 1, 5, 6, or 10 before setting hotspares.

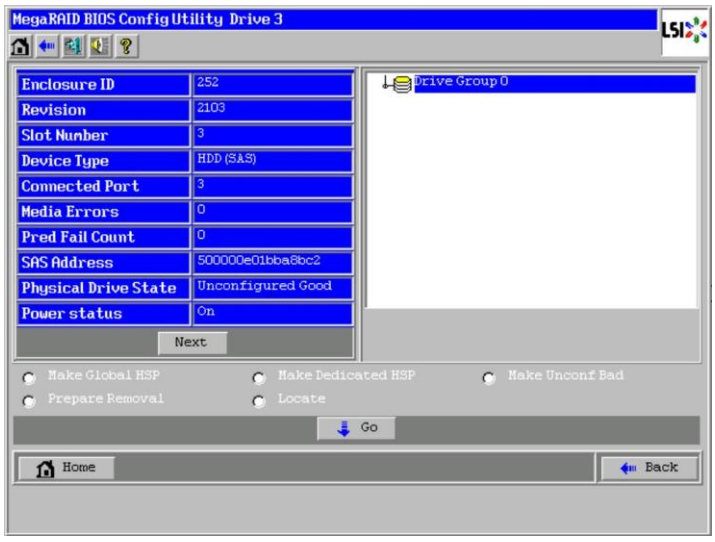
1 Click the hard disk that is recognized as **Unconfigured Drives** in the **Logical View** pane while the main menu is displayed.



Tip

Only a hard disk whose status is **Unconfigured Good** (unused) can be selected.

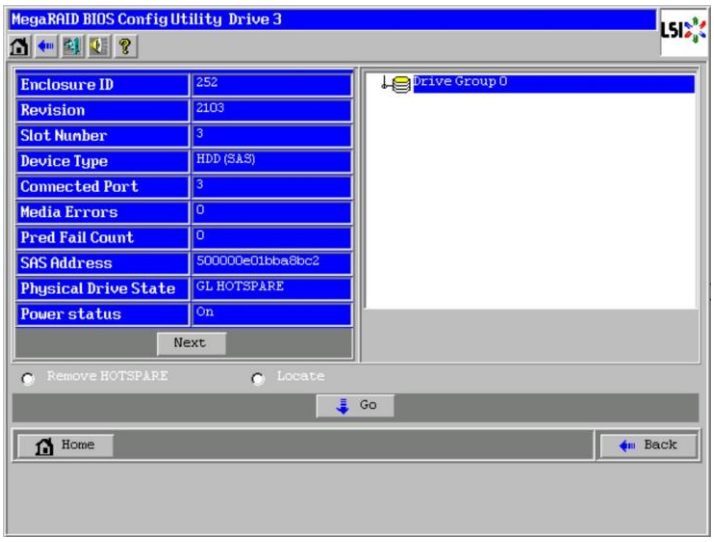
2 The following screen appears.



3 Check **Make Global HSP**.

4 Click **Go**

Hotspare is set to the specified hard disk.



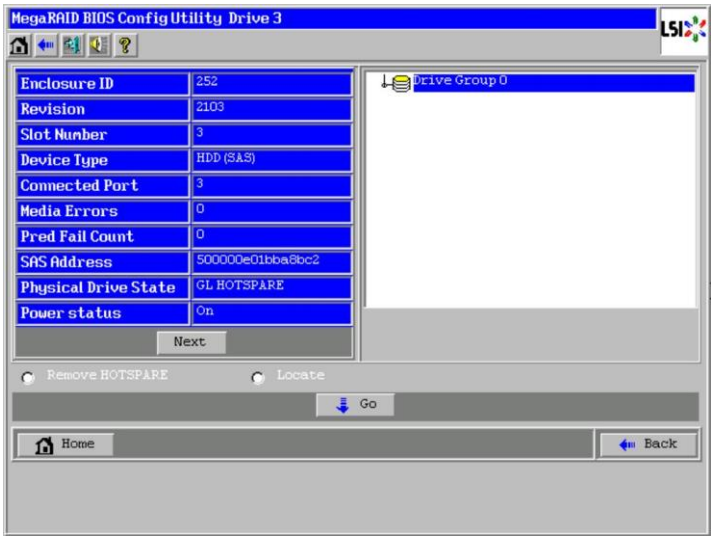
Canceling hotspares

This section describes the procedure for canceling hotspares.

1 When the main menu is displayed, click the hard disk that is set in hotspare in **Logical View** or **Physical View**.

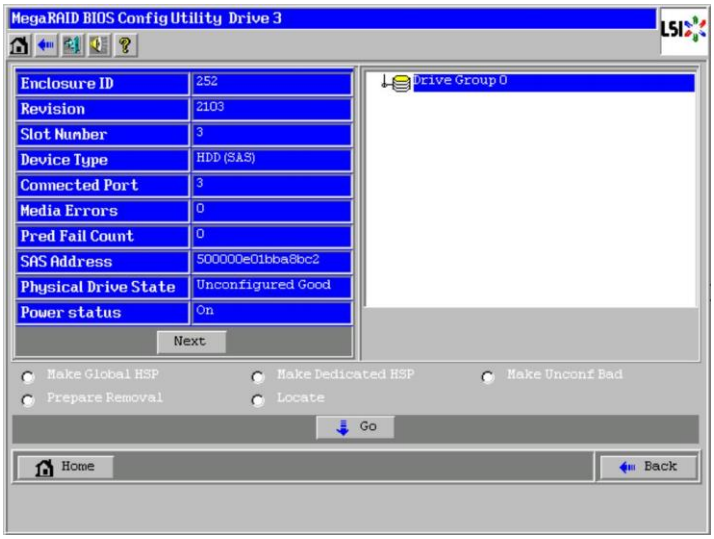
Select a hard disk with hotspare status.

The following screen appears:



2 Check **Remove HOTSPARE**, and click **Go**.

Hotspare is released.



Rebuilding disk arrays

Here is a procedure for rebuilding disk arrays in cases where a problem occurred on one hard disk in a redundant disk array configuration (RAID 1, 5, 6,10).



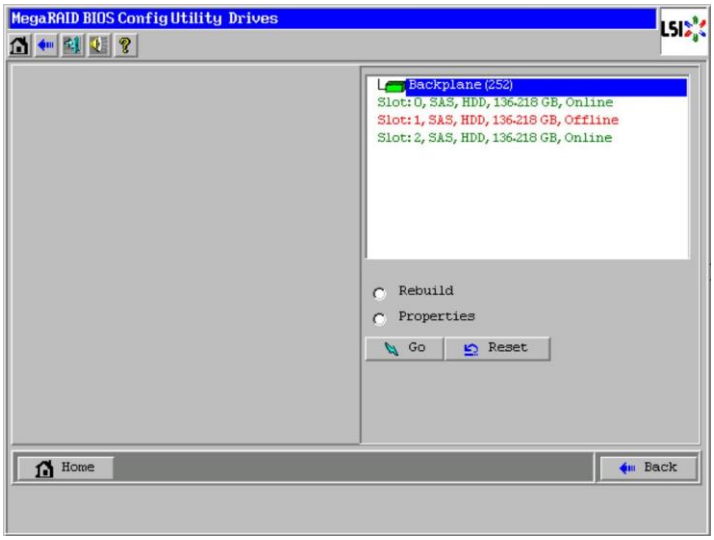
For RAID 6, the disk array can be restored even if two hard disks fail.

With hotspares configuration, rebuilding will work automatically when a hard disk problem occurs. Without hotspare configuration, rebuilding will work automatically after you replace the faulty hard disk in hot-plug.

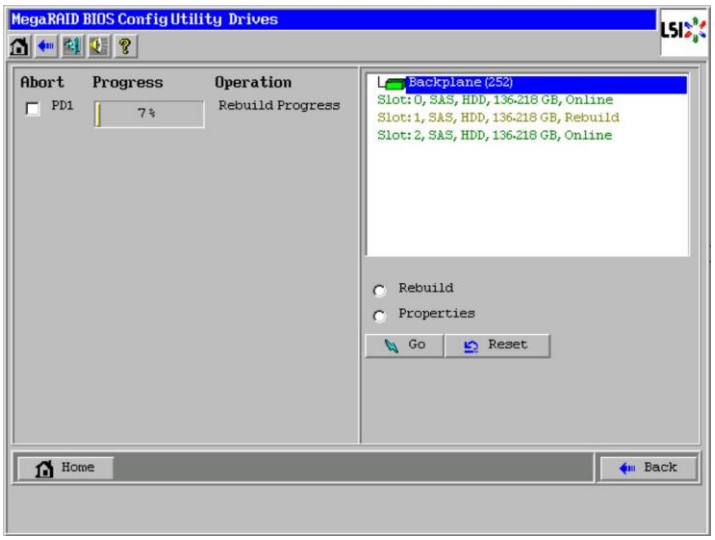
The following is a procedure for manually rebuilding when automatically rebuilding did not work.

1 Select **Drives** from the main menu.

The following screen appears:



2 Select a hard disk with the **Offline** status, check **Rebuild**, and click **Go**.
The progress of rebuilding is displayed.



3 Wait until the process is completed 100%.
A guideline for rebuilding time is shown in the table below.

RAID level	Capacity of a disk array	Rebuilding time
RAID 1	147 GB (SAS: 147GB HDD x 2)	Approximately 50 minutes
	300 GB (SAS: 300GB HDD x 2)	Approximately 100 minutes
	600 GB (SAS: 600GB HDD x 2)	Approximately 200 minutes
RAID 5	294 GB (SAS: 147GB HDD x 3)	Approximately 50 minutes
	600 GB (SAS: 300GB HDD x 3)	Approximately 100 minutes
	1200 GB (SAS: 600GB HDD x 3)	Approximately 200 minutes
RAID 6	294 GB (SAS: 147GB HDD x 4)	Approximately 80 minutes
	600 GB (SAS: 300GB HDD x 4)	Approximately 160 minutes
	1200 GB (SAS: 600GB HDD x 4)	Approximately 320 minutes
RAID 10	294 GB (SAS: 147GB HDD x 4)	Approximately 50 minutes
	600 GB (SAS: 300GB HDD x 4)	Approximately 100 minutes
	1200 GB (SAS: 600GB HDD x 4)	Approximately 200 minutes

Tip The rebuilding time is proportional to the capacity of a disk array.

4 When rebuilding is completed 100%, click **Home** to return to the main menu.

Expanding disk array capacity

This section describes how to expand a disk array in the RAID 0, 5, or 6 disk array by adding hard disks to use.

Disk array expansion can also be done from MegaRAID Storage Manager. See the *MegaRAID Storage Manager* manual in the DriverKit CD-ROM for information about how to expand disk arrays from the MegaRAID Storage Manager.

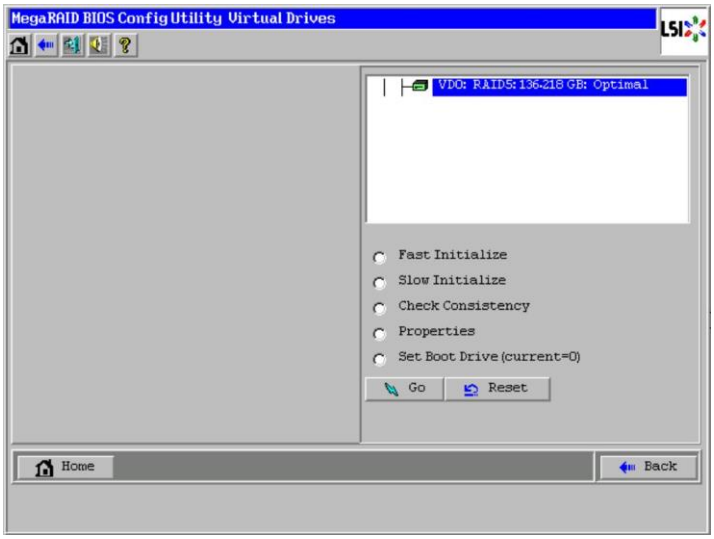


A disk array expansion cannot be cancelled during the execution.

Make sure to install a hard disk with Unconfigured Good status (unused) before expanding the capacity.

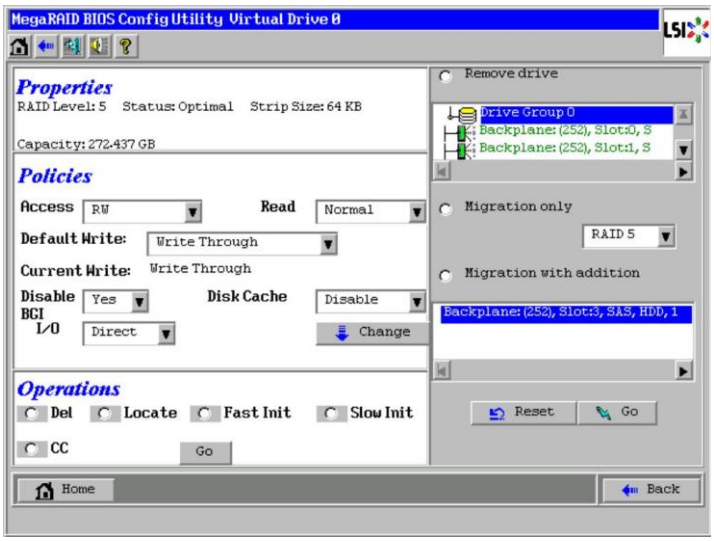
1 Select **Virtual Drives** in the main menu.

The following screen appears:



2 Select a disk array to expand the capacity from the list displayed on the upper right of the screen. Check **Properties**, and click **Go**.

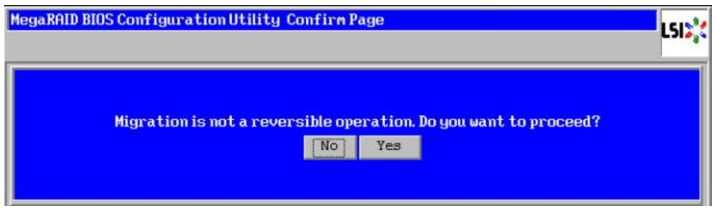
The following screen appears:



3 Select a hard disk to use for the capacity expansion from the list displayed at the lower right of the screen, check **Migration with addition**, and click **Go**.

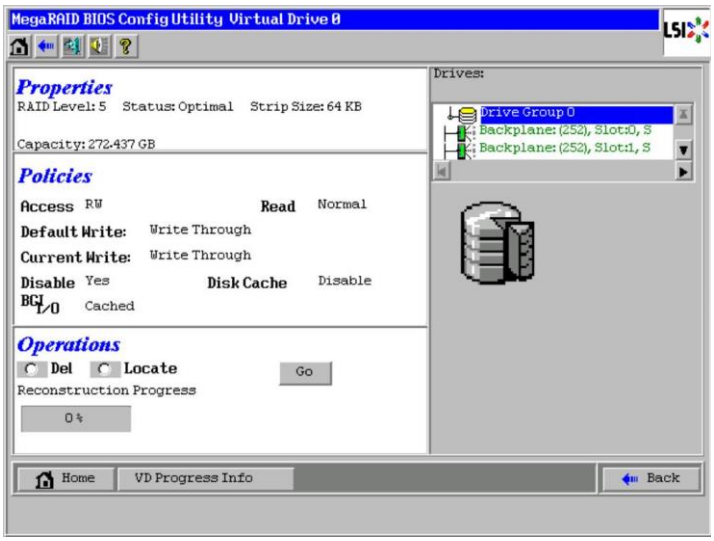
Tip To select multiple hard disks, click hard disks while pressing the **Ctrl** key.

The following screen appears:



4 Click **Yes**.

The progress of the capacity expansion is displayed.



5 Wait until the expansion is completed 100%.

A guideline of expanding time is shown in the following table.

RAID level	Capacity of a disk array	Rebuilding time for expansion
RAID 0	Expands “441 GB (SAS: 147GB HDD x 3)”	Approximately 300 minutes
	Expands “900 GB (SAS: 300GB HDD x 3)”	Approximately 600 minutes
	Expands “1800 GB (SAS: 600GB HDD x 3”	Approximately 1200 minutes
RAID 5	Expands “294 GB (SAS: 147GB HDD x 3)”	Approximately 240 minutes
	Expands “600 GB (SAS: 300GB HDD x 3)”	Approximately 480 minutes
	Expands “1200 GB (SAS: 600GB HDD x 3)”	Approximately 960 minutes
RAID 6	Expands “294 GB (SAS: 147GB HDD x 4)”	Approximately 240 minutes
	Expands “600 GB (SAS:300GB HDD x 4)"	Approximately 480 minutes
	Expands “1200 GB (SAS: 600GB HDD x 4)”	Approximately 960 minutes

Tip The rebuilding time for expansion is proportional to the capacity of a disk array regardless of the number of hard disks to add.

6 When expansion is completed 100%, click **Home** to return to the main menu.

Changing the write policy for disk arrays

This section describes the procedure for changing the write policies.

> ***NOTICE***
>
> When enabling the disk array “write cache”, connect the system equipment to a UPS. Otherwise, data in the write cache may disappear or be destroyed during a blackout or instant power failure.

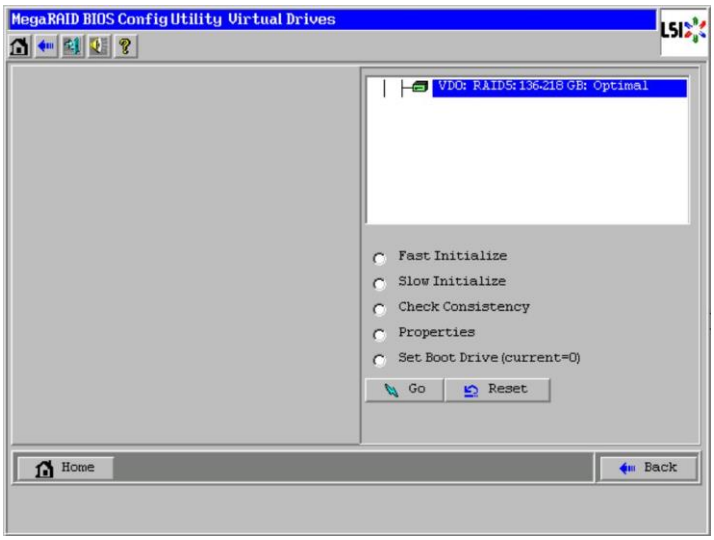
Note

In Write Policy, “Always Write Back” can be supported only when the system equipment is connected to the UPS (uninterruptible power supply).

Even in this case, set to **Write Through** when installing the operating system. Otherwise, installation may not be properly completed.

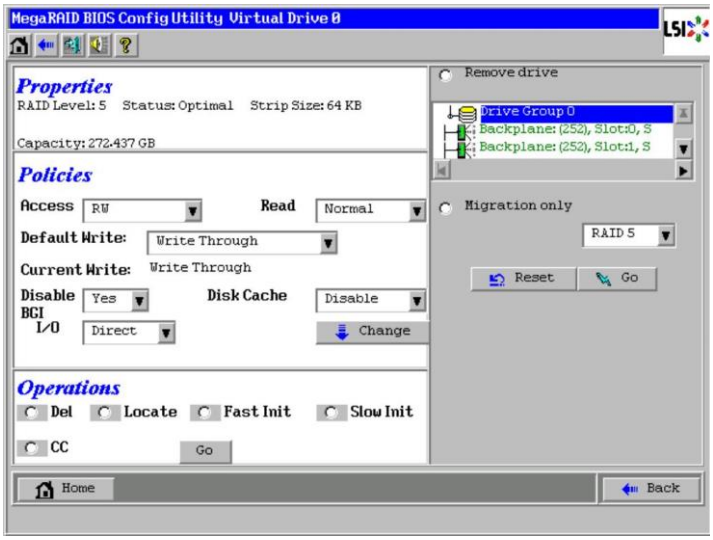
1 Select **Virtual Drives** in the main menu.

The following screen appears:



2 From the list displayed at the upper right of the screen, select a disk array for which you want to change the write policy. Check **Properties** and click **Go**.

The following screen appears:



3 Select the write policy from **Default Write** in the **Policies** pane, and click **Change**.

Setting value	Description
Always Write Back	Write cache is valid.
Write Through	Write cache is invalid.
Write Back with BBU	Write cache is valid only when the battery is installed.

Note

In Write Policy, operation with **Always Write Back** can be supported only when the system equipment is connected to the UPS (uninterruptible power supply).

Even in this case, set **Write Through** when installing the OS. Otherwise, installation might not complete properly.

Do not select **Write Back with BBU**.

4 One of the following screens appears. Click **Yes**.

- When selecting **Write Through** in the Default write setting:



- When selecting **Always Write Back** in the Default write setting:



5 Click **Home** to return to the main menu.

Tip

Set the write policy per disk array. When building multiple disk arrays, set the write policy to all disk arrays.

❑ BIOS settings for SAS internal RAID board

When using the boot from an external storage on the system equipment with the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y, change the BIOS setting: Controller BIOS setting to Disabled.

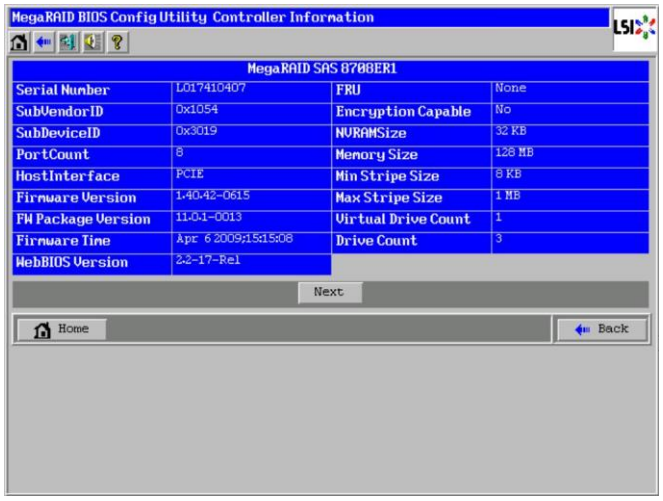
This section describes the procedure for changing the BIOS setting of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y.



When the BIOS setting: Controller BIOS setting is changed to Disabled, you cannot execute the boot from the disk array configured in the SAS internal RAID Board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y.

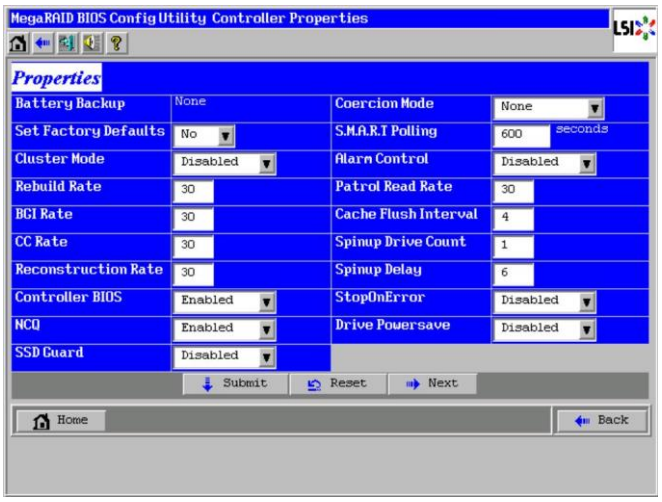
1 Select **Controller Properties** from the main menu.

The following screen appears:



2 Click **Next**.

The following screen appears:



3 Select one of the setting values in the table below from **Controller BIOS**, and click **Submit**.

Setting value	Description
Enabled	Enables BIOS of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y. Enables the boot from the disk array.
Disabled	Disables BIOS of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y. Disables the boot from the disk array.

Tip Make sure to click **Submit** after changing the setting.

4 Confirm that **Controller BIOS** is set to that value.

5 Click **Home** to return to the main menu.

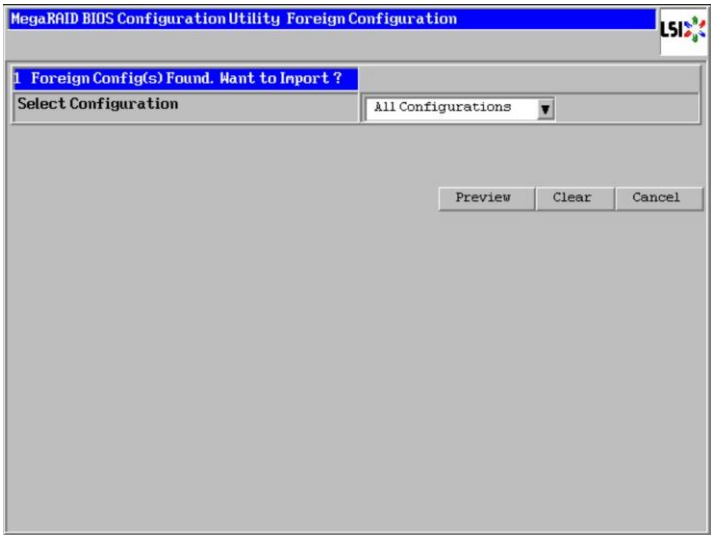
❑ Disk with a foreign configuration

This section describes how to deal with a hard disk with a different configuration detected from the disk array controller board configuration.

Differences in configuration between disks may be caused by the following conditions.

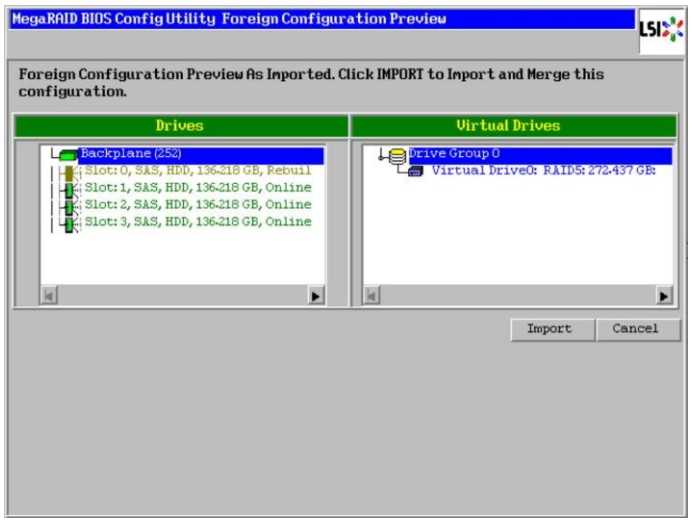
Conditions to generate foreign configuration
A disk failed and could not be recognized. Then the disk has been restored to be recognized.
A hard disk, used in another device with a specific disk array configuration, is used in the array.

1 Click **Preview**.



2 If the displayed configuration is correct, click **Import**.

If the displayed configuration is incorrect, click **Cancel**. When the screen returns to Step 1, click **Clear**.



Tip

When clicking **Clear**, a message “Previous foreign configuration will be lost. Do you want to proceed?” is displayed. Click **Yes**, and the previous foreign configuration will be eliminated.

❑ Status

Status of the disk array

The following table lists the disk arrays status.

Status indication	Description
Optimal	Normal. The disk array is perfect in function.
Partially Degraded	One hard disk fails in the RAID 6 disk array.
Degraded	One hard disk fails in the RAID 1, 5, or 10 disk array. Or two hard disks fail in the RAID 6 disk array.
Offline	The disk array is inoperable because of either failures in multiple hard disks in a redundant disk array or a failure in a hard disk in a non-redundant disk array.

Status of the hard disk

The following table lists the hard disks status.

Status indication	Description
Online	Normal.
Offline/Failed	A fault has occurred. The hard disk is separated from the disk array due to failure.
Rebuild	Rebuilding is underway.
Dedicated Hot Spare/Global Hot Spare	This is set as a hotspare (either dedicated hotspare or global hotspare).
Unconfigured GOOD	This is not used for a disk array.
Unconfigured BAD	A fault has occurred. The unrecognizable hard disk is restored to recognizable.
Missing	A fault has occurred. A *normal* hard disk has been removed.

❑ BIOS messages

The following table lists the messages for MegaRAID WebBIOS displayed at system startup.

Message	Description
Cache data was lost due to an unexpected power-off or reboot during a write operation, but the adapter has recovered. This could be due to memory problems, bad battery, or you may not have a battery installed.	An incorrect power-off or reboot has been executed during write, parity check, rebuilding, patrol read, or initializing operation. There may be a cache memory failure, if this event is registered at the reboot after the system hangs in operation or if the OS cannot boot up.
Memory/battery problems were detected. The adapter has recovered, but cached data was lost.	An unexpected power-off or reboot has been executed during write, parity check, rebuilding, patrol read or initializing operation. There may be a cache memory failure, if this event is registered at the reboot after the system hangs in operation or if the OS cannot boot up. *3
Foreign configurations found on adapter.	A hard disk with a different configuration from the disk array configuration in the disk array controller was detected. See Disk with a foreign configuration.
FW package: xxxx	This shows the firmware package version. You do not need to take any action.
The battery hardware is missing or malfunctioning, or the battery is unplugged. If you continue to boot the system, the battery-backed cache will not function. Please contact technical support for assistance. Press 'D' to disable this warning (if your controller does not have a battery).	Battery backup unit information is not set correctly. Press the 'D' key while this message is displayed. If not recovered, contact your reseller from which you purchased the product or consult maintenance personnel.
Some configured disks have been removed from your system or are no longer accessible. Please check your cables and also ensure that all disks are present.	Some hard disks with the disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller from which you purchased the product or consult maintenance personnel.
The following VDs have missing disks: X Y… If you proceed (or load the configuration utility), these VDs will be marked OFFLINE and will be inaccessible. Please check your cables and ensure that all disks are present.	Since some hard disks have been removed, the disk array is set in OFF LINE. When this message is displayed even if the device is installed properly, contact your reseller from which you purchased the product or consult maintenance personnel.
The following VDs are missing: X Y … If you proceed (or load the configuration utility), these VDs will be removed from your configuration. If you wish to use them at a later time, they will have to be imported. If you believe these VDs should be present, please power off your system and check your cables to ensure all disks are present.	Some disk array configurations are removed. When this message is displayed even if the device is installed properly, contact your reseller from which you purchased the product or consult maintenance personnel.

Message	Description
All of the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your cables to ensure all disks are present.	All hard disks with disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller from which you purchased the product or consult maintenance personnel.
Press any key to continue, or 'C' to load the configuration utility.	Press the [C] key while this message is displayed, MegaRAID WebBIOS will start.
Press <Ctrl> <H> for WebBIOS.	When this message is displayed, press the [Ctrl] and [H] keys at the same time to start MegaRAID WebBIOS.
Your battery is bad or missing, and you have VDs configured for write-back mode. Because the battery is not usable, these VDs will actually run in write-through mode until the battery is replaced.	Write cache is not enabled because MegaRAID Storage Manager has set the write policy (write cache setting) to Write Back. Change the write policy setting from MegaRAID WebBIOS referring to Changing the write policy for disk arrays. Do not change the write cache from the current MegaRAID Storage Manager.
Multibit ECC errors were detected on the controller. DIMM on the controller needs replacement. If you continue, data corruption can occur. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM please press 'X' to continue.	An error has occurred in the cache memory of the disk array controller. When this message is displayed, contact your reseller from which you purchased the product or consult maintenance personnel.
Multiple Single-bit ECC errors were detected during the previous boot of the controller. DIMM on the controller needs replacement. If you continue, data corruption can occur. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM please press 'X' to continue.	
Single-bit overflow ECC errors were detected during the previous boot of the controller. DIMM on the controller needs replacement. If you continue, data corruption can occur. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM please press 'X' to continue.	

MegaRAID SAS 2108

❑ Checking a disk array controller firmware version

Check the firmware version of a disk array controller before operating MegaRAID Web BIOS.

Tip

Some of the screens and content of MegaRAID Web BIOS may depend on the disk array controller firmware version. Check your disk array controller firmware version with the following procedure, and see contents for the firmware version.

1 Turn on the power supply to the system equipment.

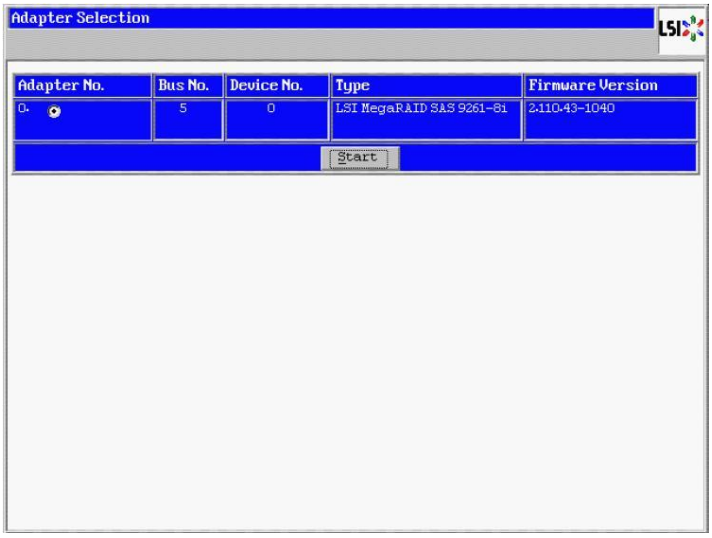
2 When the following screen appears, press and hold the **Ctrl** key on the lower left of the keyboard and press the **H** key.

The MegaRAID WebBIOS is started.

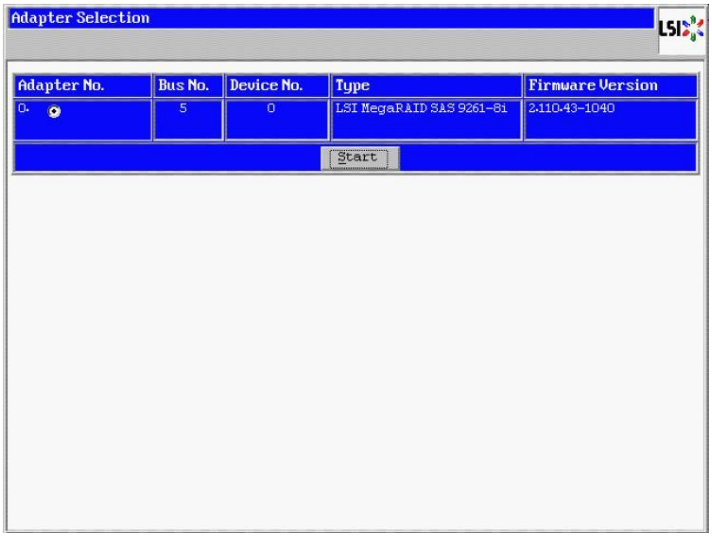
```
LSI MegaRAID SAS-MFI BIOS
Version xx.xx.xx (Build xxxxxx xx, 20xx)
Copyright(c) 20xx LSI Corporation
HA -x (Bus xx Dev xx) MegaRAID SAS xxxxxxxxx
FW package: xx.xx.xx.-xxxx
x Virtual Drive(s) found on the host adapter.
x Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS
```

If the operating system was been started before you press the keys, shutdown the operating system and then restart the system equipment. Check the manual for ending your operating system because some operating systems, such as Windows, require shutdown and other special operations for termination.

3 The following screen is displayed.



4 Check the **Firmware Version** in the following screen to find your disk array controller firmware version.



Tip See the following table to find your firmware version and lead-in phrase which includes the firmware version,

Firmware version	Lead-in phrase
2.110.63-1184	Firmware version; 2.110.63-1184
2.120.233-1474	Firmware version; 2.120.233-1474 (or later)

❑ Starting and ending MegaRAID WebBIOS

Use the following procedure to start the MegaRAID WebBIOS.

1 Turn on the power supply to the system equipment.

2 When the following screen appears, press and hold the **Ctrl** key and press the **H** key.

The MegaRAID WebBIOS is started.

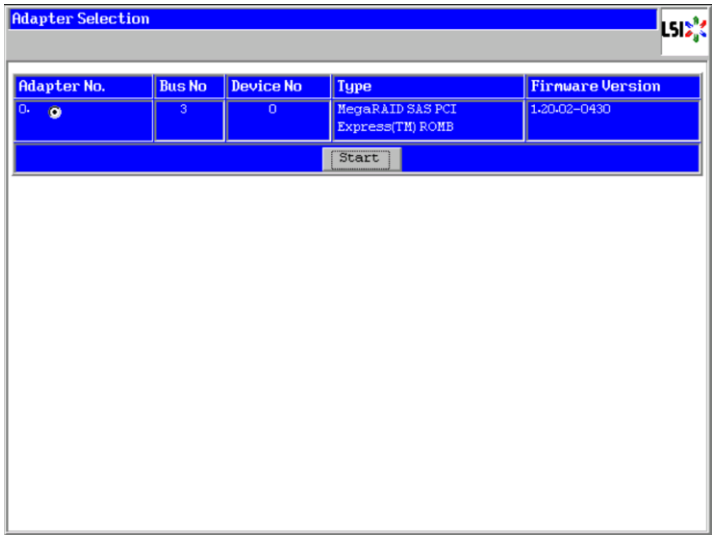
```
LSI MegaRAID SAS-MFI BIOS
Version x.xx.xx (Build xxx xx, xxxx)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus x Dev x) MegaRAID SAS 8708 ERI
FW package: x.x.x-xxxx

x Virtual Drive(s) found on the host adapter.

x Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS
```

If the operating system was started before you press the keys, shutdown the operating system and restart the system equipment. Check the manual for ending your operating system because some operating systems, such as Windows, require shutdown and other special operations when the particular operating system is terminated.

3 The MegaRAID WebBIOS is started and **Adapter Selection** appears.



4 Press the **Ctrl** key once.

Note

Without pressing the **Ctrl** key, your keyboard and mouse might not operate properly.

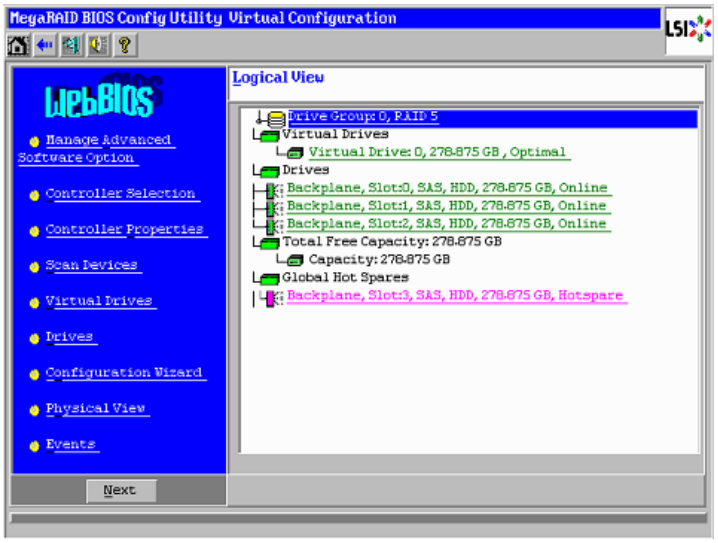
If the keyboard or mouse is not available when you operate MegaRAID WebBIOS, press the **Ctrl** key once.

5 Press **Enter** once.

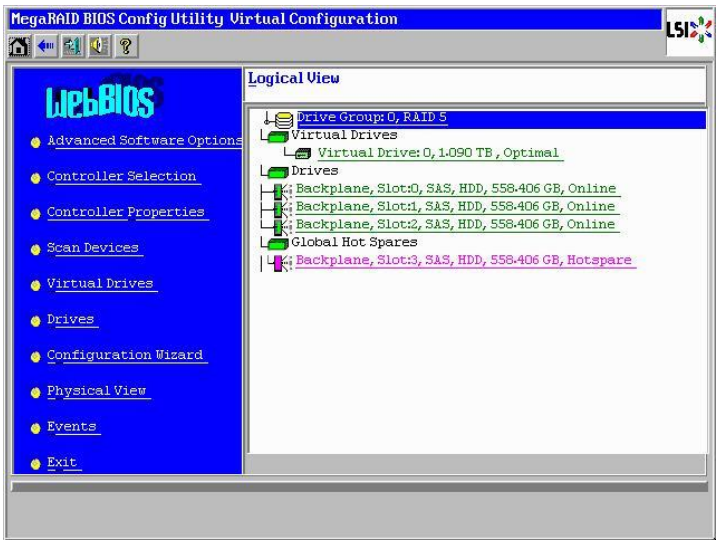
Without pressing **Enter**, the mouse will not work properly.

The main menu is displayed.

Firmware version: 2.110.63-1184

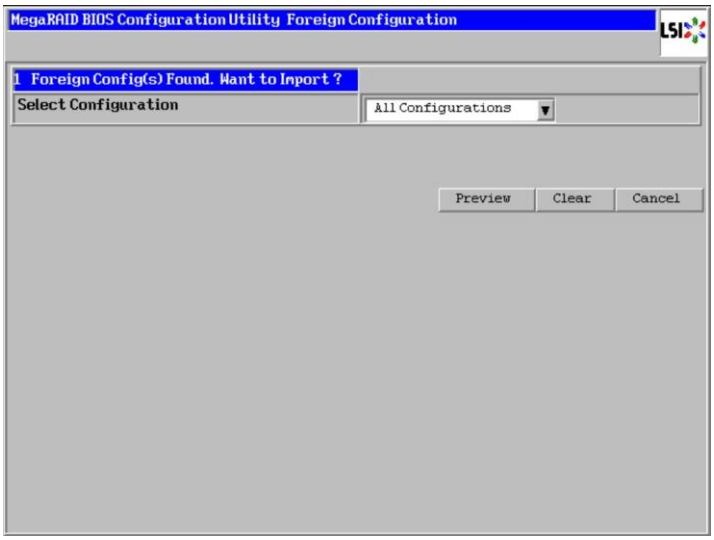


Firmware version: 2.120.233-1474 or later



Tip

If a hard disk which has different disk array configuration coming from the record in the disk array controller board exists, the following screen is displayed. See Disk with foreign configuration for more details.



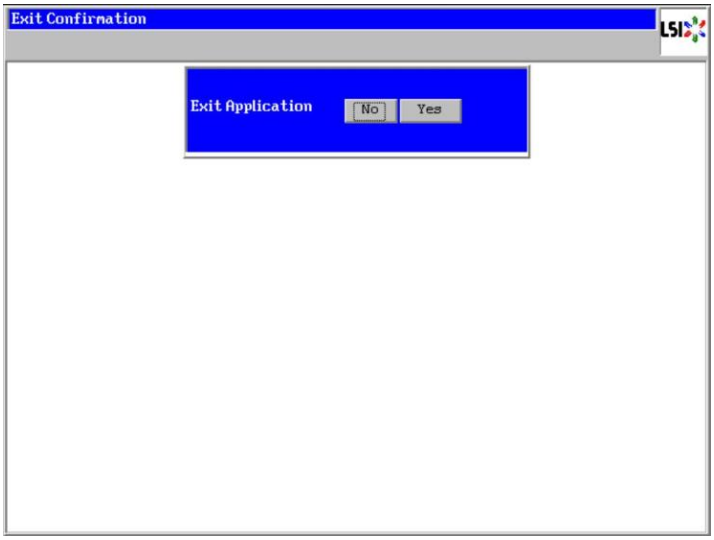
Ending Procedure

Use the following procedure to end the MegaRAID WebBIOS.

Firmware version: 2.110.63-1184

1 From the main menu, click **Next** and then **Exit**.
The exit confirmation screen appears.

Tip When you want to return to the main menu, click Home or .



2 Click **Yes**.
Clicking **No** returns you to the main menu.

3 When the following message appears, power off the system equipment. Or, with the remote console application (Reclient), click **C+A+D** in the toolbar of the system console; with the remote console application (Java application), click **Keyboard > (Ctrl+Alt+Del)** in the toolbar, or press the **Alt + L** keys, to restart the system equipment.

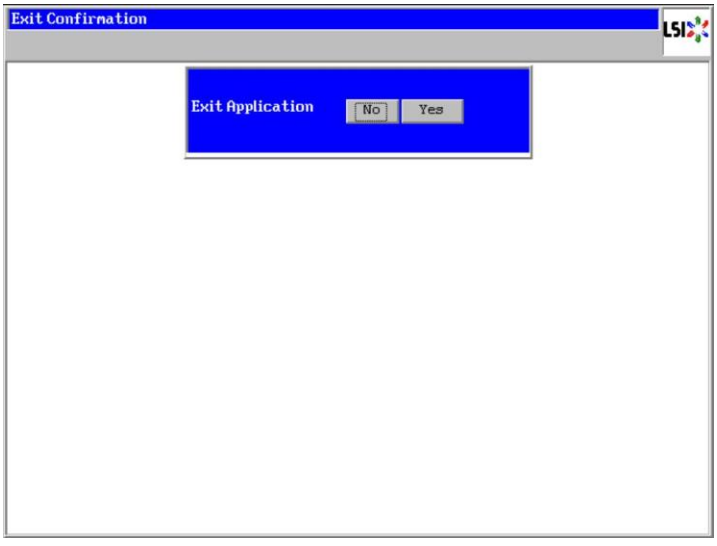


Firmware version: 2.120.233-1474 or later

1 From the main menu, click **Exit**.

The exit confirmation screen appears.

Tip When you want to return to the main menu, click Home or .



2 Click **Yes**.

Clicking **No** returns you to the main menu.

3 When the following message appears, power off the system equipment. Or, with the remote console application (Reclient), click **C+A+D** in the toolbar; with the remote console application (Java application), click **Keyboard > (Ctrl+Alt+Del**) in the toolbar, or press the **Alt + L** keys, to restart the system equipment.



Tip

For the remote console (Reclient), see the Hitachi Compute *Blade 2000 Remote Console Application User's Guide* contained in the remote console application CD that came with the system equipment.

For the remote console (Java application), see "Remote Console Application (Java Application)" in Chapter 3.

❑ Operation for MegaRAID WebBIOS

For MegaRAID WebBIOS, you can set individual items by using the following keys.

Connect a mouse to the remote console before starting MegaRAID WebBIOS.

Key/mouse	Operation
Mouse	Moves the mouse cursor.
Mouse - left button	- Selects an item that the mouse cursor is placed on. - Moves the cursor to an item to which the mouse cursor points. - Selects a disk array or physical hard disk.
0 to 9	Enters numerical values.
Ctrl	Selects multiple disk arrays or hard disks.
Del, Back Space	Deletes an entered value.

❑ Key operation for MegaRAID WebBIOS

This section describes how to operate the MegaRAID WebBIOS only with the keyboard.

Operating MegaRAID WebBIOS with Keyboard

You can set the following items for MegaRAID WebBIOS using the keyboard.

Key	Operation
Tab	Moves the cursor in order. *1
Shift + Tab *2	Moves the cursor in reverse order.
Enter, Space	- Selects the item that the cursor is put on. - Determines an item setting. - Determines a disk array or physical hard disk.
[↑], [↓]	- Selects a disk array or physical hard disk. - Selects a setting value.
Shift	Selects multiple disk arrays or hard disks.
0 to 9	Inputs a numerical value.
Del, Back Space	Deletes an entered value.

*1 The item selected by the cursor is encircled by the dotted line.

*2 **Shift + Tab** is to press the **Tab** key while pressing the **Shift** key.



It may be hard to find the cursor on some screens. In this case, press the **Tab** key or **Shift + Tab** keys to move the cursor so that you can see it, and then move the cursor to the position to perform the operation.

Screen composition for MegaRAID WebBIOS

The main menu of the MegaRAID WebBIOS utility includes the Menu Icon, which is not used in operation with the keyboard.

Operation in MegaRAID WebBIOS setting/disk array configuration

When operating MegaRAID WebBIOS only with the keyboard, replace the mouse with the keyboard as follows:

- Click (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.
- Place a check mark in (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.

Execute a specific operation in setting or configuring a disk array, as follows:

- Select **Menu> Logical View > Physical View** in the main menu:

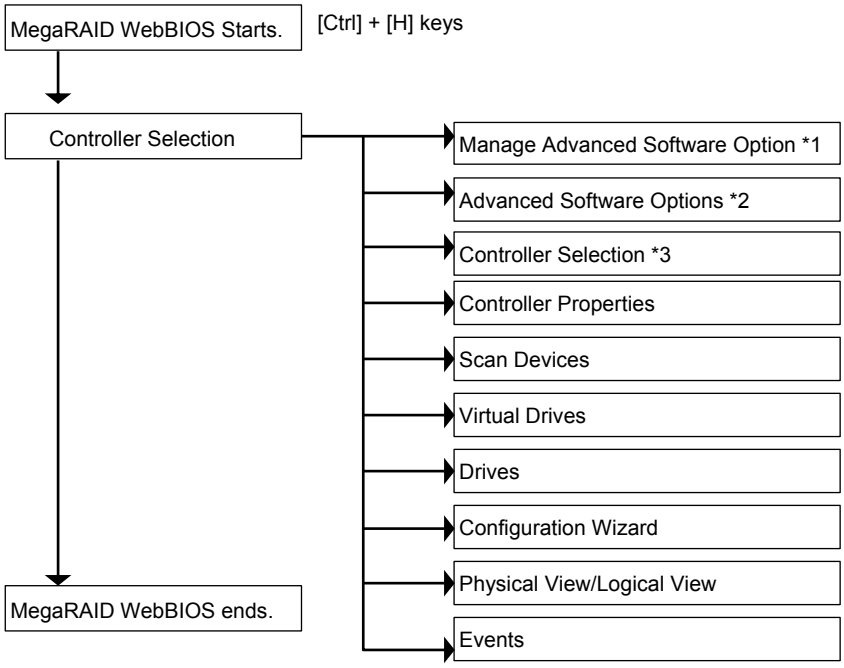
  Press the **Tab** key or press the **Tab** key while pressing the **Shift** key to move the cursor among **Menu**, **Logical View**, and **Physical View**.
  - When displaying the main menu, press the **Tab** key seven times to move the cursor to **Controller Selection** that is selected.
  - Move the cursor to **Events** or **Exit** using the **Tab** key. With the cursor on **Events** or **Exit**, press the **Tab** key once, and the cursor moves to **Logical View** or **Physical View** that is selected on the right of the screen.
  - With the cursor on **Logical View** or **Physical View**, press the **Tab** key twice, and the cursor moves to that is selected on the upper left of the screen.



- You can select a hard disk or disk array using the [↑] and [↓] keys on the selection screen of **Logical View** or **Physical View**.
- Setting items in each menu.
  To change a setting value, put the cursor on the setting item box and select a new setting value using the [↑] and [↓] keys, or enter the setting value using the numerical keys.
- Selecting multiple hard disks in disk array configuration.
  Press and hold the **Shift** key and select hard disks using the [↑] and [↓] keys, and then press **Enter** or **Space** key.

❑ Configuration of MegaRAID WebBIOS

The MegaRAID WebBIOS is configured as shown below.



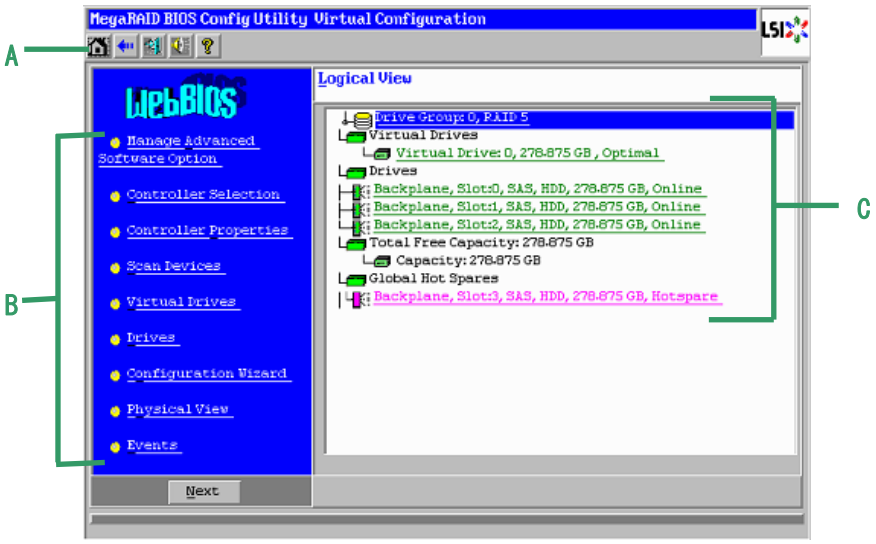
*1 This item is displayed for firmware version; 2.110.63-1184.

*2 This item is displayed for firmware version; 2.120.233-1474

*3 “Adapter Selection” is displayed on the Controller Selection window.

❑ Screen configuration of MegaRAID WebBIOS

The following screen shows the MegaRAID WebBIOS configuration.



A Menu icon

The following icons are available.

Icons	Description
	Return to the main menu.
	Return to the previous screen
	End the utility.
	Temporarily stop ringing the buzzer on the disk array controller board. *1
	Display the version of MegaRAID WebBIOS,

*1 This function is not supported.

B Menu

Menu items for MegaRAID WebBIOS are displayed. Click each item to go to the respective menu screen.

C Logical View/Physical View

Hard disks or disk arrays connected to the disk array controller are displayed.

Tip

Click a hard disk from disks displayed in **Logical View** or **Physical View**, and the same screen is displayed as when you select **Drives > Properties** from the menu.

Select a disk array from disks displayed in **Logical View**, and the same screen is displayed as when you select **Virtual Drives > Properties** from the menu.

❑ Setting items for MegaRAID WebBIOS

This section describes the setting items and values for MegaRAID WebBIOS.

- The same alphanumeric characters are used to associate the setup screen and each of the items.
- In the table, the underlined values are Default values. Those in brackets [ ] are recommended values.

  Example:

  [Enabled (valid)]/Disabled (invalid): "Enabled" is the Default and also the recommended value.

  [Enabled (valid)]/Disabled (invalid): "Disabled" is the Default value; and "Enabled" is the recommended value, which requires a setting change.

  When you need to change the setting from the Default to the recommended value, the recommended value is emphasized in red.

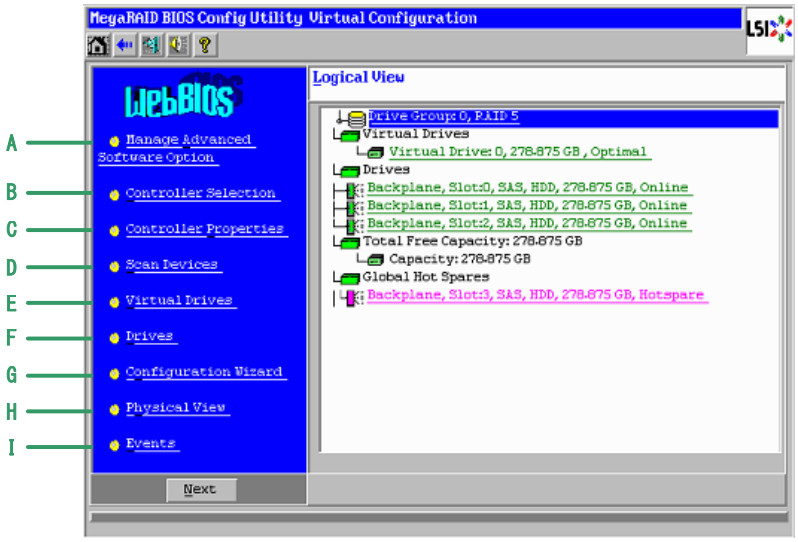
Note

Unless otherwise specified, use the recommended values for all setting items. If you set non-recommended values, the equipment is not supported and might not operate properly.

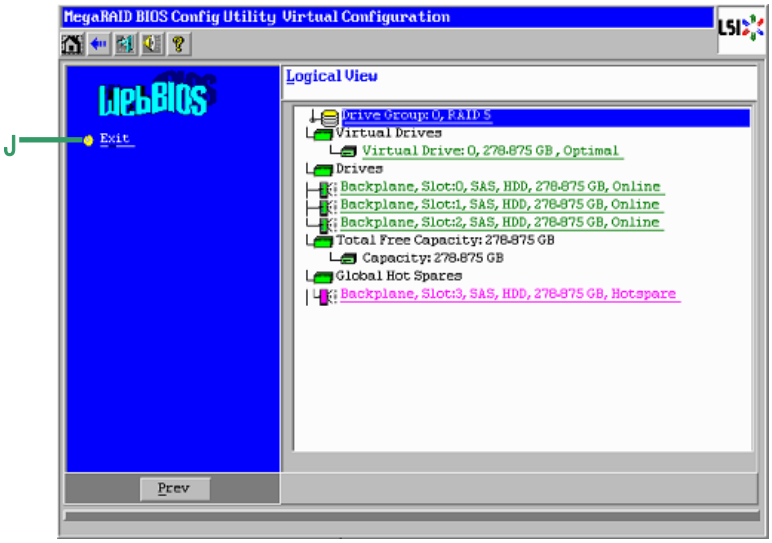
Main menu

Start MegaRAID WebBIOS, and the following main menu appears:

Firmware version; 2.110.63-1184



When you click **Next**, the following screen appears:



When you click **Prev**, the screen returns to the previous screen.

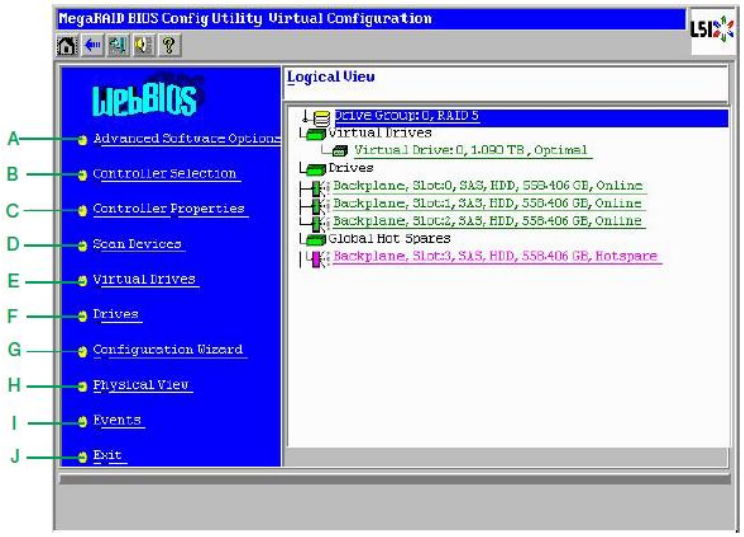
Menu		Content	Setting/display value
A	Manage Advanced Software Option	Setting advanced functions	-
B	Controller Selection *1	Selecting the disk array controller to be operated	-
C	Controller Properties	Viewing and setting the hardware information on the disk array controller board	See Controller properties: Menu for setting the disk array controller board.
D	Scan Devices	Scanning the installed devices	-
E	Virtual Drives	Viewing and setting the disk array (logical drive) information	See Virtual drives: Viewing and setting disk array information.
F	Drives	Viewing and setting the hard disk (physical drive) information	See Drives: Viewing physical hard disk information.
G	Configuration Wizard	Building or formatting disk arrays	See Building disk arrays.
H	Physical View/Logical View	Switching display modes	See Switching the display mode.
I	Events	Displaying events	-
J	Exit	Ending the MegaRAID WebBIOS	See Ending procedure in Starting and ending MegaRAID WebBIOS.

*1 Adapter Selection is displayed on the Controller Selection screen.



Do not use **Manage Advanced Software Option** and **Events** because they are not supported.

Firmware version; 2.120.233-1474 or later



Menu		Content	Setting/display value
A	Advanced Software Options	Setting advanced functions	-
B	Controller Selection *1	Selecting the disk array controller to be operated	-
C	Controller Properties	Viewing and setting the hardware information on the disk array controller board	See "Controller properties: Menu for setting the disk array controller board".
D	Scan Devices	Scanning the installed devices	-
E	Virtual Drives	Viewing and setting the disk array (logical drive) information	See "Virtual drives: Viewing and setting disk array information".
F	Drives	Viewing and setting the hard disk (physical drive) information	See "Drives: Viewing physical hard disk information".
G	Configuration Wizard	Building or formatting disk arrays	See "Building disk arrays".
H	Physical View/Logical View	Switching display modes	See "Switching the display mode.
I	Events	Displaying events	-
J	Exit	Ending the MegaRAID WebBIOS	See Ending procedure in Starting and ending MegaRAID WebBIOS.

*1 Adapter Selection is displayed on the Controller Selection screen.

Tip

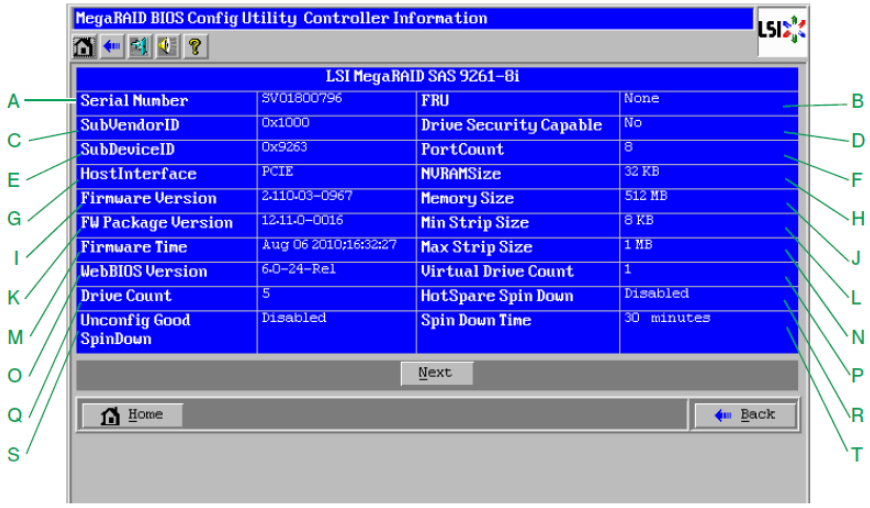
Do not use **Advanced Software Options** and **Events** because they are not supported.

Controller properties: Menu for setting the disk array controller board

You can display and set the hardware information about the disk array controller board.

Select **Controller Properties** from the main menu. The following screen appears:

Firmware version; 2.110.63-1184

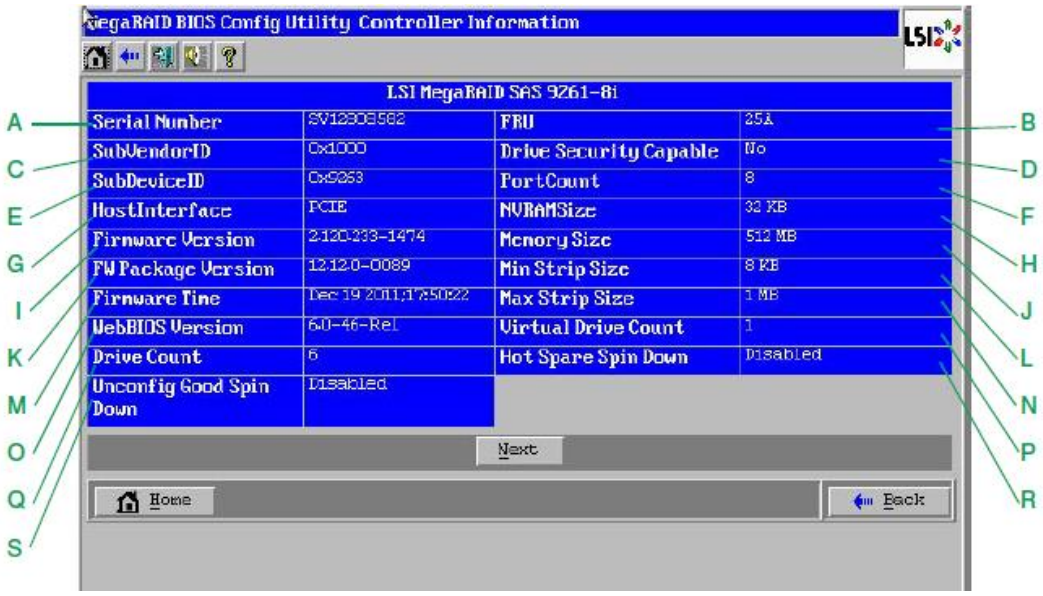


Display item		What is displayed
A	Serial Number	Serial number
B	FRU	Board name per maintenance
C	SubVendorID	Sub-vendor ID
D	Drive Security Capable	Encryption function: Enable or Disable
E	SubDeviceID	Sub-device ID
F	PortCount	Number of ports installed
G	HostInterface	Host interface
H	NVRAM Size	Size of non volatile RAM (NVRAM) installed
I	Firmware Version	Firmware version
J	Memory Size	Size of memory installed
K	FW Package Version	Firmware package version
L	Min Stripe Size	Minimum stripe size
M	Firmware Time	Current time at which the firmware acquires
N	Max Stripe Size	Maximum stripe size
O	WebBIOS Version	MegaRAID WebBIOS version
P	Virtual Drive Count	Exisiting number of array configurations (logical devices)
Q	Disk Count	Number of physical devices installed
R	Hot Spare Spin Down	Power capping mode set to a hard disk with hotspare
S	Unconfig Good Spin Down	Power capping mode set to unused hard disks
T	Spin Down Time	Time required for the power capping mode

Tip

You cannot change those settings for the items displayed here.

Firmware version; 2.120.233-1474 or later



Display item		What is displayed
A	Serial Number	Serial number
B	FRU	Board name per maintenance
C	SubVendorID	Sub-vendor ID
D	Drive Security Capable	Encryption function: Enable or Disable
E	SubDeviceID	Sub-device ID
F	PortCount	Number of ports installed
G	HostInterface	Host interface
H	NVRAM Size	Size of NVRAM installed
I	Firmware Version	Firmware version
J	Memory Size	Size of memory installed
K	FW Package Version	Firmware package version
L	Min Stripe Size	Minimum stripe size
M	Firmware Time	Current time at which the firmware acquires
N	Max Stripe Size	Maximum stripe size
O	WebBIOS Version	MegaRAID WebBIOS version
P	Virtual Drive Count	Exisiting number of array configurations (logical devices)
Q	Disk Count	Number of physical devices installed
R	Hot Spare Spin Down	Power capping mode set to a hard disk with hopspare
S	Unconfig Good Spin Down	Power capping mode set to unused hard disks

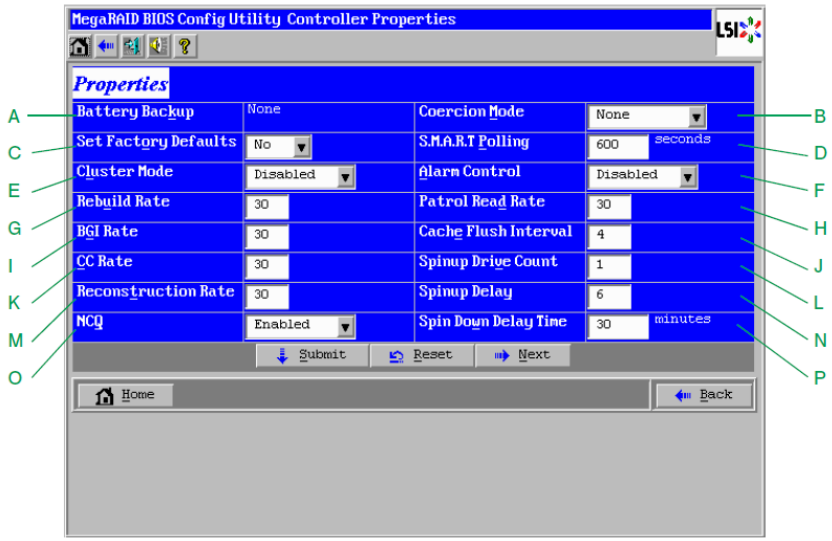
Tip

You cannot change the settings for those items displayed here.

Properties: Controller properties submenu 1

Click **Next** in the **Controller Properties** screen, and the following screen appears:

Firmware version; 2.110.63-1184



Display item		Display/content	Setting/display value **
A	Battery Backup	Battery backup unit mount status.	None
B	Coercion Mode *1	Setting the capacity control for the physical hard disk used for disk array building	[None (using the entire capacity)] / 128 MB-way (using a capacity as a multiple of 128 MB) / 1 GB-way (using a capacity as a multiple of 1 GB)
C	Set Factory Defaults *2	Returning all the settings to their Defaults values	—
D	S.M.A.R.T Polling *4	Setting the interval of S.M.A.R.T. reporting	0 to 65535 / 300 / [600]
E	Cluster Mode *3	Setting the cluster mode	[Disabled (invalid)] / Enabled (valid)
F	Alarm Control	Sounding the buzzer on the controller in the event of a fault at a connected device	[Disabled (not sounding)] / Enabled (sounding) / Silence (stop sounding temporarily)
G	Rebuild Rate *3	Priority of rebuilding	0 to 100 / [30]
H	Patrol Read Rate *3	Priority of patrol reading	0 to 100 / [30]
I	BGI Rate *3	Priority of background initializing	0 to 100 / [30]
J	Cache Flush Interval *3	Flash timing for write-cache data	1 to 255 / [4]
K	CC Rate *3	Priority of integrity inspection	0 to 100 / [30]
L	Spinup Drive Count *4	Number of hard disk motors started at system startup	0 to 8 / [1]
M	Reconstruction Rate *3	Priority of capacity expansion	0 to 100 / [30]
N	Spinup Delay *4	Timing for hard disk motors started at system startup	0 to xxx / [6]
O	NCQ *4	Setting the NCQ command	[Enabled] / Disabled

Display item		Display/content	Setting/display value **
P	Spin Down Delay Time *4	Setting the saving mode to a hard disk	0 to 1440 / [30]

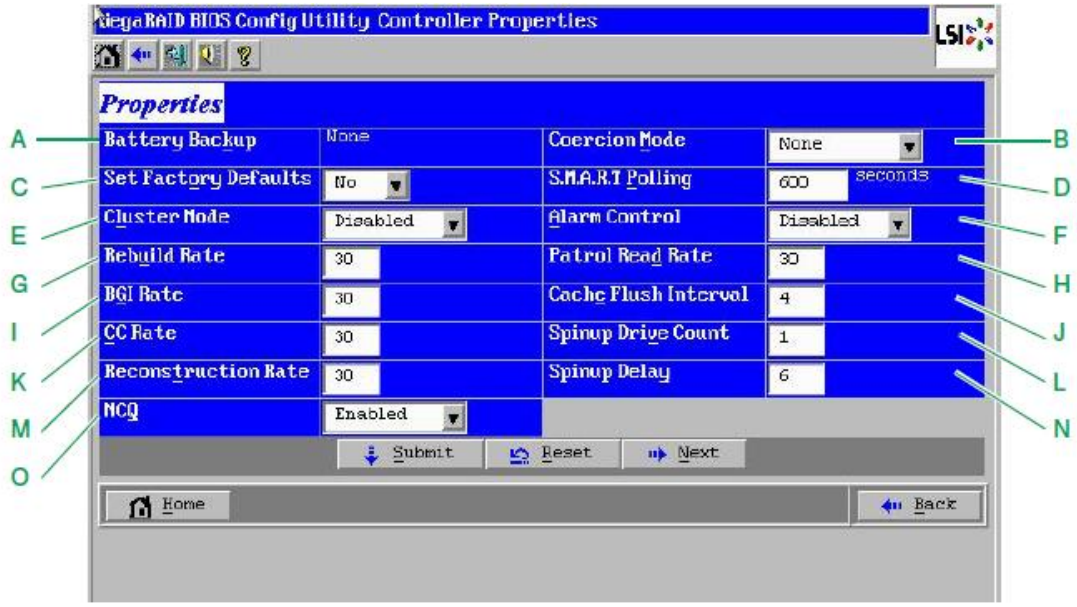
*1 This can be changed only when no disk arrays have been set at all.

*2 Do not use **Set Factory Defaults**. This setting must be changed to the recommended values.

*3 Change the value to the recommanded value.

*4 Always use the **Default** setting.

Firmware version; 2.120.233-1474 or later



Display item		Display/content	Setting/display value **
A	Battery Backup	Battery backup unit mount status.	None
B	Coercion Mode *1	Setting the capacity control for the physical hard disk used for disk array building	[None (using the entire capacity)] / 128MB-way (using a capacity as a multiple of 128MB) / 1GB-way (using a capacity as a multiple of 1GB)
C	Set Factory Defaults *2	Returning all the settings to their Defaults values	—
D	S.M.A.R.T Polling *4	Setting the interval of S.M.A.R.T. reporting	0 to 65535 / 300 / [600]
E	Cluster Mode *3	Setting the cluster mode	[Disabled (invalid)] / Enabled (valid)
F	Alarm Control	Sounding the buzzer on the controller in the event of a fault at a connected device	[Disabled (not sounding)] / Enabled (sounding) / Silence (stop sounding temporarily)
G	Rebuild Rate *3	Priority of rebuilding	0 to 100 / [30]
H	Patrol Read Rate *3	Priority of patrol reading	0 to 100 / [30]
I	BGI Rate *3	Priority of background initializing	0 to 100 / [30]
J	Cache Flush Interval *3	Flush timing for write-cache data	1 to 255 / [4]
K	CC Rate *3	Priority of consistency inspection	0 to 100 / [30]
L	Spinup Drive Count *4	Number of hard disk motors to start	0 to 8 / [1]

Display item		Display/content	Setting/display value **
		at system startup	
M	Reconstruction Rate *3	Priority of capacity expansion	0 to 100 / [30]
N	Spinup Delay *3	Timing for hard disk motors to start at system startup	0 to xxx / [6]
O	NCQ *4	Setting the NCQ command	[Enabled] / Disabled

*1 This can be changed only when no disk arrays have been set at all.

*2 Do not use **Set Factory Defaults**. This setting must be changed to the recommended values.

*3 Change the value to the recommanded value.

*4 Always use the **Default** setting.



- Place the mouse cursor on a setting item and left-click the mouse to change the setting values. Or, left-click the mouse to move the cursor and enter a value from the keyboard. Click **Submit** after the setting.
- Values of **Spin Drive Count** and **Spin Delay** are fixed, which will not take effect even though you have changed the values.

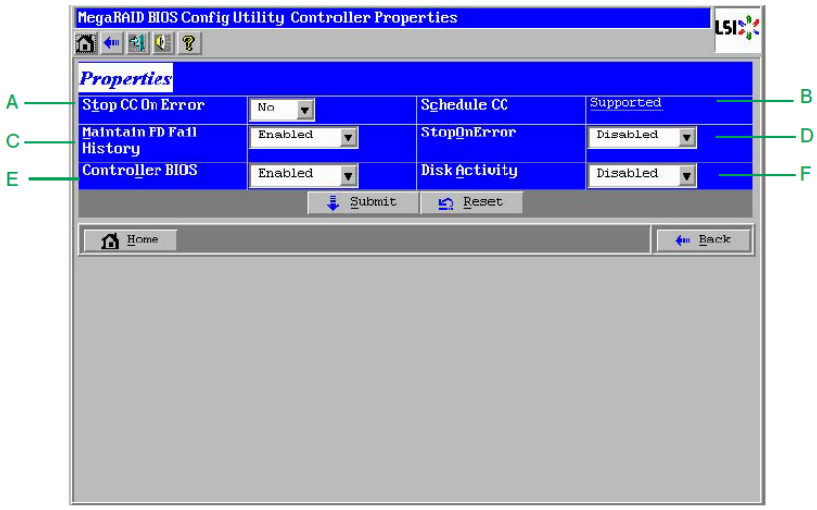
Properties: Controller properties submenu 2

Click **Next** in the **Properties: Controller properties submenu 1** screen, and the following screen appears.

Firmware version; 2.110.63-1184

Note

Stop CC On Error, Schedule CC, Maintain PD Fail History, and Disk Activity are not supported. Do not set those items.



Setting item		Description	Setting/display value **
A	Stop CC On Error *1	Sets an operation when an error is detected at the consistency check.	[No (continuous operation)] / Yes (stops the consistency check.)
B	Schedule CC *1	Sets a consistency check schedule.	When clicking [Supported], the screen moves to “Schedule CC Page: Schedule Consistency Check setting submenu”.
C	Maintain PD Fail History *1	Sets whether or not a failed hard disk can be used.	[Enabled (Registers failed hard disk information.)] / Disabled (Not register failed hard disk information.)
D	Stop On Error *2	Sets whether or not to boot the OS when an error is detected during the consistency check.	[Disabled)] / Enabled
E	Controller BIOS	Sets the disk array controller BIOS.	[Enabled)] / Disabled
F	Disc Activity *1	Sets hard disk LED switching.	[Disabled)] / Enabled

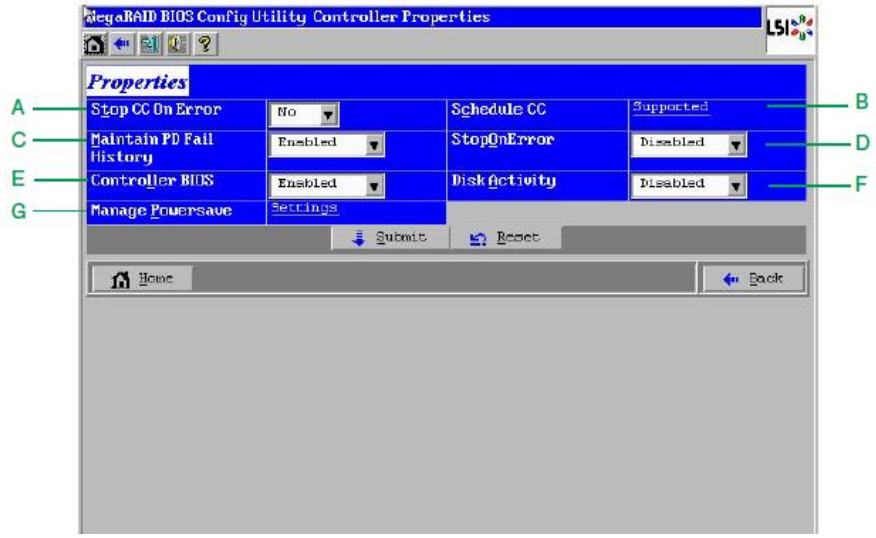
*1 Do not set this item, which is not supported.

*2 Make sure to use this item with the default setting.

Firmware version; 2.120.233-1474 or later

Note

Stop CC On Error, Schedule CC, Maintain PD Fail History, Disk Activity and Manage Powersave are not supported. Do not set those items.



Setting item		Description	Setting/display value **
A	Stop CC On Error *1	Sets an operation when an error is detected at the consistency check.	[No (continuous operation)] / Yes (stops the consistency check.)
B	Schedule CC *1	Sets a consistency check schedule.	When clicking [Supported], the screen moves to “Schedule CC Page: Schedule Consistency Check setting submenu”.
C	Maintain PD Fail History *1	Sets whether or not a failed hard disk can be used.	[Enabled (Registers failed hard disk information.)] / Disabled (Not registers failed hard disk information.)
D	Stop On Error *2	Sets whether or not to boot the OS when an error is detected at the system startup.	[Disabled)] / Enabled
E	Controller BIOS	Sets the disk array controller BIOS	[Enabled)] / Disabled
F	Disc Activity *1	Sets hard disk LED switching.	[Disabled)] / Enabled
G	Manage Powersave *1	Manages power saving	Click “Settings” to go to Power save setting: Power save setting sub menu .

*1 Do not set this item, which is not supported.

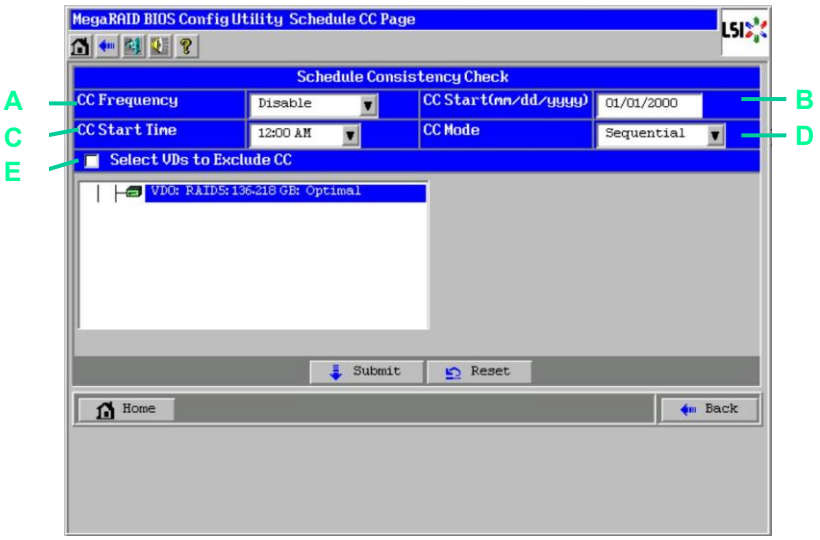
*2 Make sure to use this item with the default setting.

Schedule CC page: Schedule consistency check setting submenu

Click **Supported** of Schedule CC in the **Properties: Controller Properties submenu 2** screen, and the following screen appears.

Note

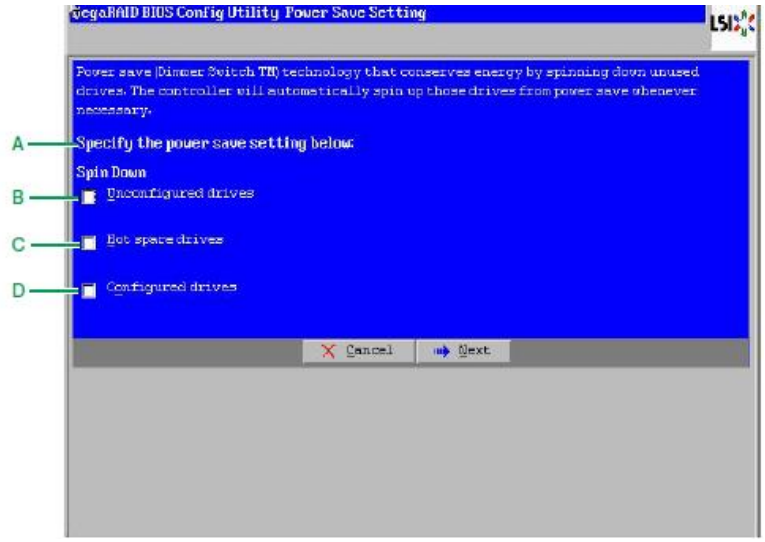
The following items are not supported. Do not set those items.



Setting item		Description	Setting/display value **
A	CC Frequency	Sets the CC schedule function: Enable or Disable	[Disable (invalid schedule)] / Enabled (valid schedule)
B	CC Start (mm/dd/yyyy)	Sets on what date the consistency check starts.	Choose any date.
C	CC Start Time	Sets on what time the consistency check starts.	12:00 AM. to 11:00 PM. / [The nearest to the present time]
D	CC Mode	Sets if the consistency check is executed on multiple disk arrays.	[Sequential (a consistency check per array)] / Concurrent (a consistency check on multiple arrays)
E	Select VDs to Execute CC	Specifies a disk array on which the consistency check is executed.	Choose any array configuration.

Power save setting: Power save setting sub menu

On the **Properties: Controller properties submenu 2 screen**, click **Manage Powersave > Settings** to show the following screen. This item, however, is not supported by this system. Leave all values at their default setting.

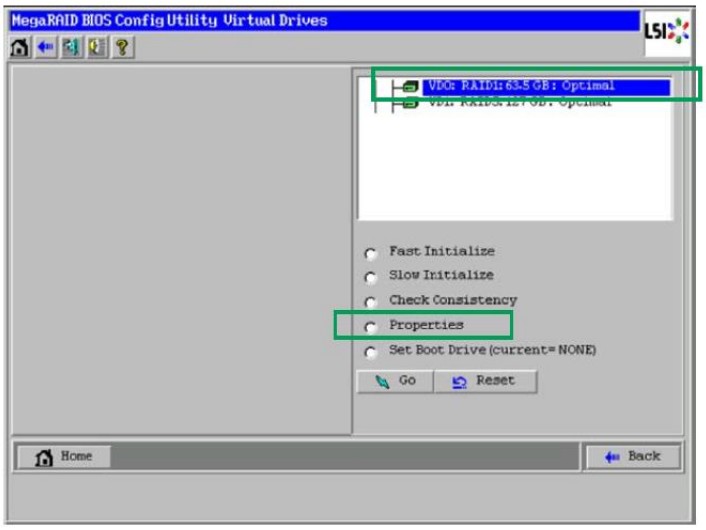


Setting item		Description	Setting/display value **
A	Specify the power save setting below *1	Displays disk power saving settings	Setting items is described in item B to D.
B	Unconfigured drivers	Enables/Disables unused disks.	Checked: enabled [Unchecked: disabled]
C	Hot spare drives	Enables/Disables a hot-spared disk.	Checked: enabled [Unchecked: disabled]
D	Configured drives	Enables/Disables disks used for disk arrays.	Checked: enabled [Unchecked: disabled]

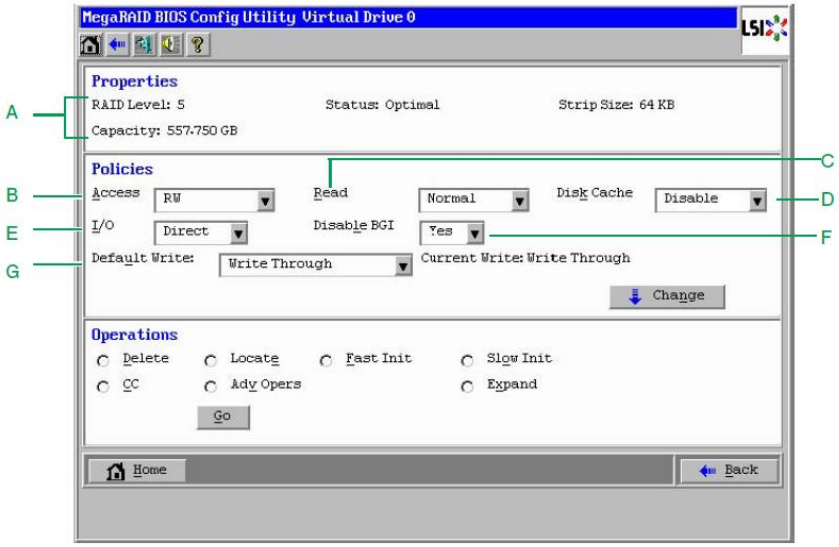
Virtual drives: Viewing and setting disk array information

You can view and change the information on the disk array (logical drive) that is already set.

Select **Virtual Drives** in the main menu, and the following screen appears:



Select a disk array for viewing information and changing the setting from the list on the upper right of the screen. Check **Properties** and then click **Go**, and the disk array properties screen appears.



NOTICE

When enabling the write cache of the disk array, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

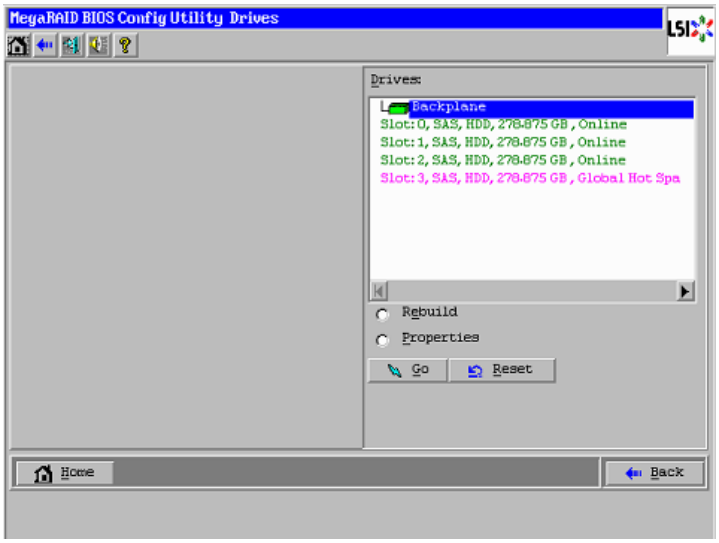
Display item		What is displayed	Setting/display value **
A	RAID Level	RAID level	-
	Status	Status of the disk array	-
	Strip Size	Stripe size of the disk array	-
	Capacity	Size of the disk array	-
B	Access	Access mode	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
C	Read	Read policy	[Normal (no advance reading)] / Ahead (always advance reading) / Adaptive (advance reading only in the event of sequential access)
D	Disk Cache	Setting the cache installed in a physical hard disk	[Disable (cache: not used)] / [Enable (cache: used) / No change (based on the hard disk setting)]
E	I/O	Setting the read-cache operation	[Direct (reading from the cache at a cache hit)] / [Cached (always reading from the cache)]
F	Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
G	Default Write*1	Setting the write cache	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)

*1 Default Write supports setting in Always Write Back only when the system equipment is connected to UPS. Even so, set **Write through** when installing OS. Otherwise, the installation may not finish properly. Do not set **Write Back with BBU**.

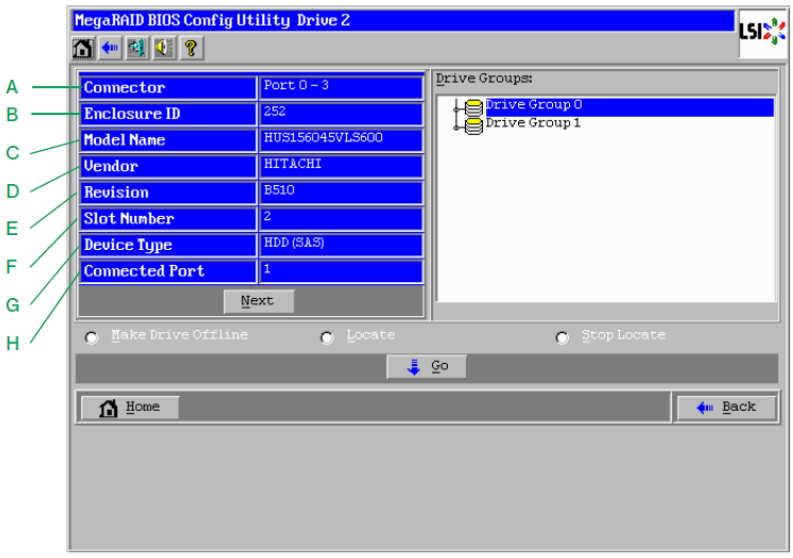
Drives: Viewing physical hard disk information

Here you display the information on the physical hard disk in the physical drive connected to the disk array controller.

Select **Drives** in the main menu and the following screen appears:

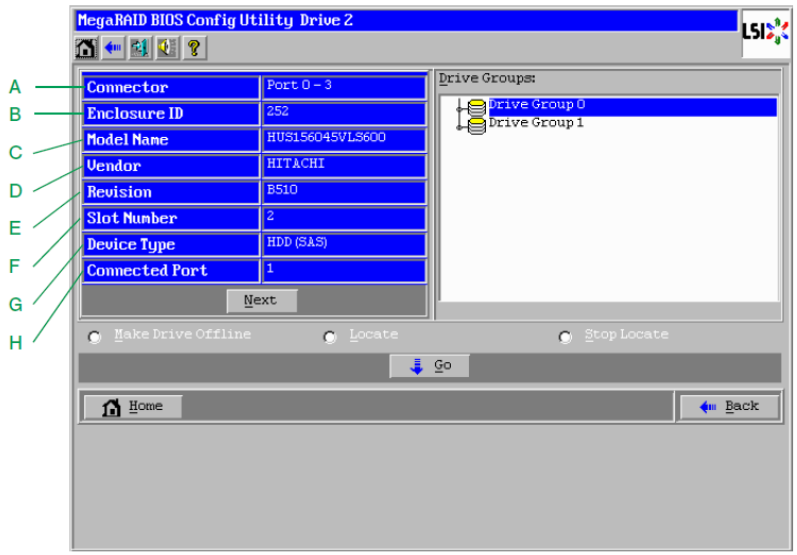


Select a disk array for viewing and setting information from the list on the upper right of the screen. Check **Properties** and then click **Go**. The hard disk properties screen appears.



When clicking **Next**, you can view the following screen.

Drives properties: Disk properties menu 1



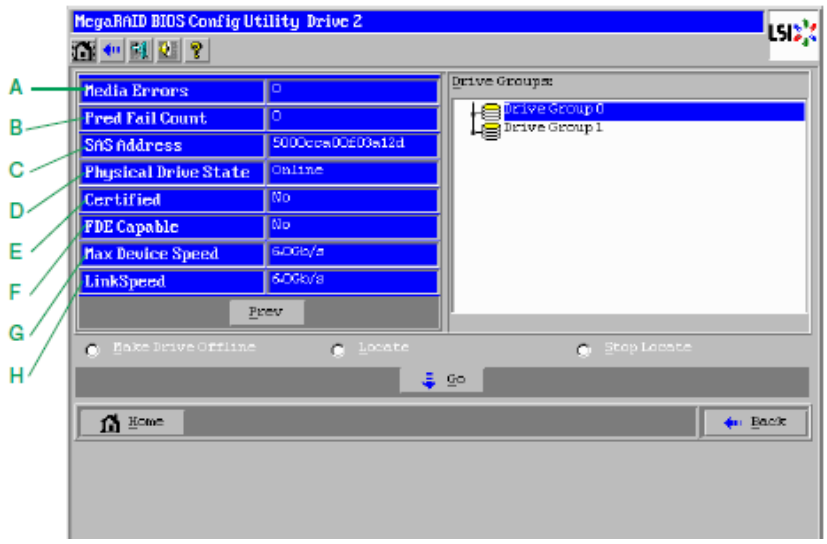
Display item		What is displayed
A	Connector	Disk array controller board connector connected
B	Enclosure ID	ID number of the enclosure device connected
C	Model Name	Disk model name
D	Vendor	Vendor name
E	Revision	Firmware version
F	Slot Number	Number of the slot installed
G	Device Type	Device type
H	Connected Port	Port number of the disk array controller board connected

Tip

You cannot change the settings for those items displayed here.

Drives properties: Disk properties menu 2

Firmware version; 2.110.63-1184

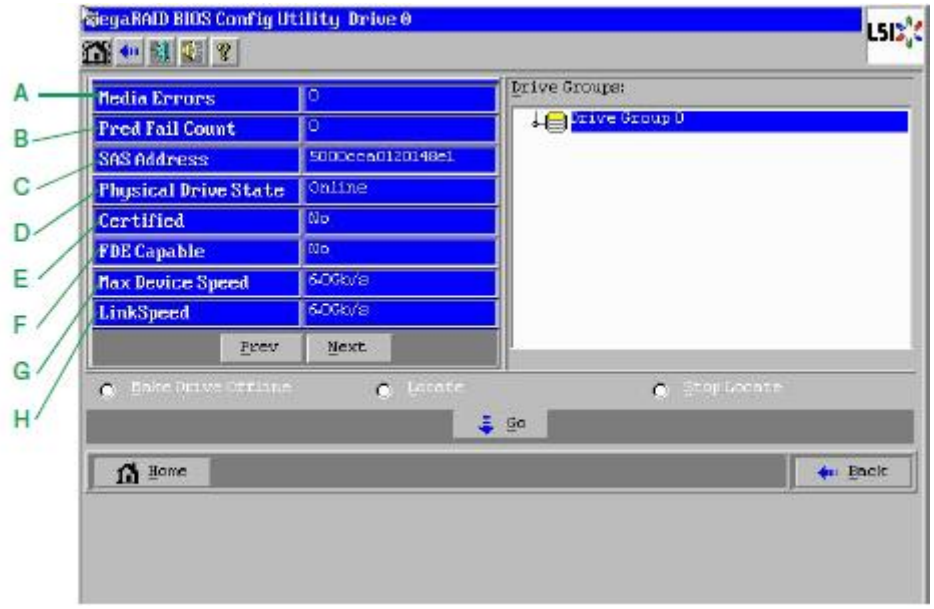


Display item		What is displayed
A	Media Errors	Number of media errors detected
B	Pred Fail Count	Number of S.M.A.R.T. warnings reported
C	SAS Address	SAS address
D	Physical Drive State	Physical hard disk status
E	Certified	Certification
F	FDE Capable	Full Disk Encryption: Capable or No
G	Max Device Speed	The maximum connection speed
H	Link Speed	Link speed

Tip

- Items described in the table above cannot be changed.
- For the status of the physical hard disk, see Status.
- Media Errors and Pred Fail Count are cleared when the system power is turned off.

Firmware version; 2.120.233-1474 or later



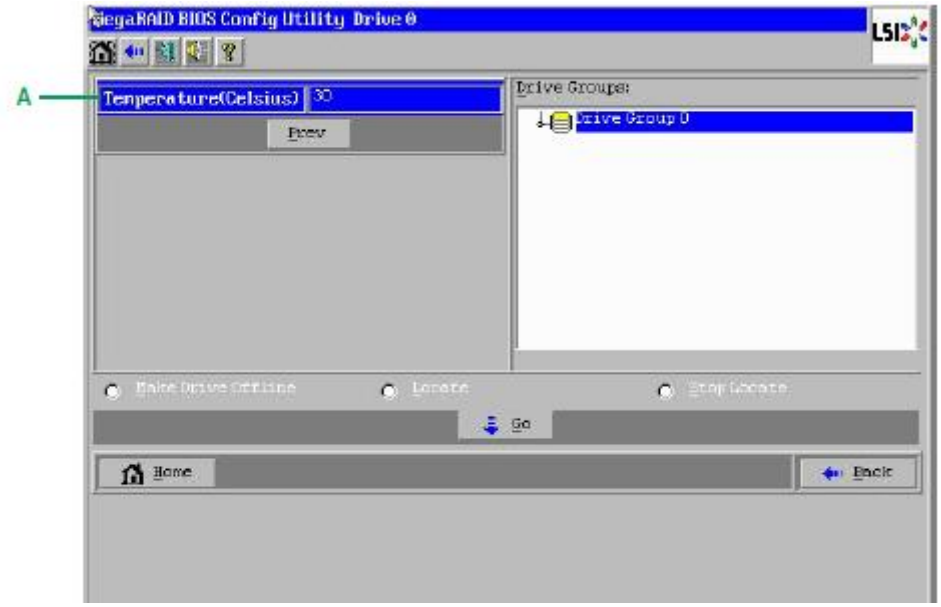
Display item		What is displayed
A	Media Errors	Number of media errors detected
B	Pred Fail Count	Number of S.M.A.R.T. warnings reported
C	SAS Address	SAS address
D	Physical Drive State	Physical hard disk status
E	Certified	Certification
F	FDE Capable	Full Disk Encryption: Capable or No
G	Max Device Speed	The maximum connection speed
H	Link Speed	Link speed

Tip

- Items described in the table above cannot be changed.
- For the status of the physical hard disk, see Status.
- Media Errors and Pred Fail Count are cleared when the system power is turned off.

Drives properties: Disk properties menu 3

Firmware version; 2.120.233-1474



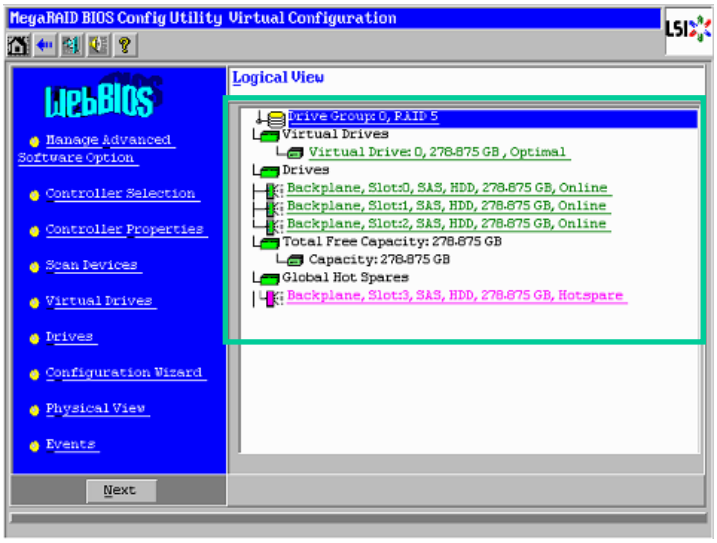
Display item		What is displayed
A	Temperature (Celsius)	Disk temperature

Tip You cannot change the setting for the item displayed here.

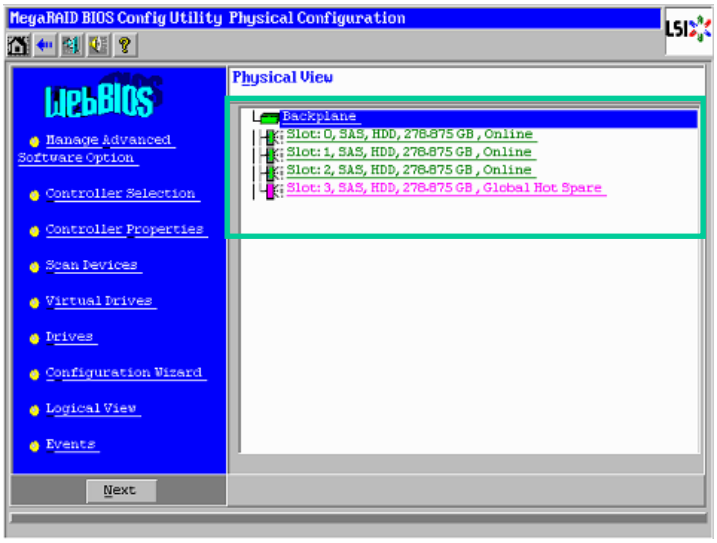
❑ Switching the display mode

This section describes switching disk array display modes in the main menu.

There are two types of display mode: Logical View and Physical View
The Logical View mode displays a list of disk array configurations that are already set, physical hard disks comprising a disk array configuration, and hot spare information.
The Physical View mode displays a list of physical hard disks.



Logical View mode:
Disk array/Physical hard disks/Global hot spare



Physical View mode:
List of physical hard disks

Tip

- The Logical View mode is applied when the MegaRAID WebBIOS is started.
- To switch to the physical view mode, click **Physical View** in the Logical View mode from the main menu.
- To switch to the logical view mode, click **Logical View** in the Physical View mode from the main menu.

❑ Building disk arrays

This section describes the procedure for building disk arrays.

The building of disk arrays should be entirely performed from the Configuration Wizard.

> ***NOTICE***
>
> You must not change the disk array during system operations. If you do, all data will be lost from those disks due to change in the disk array.

Note

Make sure to set each item to the recommended value unless other specific directions are given. Otherwise, the system might not properly operate. We are not responsible for a malfunction due to a setting except our recommended values.

Building disk arrays for RAID 0, 1, 5, and 6

This section describes the procedure for building new disk arrays.

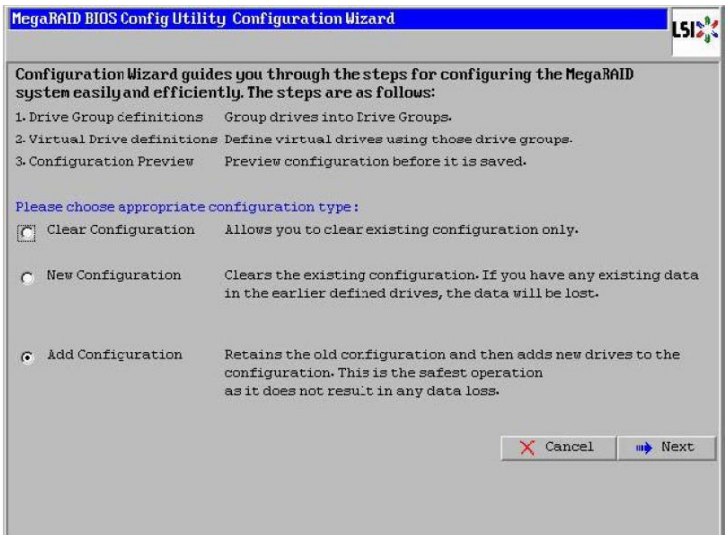
> ***NOTICE***
>
> RAID0 configuration (single hard disk configuration) has no redundancy. Thus, if the hard disk fails, all data will be lost.
>
> It is recommended that you use the system with RAID1/RAID5/RAID6/ RAID10 configuration to ensure data redundancy and improve resistance to failure.

Tip

To build RAID 10, see Building disk arrays for RAID 10.
For information about how to set hotspare, see Setting hotspares.

1 Select **Configuration Wizard** from the main menu.

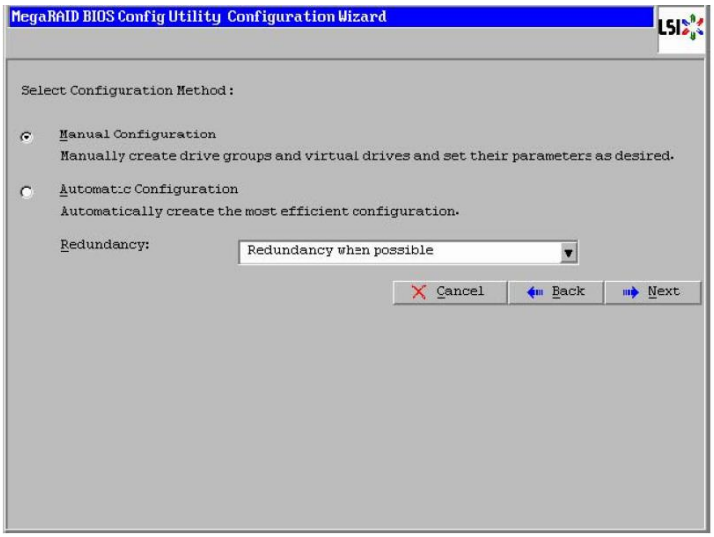
The following screen appears:



NOTICE

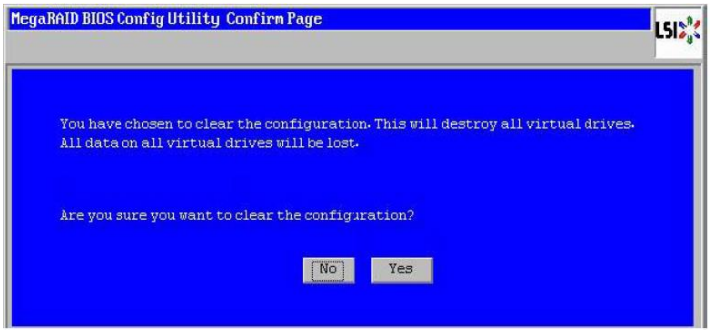
If you select **New Configuration**, all data in those hard disks including the disk array information will be lost. Backup your required data before selecting **New Configuration**.

2 Check **New Configuration** or **Add Configuration** and click **Next**.
The following screen appears:



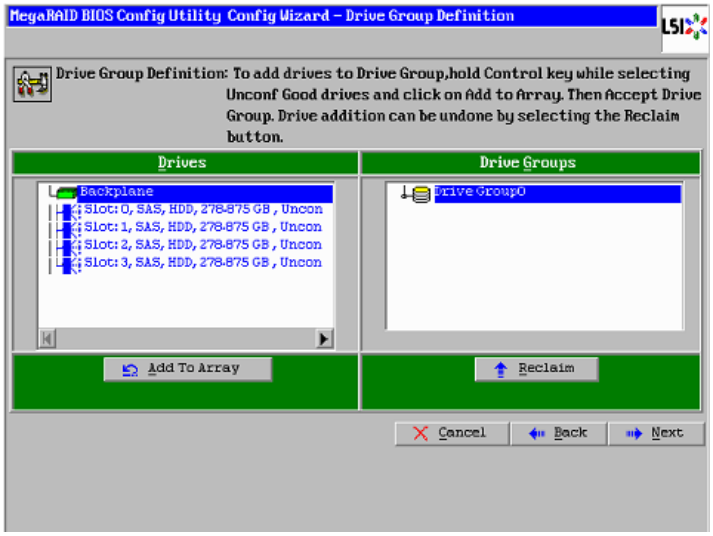
Tip

- The existing disk arrays will remain when you select **Add Configuration**. Add Configuration should be selected when you want to keep the existing disk arrays, and to build disk arrays using additional hard disks.
- If you select **New Configuration**, you lose the existing disk arrays. This should be selected when you discard the existing disk array and build a new one.
- If you select **New Configuration**, the following screen appears. Clicking **Yes** allows you to build a disk array.

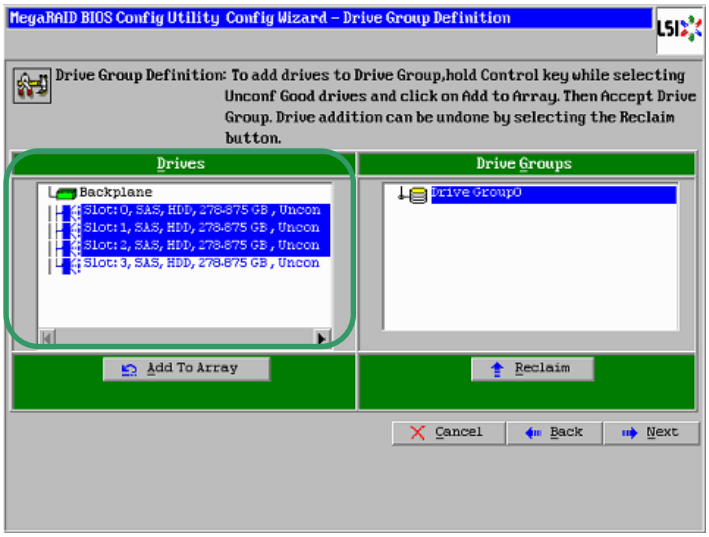


3 Check **Manual Configuration** and click **Next**.

The following screen appears:



4 Select a hard disk to be used for building a disk array.



The number of hard disks required varies depending on the RAID level to be set. The following table summarizes the number of hard disks required.

RAID level	Number of hard disks required
RAID 0	1 or more
RAID 1	2
RAID 5	3 or more
RAID 6	4 or more

Note

RAID 6 with 3 hard disks is not supported. If you set this, the system might not operate properly.

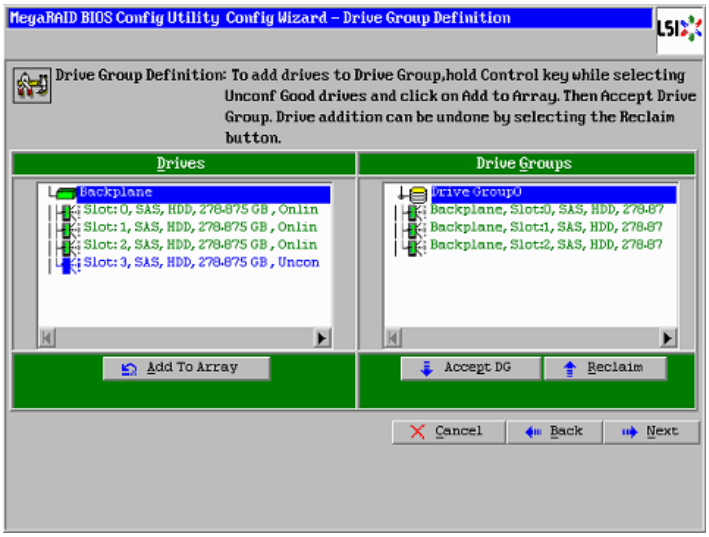
Tip

You can select only a hard disk whose status is **Unconfigured Good** (unused).

To select multiple hard disks, click them while pressing the **Ctrl** key.

5 After selecting all hard disks for building a disk array, click **Add to Array**.

Status of those selected hard disks is **Online** as shown in the **Drives** pane.

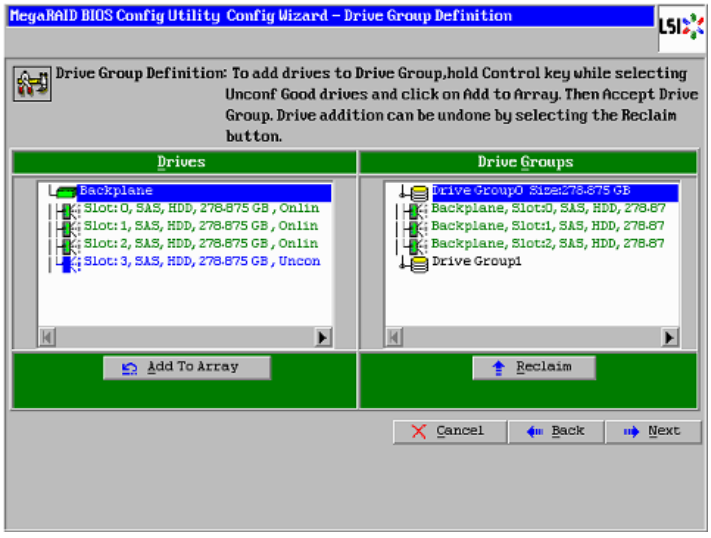


Tip

To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

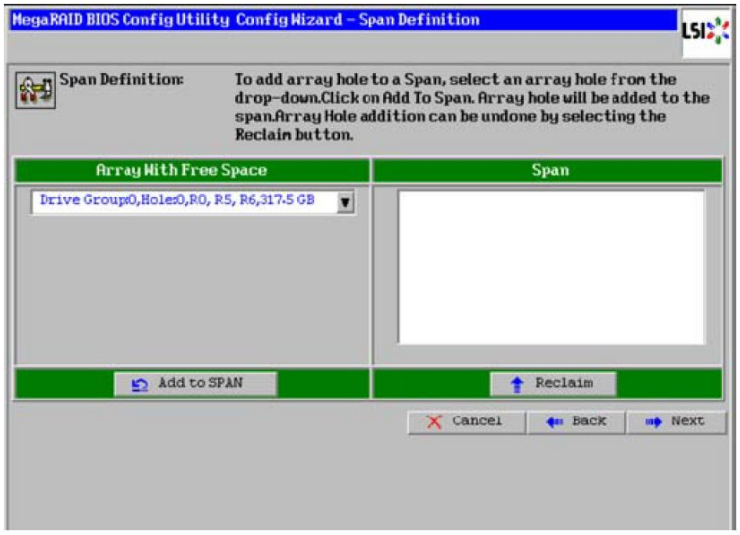
6 Click **Accept DG**.

The following screen appears:



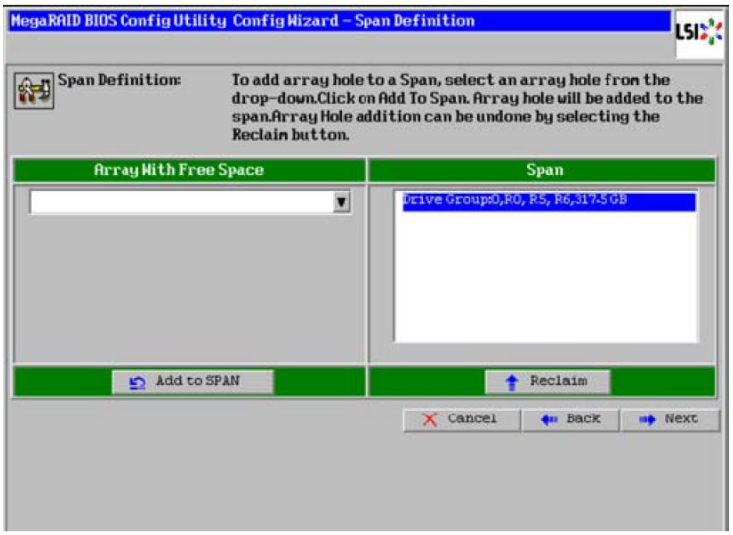
7 Click **Next**.

The following screen appears:



8 Click **Add to SPAN**.

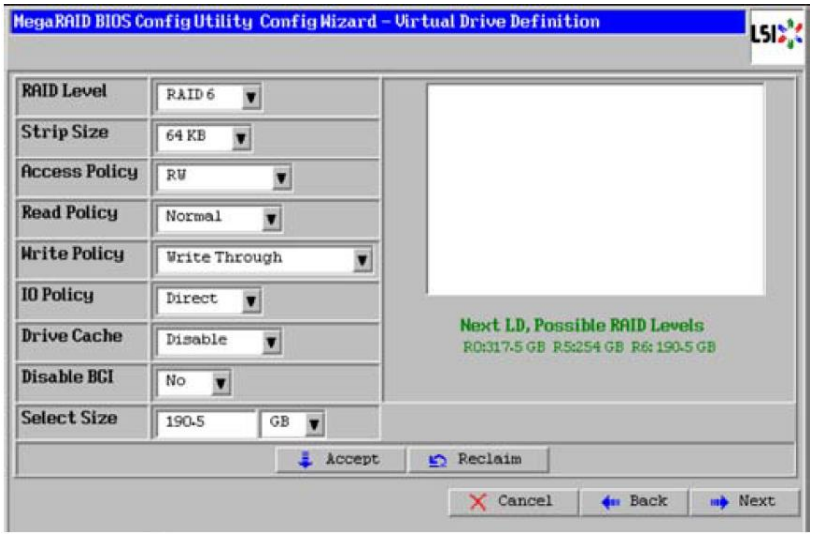
The following screen appears:



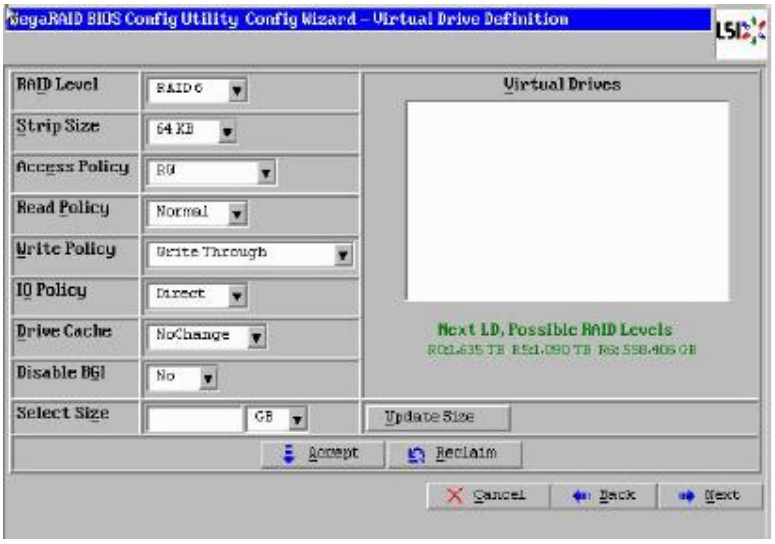
9 Click **Next**.

The following screen appears:

Firmware version; 2.110.63-1184



Firmware version; 2.120.233-1474 or later



10 Specify the RAID level, stripe size, read policy, write policy, and disk array size.

NOTICE

When enabling the write cache of the disk array, connect the system equipment to a UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Set each item value in the following table.

Item	Content	Setting value **
RAID Level *1	RAID Level	Specify any level.
Stripe Size *2	Stripe size (only RAID 0 and 5)	8 KB / 16 KB / 32 KB / [64 KB] / 128 KB / 256 KB / 512 KB / 1 MB
Access Policy	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advance reading)] / Ahead (always advance reading) / Adaptive (advance reading only in the event of sequential access)
Write Policy *3	Write policy	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)
IO Policy	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)
Drive Cache	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)
Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *4 *5	Size of a disk array	Entering the maximum capacity value.

*1 RAID 6 with three hard disks and RAID 1 with three or more hard disks are not supported.

*2 For RAID 1, set 64 KB by Default.

*3 In Write Policy, **Write Back** can be set only when the system equipment is already connected to the UPS (uninterruptible power supply). Confirm that the checkmark is removed from **Wrthru for BAD BBU** at that time. Even in this case, set **Write Through** when the operating system is installed. Otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays. Do not select **Write Back with BBU**.

*4 Maximum capacity size that can be set is shown under **Next LD, Possible RAID Levels** at the right of the screen. Change the maximum capacity value for your RAID level. Type the fraction portion of the maximum capacity value correctly and do not omit the value 0 (zero).

*5 For firmware version: 2.120.233-1474 or later, clicking **Update Size** inputs the maximum capacity at the RAID level specified in RAID Level.

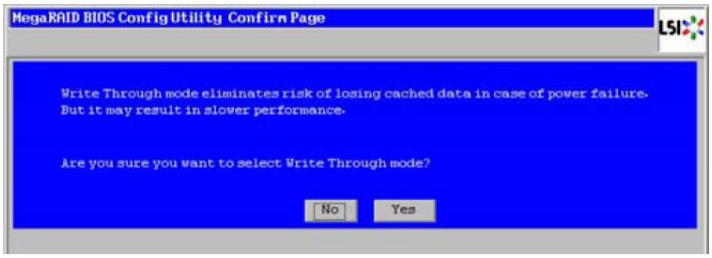


- When you configure a disk array to install an OS and put a value larger than 2 TB, the OS can recognize up to 2 TB.
- If you specify a larger disk array size than the maximum capacity, “Unacceptable size” appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

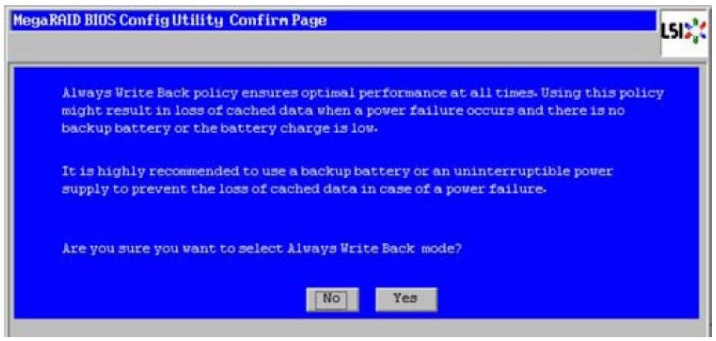
11 Click **Accept**.

One of the following screens appears.

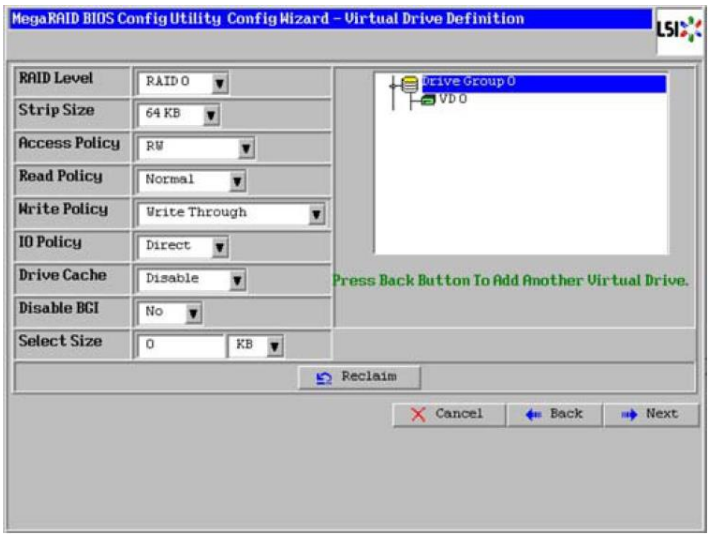
- When selecting **Write Through** in the write policy setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the write policy setting, the following screen appears. Click **Yes**.

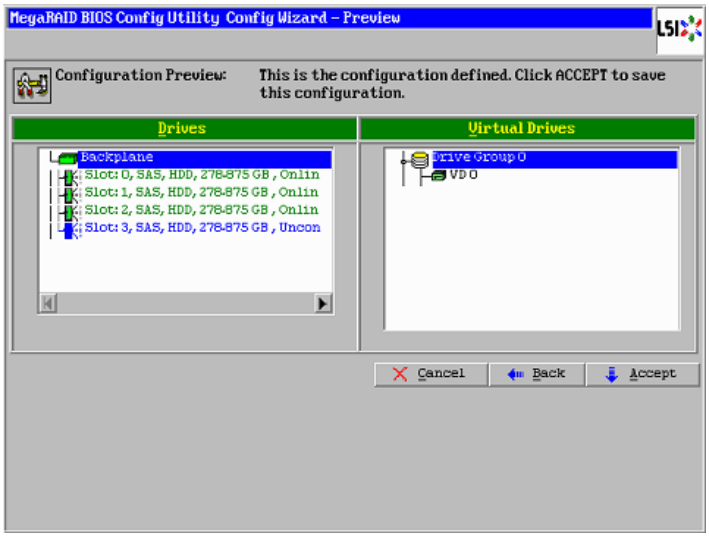


The following screen appears.



12 Click **Next**.

The following screen appears:



13 Click **Accept**.

The following screen appears:



14 Click **Yes**.

The following screen appears:



15 Click **No**.

The screen returns to the main menu.

16 Initialize the disk array that you have built referring to Initializing disk arrays.

Building disk arrays for RAID 10

The following procedure describes building disk arrays for RAID 10.

The following table summarizes the number of hard disks required for building RAID 10.

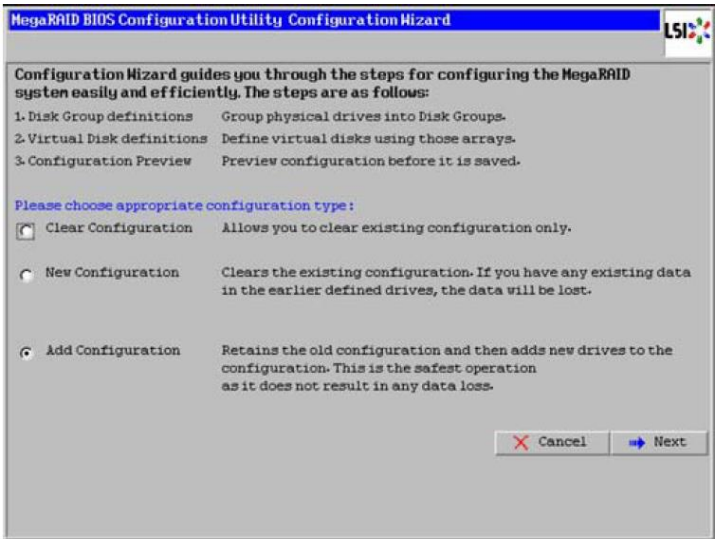
RAID level	Number of hard disks required
RAID 10	4

Tip

See Setting hotspares for information about how to set hotspare.

1 Select **Configuration Wizard** from the main menu.

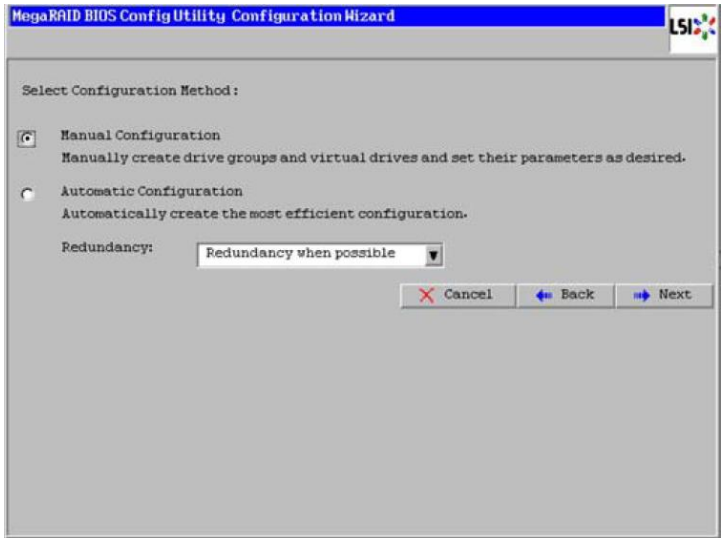
The following screen appears:



NOTICE

If you select **New Configuration**, all data in those hard disks including the disk array information will be lost. Backup your required data before selecting New Configuration.

2 Check **New Configuration** or **Add Configuration** and click **Next**.
The following screen appears:



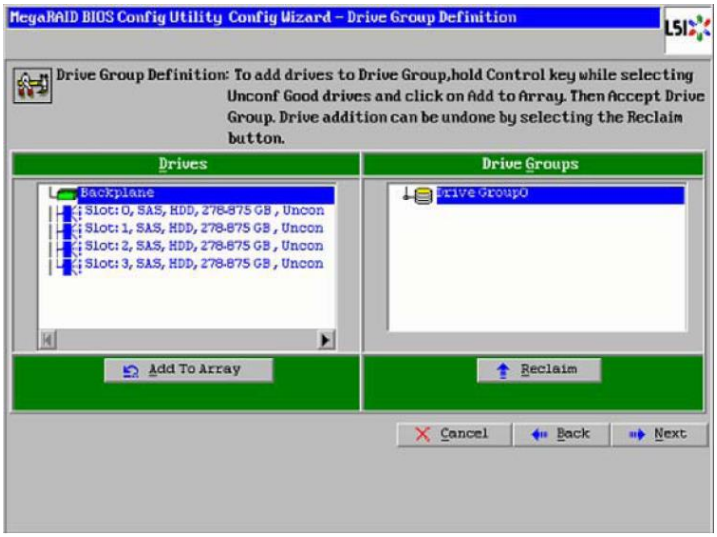
Tip

- The existing disk arrays will remain when you select **Add Configuration**. **Add Configuration** should be selected when you want to keep the existing disk arrays and to build disk arrays through an additional hard disk.
- If you select **New Configuration**, you lose the existing disk arrays. This should be selected when you discard the existing disk array and build a new one.
- If you select **New Configuration**, the following screen appears first. Clicking **Yes** here allows you to build a disk array.

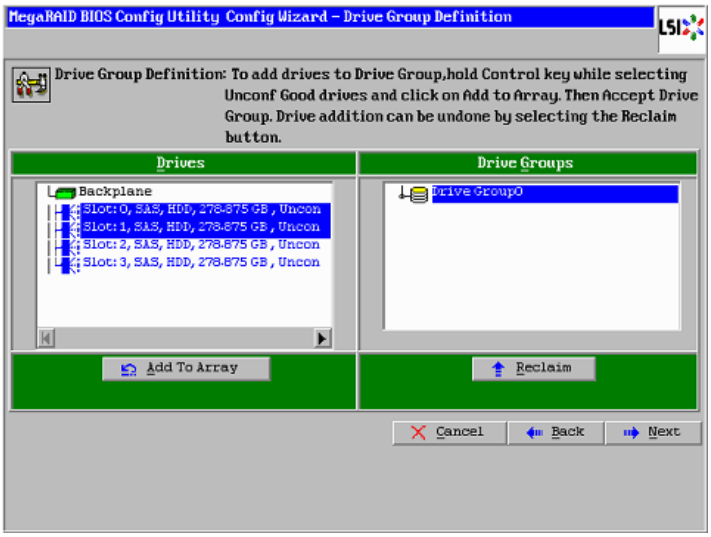


3 Check **Manual Configuration**, and click **Next**.

The following screen appears:



4 Select two hard disks to be used for building a disk array.

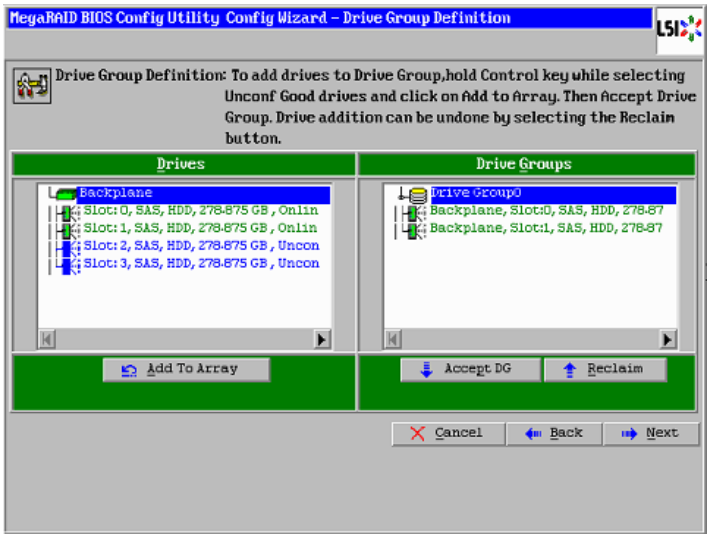


Tip

You can select only a hard disk whose status is **Unconfigured Good** (unused).

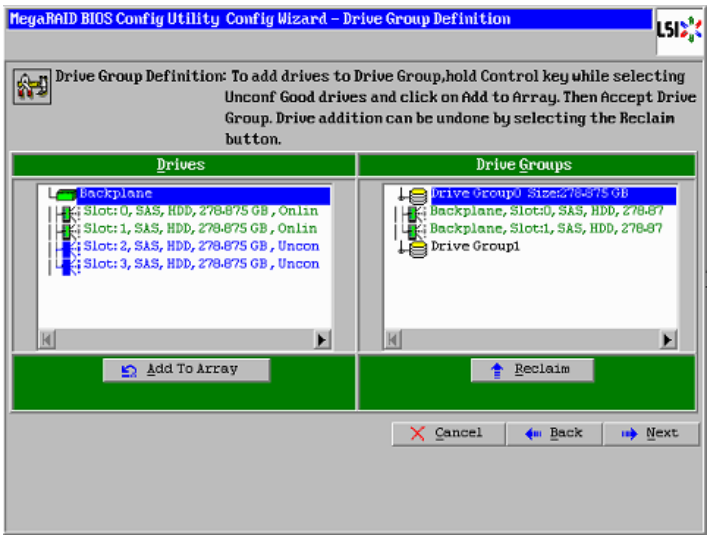
To select multiple hard disks, click them while pressing the **Ctrl** key.

5 After selecting two hard disks for building a disk array, click **Add to Array**.
Status of those selected hard disks is **Online** as shown in the **Drives** pane.



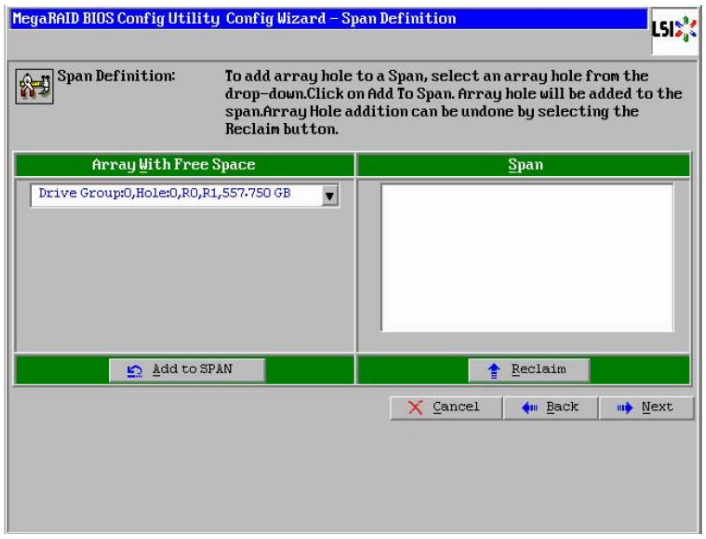
Tip To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

6 Click **Accept DG**.
The following screen appears:



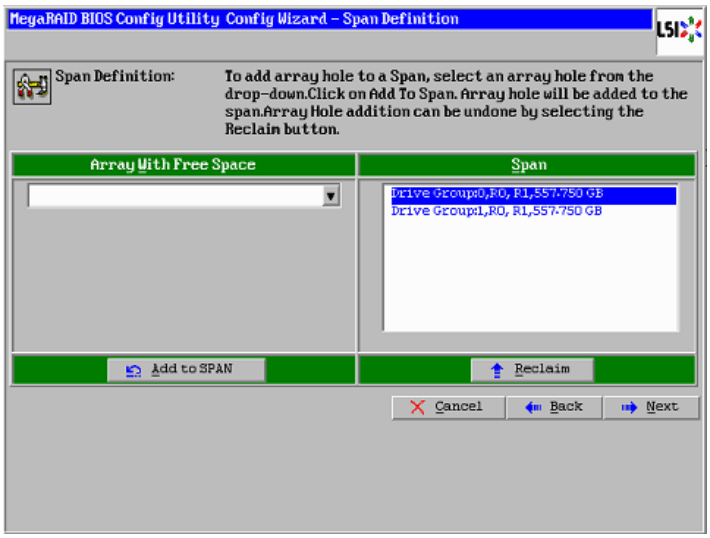
7 Repeat steps 4, 5, and 6 until selecting all hard disks used for RAID 10, and then click **Next**.

The following screen appears:



8 Click **Add to SPAN** the same number of times as repeated in steps 4, 5, and 6 in step 7.

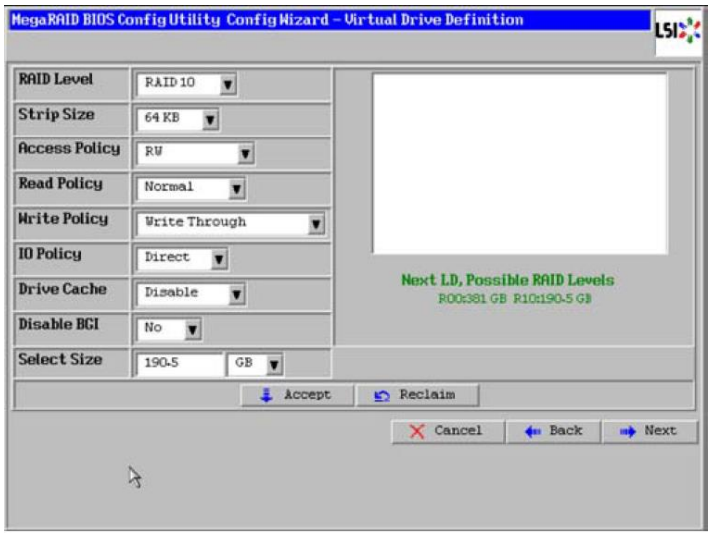
Click it until the pane under **Array With Free Space** becomes blank.



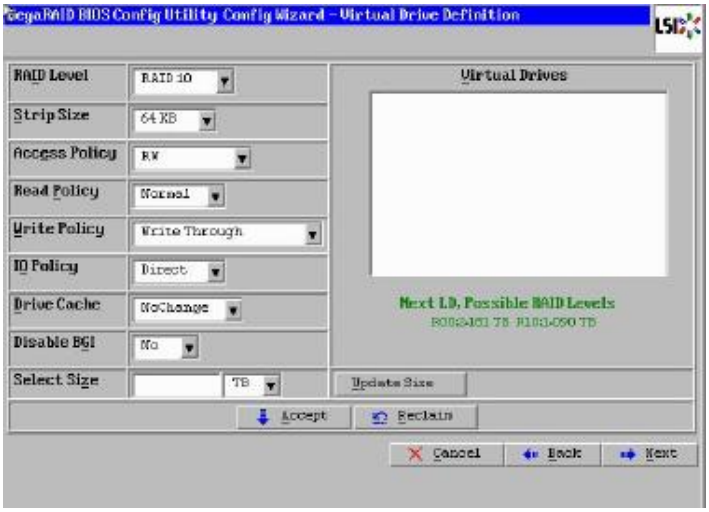
9 Click **Next**.

The following screen appears:

Firmware version; 2.110.63-1184



Firmware version; 2.120.233-1474 or later



10 With all the RAID disk array configurations selected, specify RAID level, stripe size, read policy, write policy, and disk array size.

> ***NOTICE***
>
> When enabling the write cache of the disk array, connect the system equipment to a UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Set each item to the following values.

Item	Content	Setting value **
RAID Level	RAID Level	[RAID 10]
Stripe Size	Stripe size	8 KB / 16 KB / 32 KB / [64 KB] / 128 KB / 256 KG / 512 KB / 1 MB
Access Policy	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advanced reading)] / Ahead (always advanced reading) / Adaptive (advanced reading only in the event of sequential access)
Write Policy *1	Write policy	[Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.)
IO Policy	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)
Drive Cache	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)
Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *2	Size of a disk array	Entering the maximum capacity value.

*1 In Write Policy, **Always Write Back** can be set only when the system equipment is already connected to the UPS (uninterruptible power supply). Even in this case, set **Write Through** when the operating system is installed. Otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays. Do not use **Write Back with BBU**.

*2 Keep the existing maximum capacity value in **Select Size**.

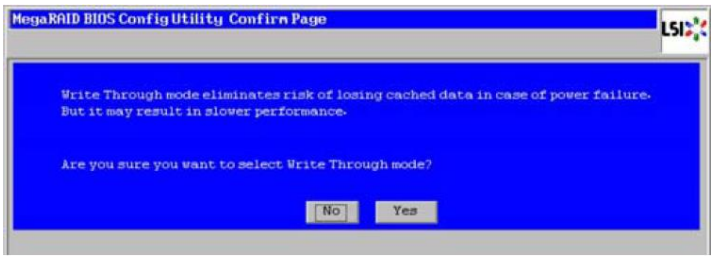
Tip

- When you configure a disk array to install an OS and put a value larger than 2 TB, the OS can only recognize up to 2 TB.
- If you specify a larger disk array size than the maximum capacity, **Unacceptable size** appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

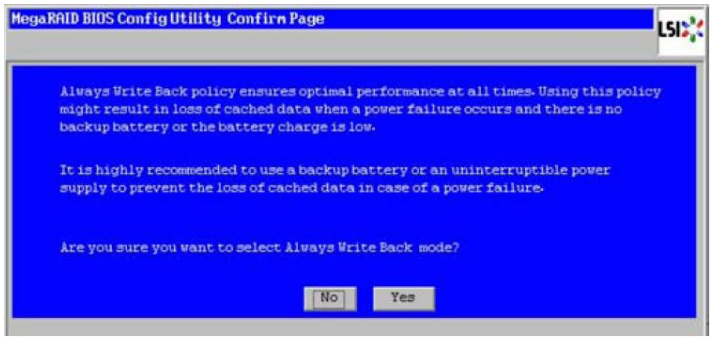
11 Click **Accept**.

One of the following screens appears.

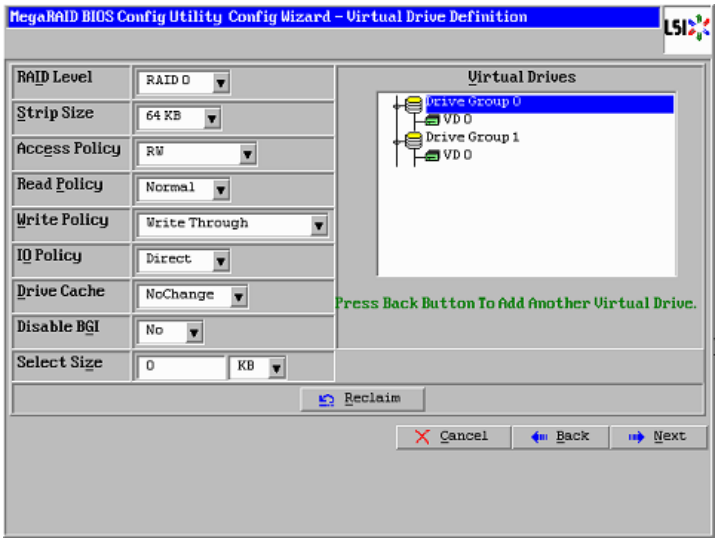
- When selecting **Write Through** in the write policy setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the write policy setting, the following screen appears. Click **Yes**.

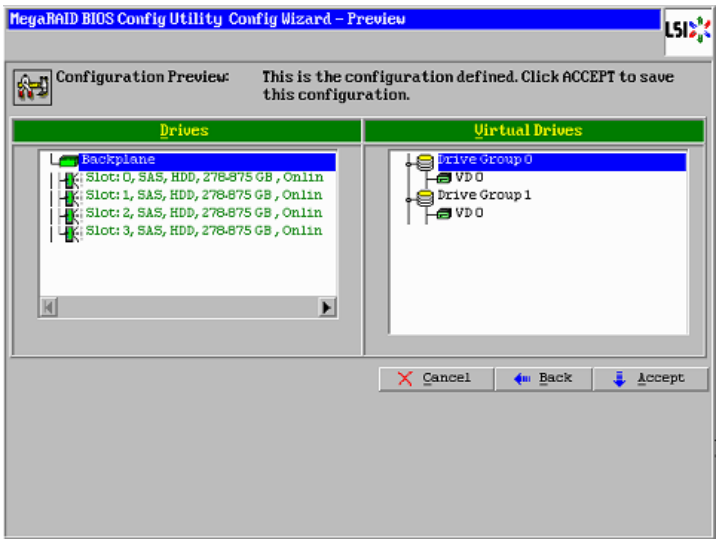


The following screen appears.



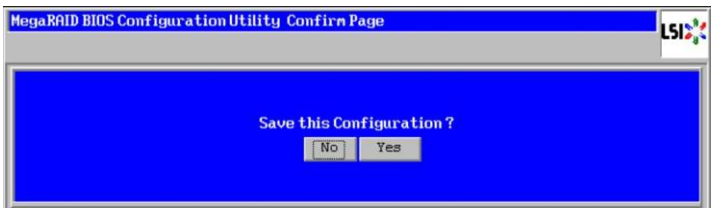
12 Click **Next**.

The following screen appears:



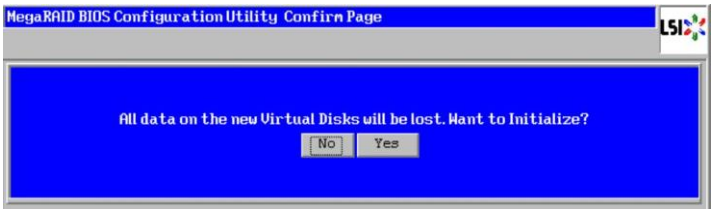
13 Click **Accept**.

The following screen appears:



14 Click **Yes**.

The following screen appears:



15 Click **No**.

The screen returns to the main menu.

16 Initialize the disk array that you have built referring to “Initializing disk arrays”.

Initializing disk arrays

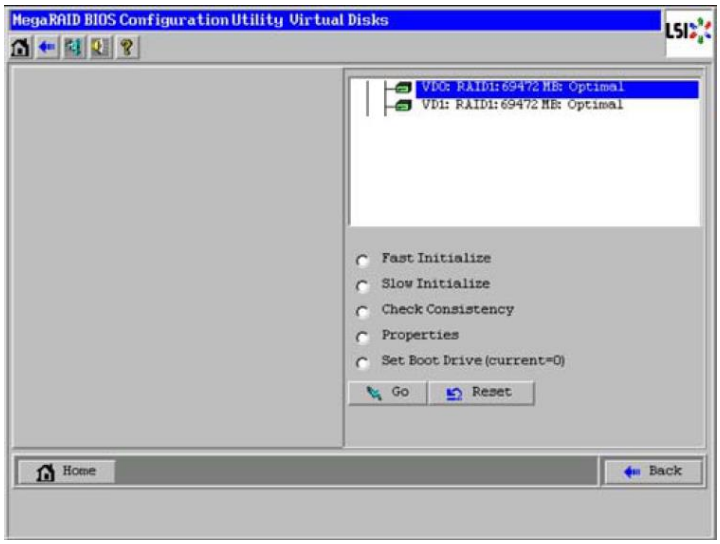
This section describes the procedure for initializing disk arrays

NOTICE

When a disk array is initialized, all data in those hard disks including the disk array information will be lost. Backup your required data before initializing a disk array.

1 Select **Virtual Drives** from the main menu.

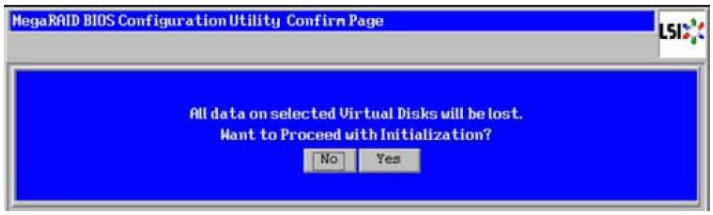
The following screen appears:



2 From the list of disk arrays displayed in the frame at the upper right, select a disk array configuration to initialize.

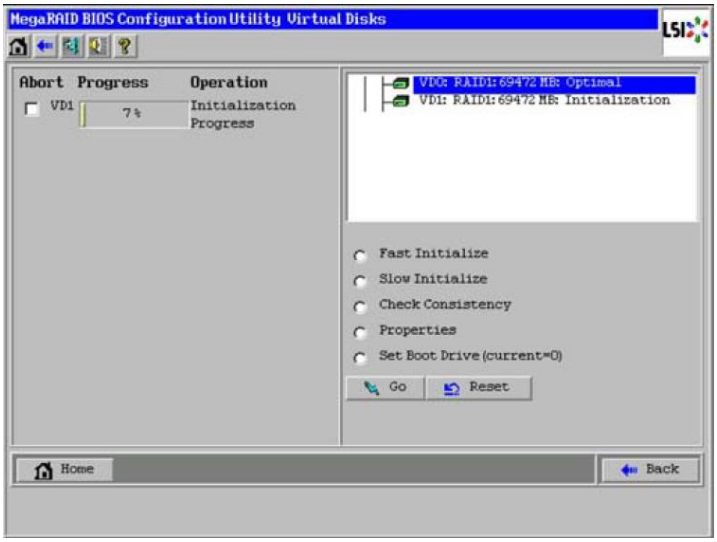
3 Check **Slow Initialize** and click **Go**.

The following screen appears:



4 Click **Yes**.

The progress of initialization is displayed.



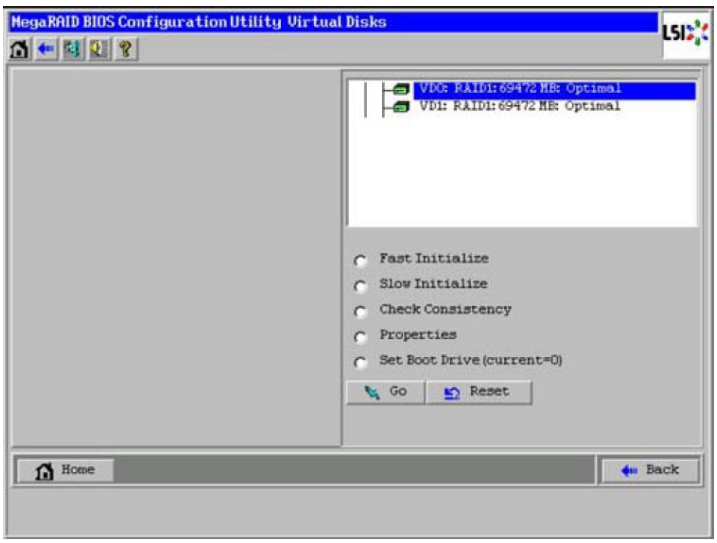
5 Wait until the process is completed 100%.

A guideline for initialization time is shown in the table below.

Single hard disk capacity	Initialization time
147 GB (SAS type)	Approximately 50 minutes
300 GB (SAS type)	Approximately 100 minutes

Tip The initialization time varies depending on the single hard disk capacity regardless of the RAID level or disk array capacity.

6 When initialization is completed 100%, click **Home** to return to the main menu.



Deleting disk arrays

This section describes the procedure for deleting disk arrays.

> ***NOTICE***
>
> When a disk array is deleted, all data in those hard disks including the disk array information will be lost. Backup your required data before deleting a disk array.

Deleting all disk arrays simultaneously

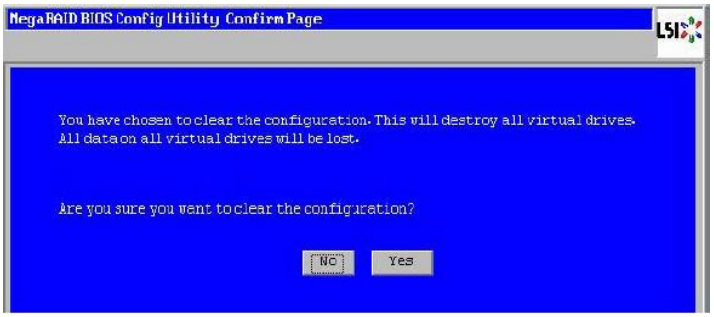
1 Select **Configuration Wizard** from the main menu.

The following screen appears:



2 Check **Clear Configuration** and click **Next**.

The following screen appears:

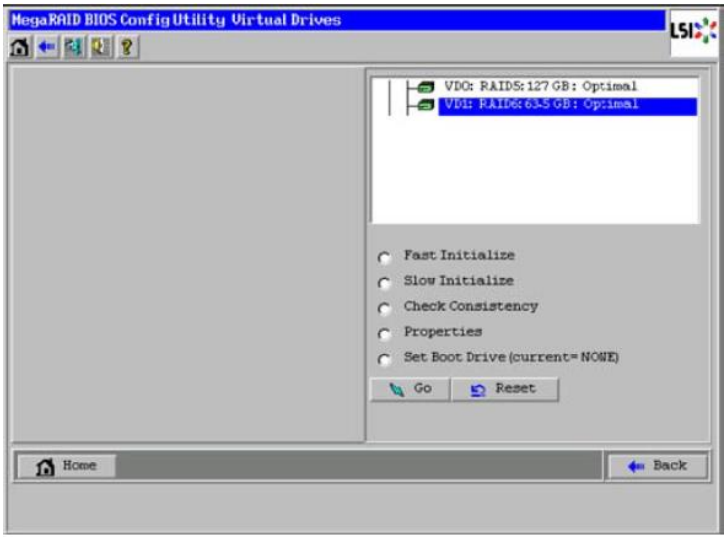


3 Click **Yes**.

Deleting disk arrays selectively

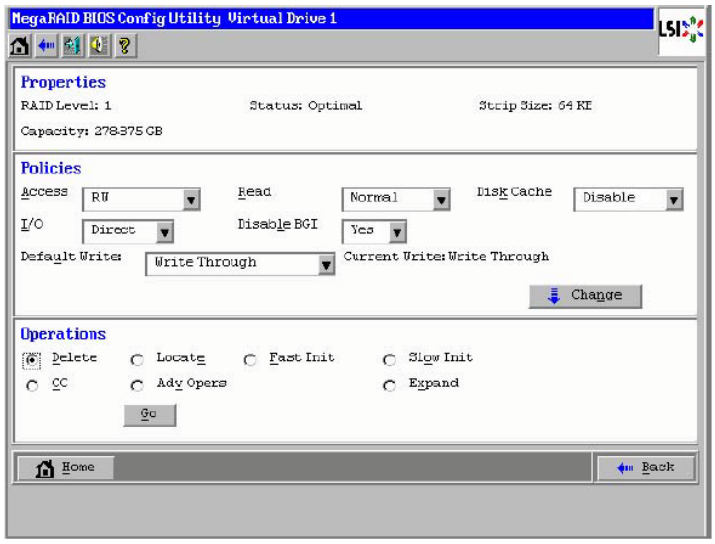
1 Select **Virtual Drives** from the main menu.

The following screen appears:



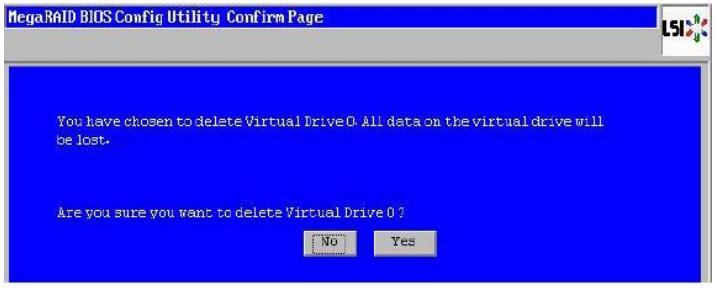
2 From the list displayed at the upper right of the screen, select a disk array that you want to delete. Check **Properties** and click **Go**.

The following screen appears:



3 Check **Delete** and click **Go**.

The following screen appears:



4 Click **Yes**.

Checking disk arrays for consistency

This section describes how to check the consistency of disk arrays.

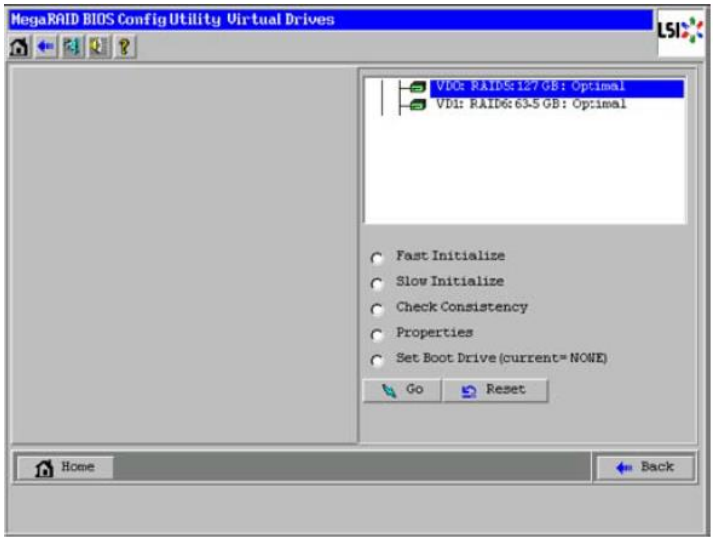
Consistency check can be done from MegaRAID Storage Manager. See the *MegaRAID Storage Manager* in the DriverKit CD-ROM for information about how to check consistency from the MegaRAID Storage Manager.

Tip

Consistency check on disk arrays can be executed only for RAID 1, 5, 6, and 10.

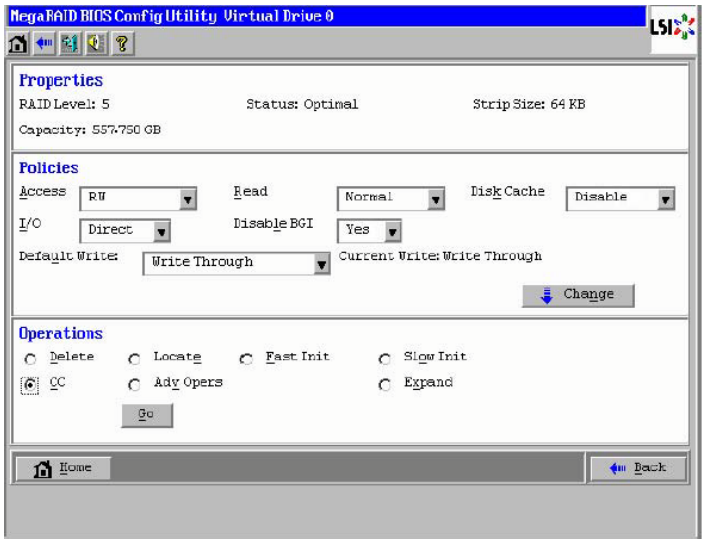
1 Select **Virtual Drives** from the main menu.

The following screen appears:



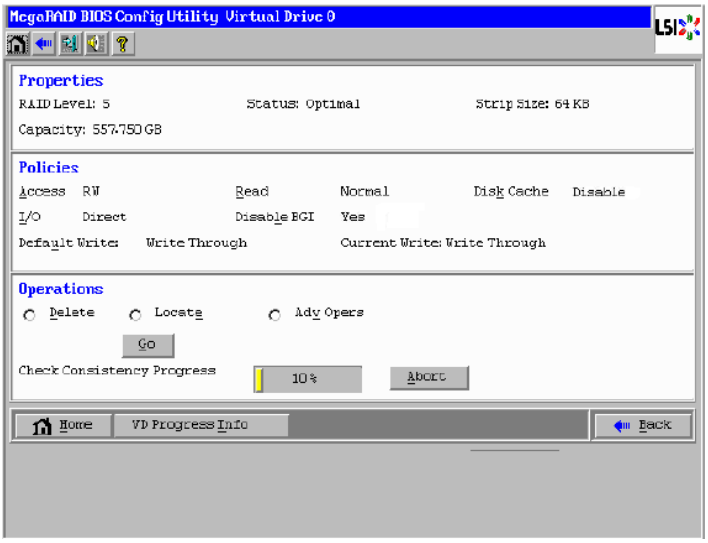
2 From the list displayed at the upper right of the screen, select a disk array that you want to check the consistency. Then check **Properties** and click **Go**.

The following screen appears:



3 Check **CC** and click **Go**.

The progress of consistency check is displayed.



4 Wait until the processing is completed 100%.

5 When the consistency check is completed 100%, click **Home** to return to the main menu.

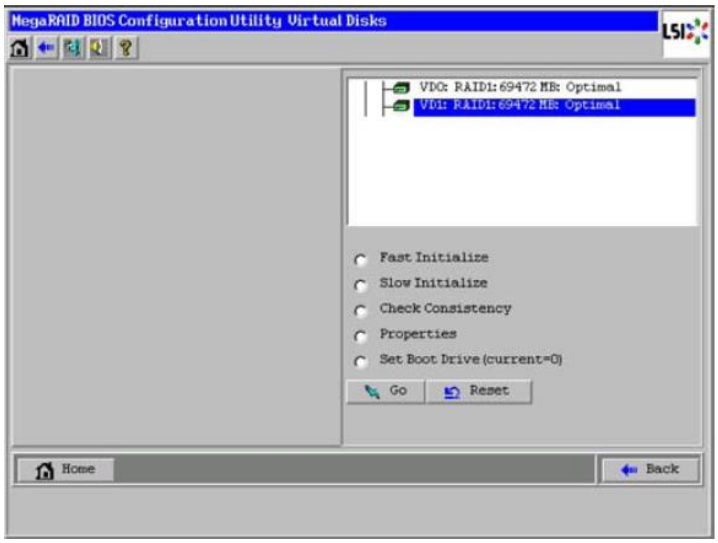
Changing the order of booting disk arrays

This section describes the procedure for changing the booting order in an environment in which multiple disk arrays are set.

Normally, the highest order of booting is assigned to the disk array that was first set. You can assign a disk array that has been built later, however, to the highest in the boot order.

1 Select **Virtual Drives** from the main menu.

The following screen appears:



Tip **Set Boot Drive** is followed by the number of the current disk array being booted.

2 From the list displayed at the upper right of the screen, select a disk array for which you want to set a boot device. Next, check **Set Boot Drive** and click **Go**.

Setting hotspares

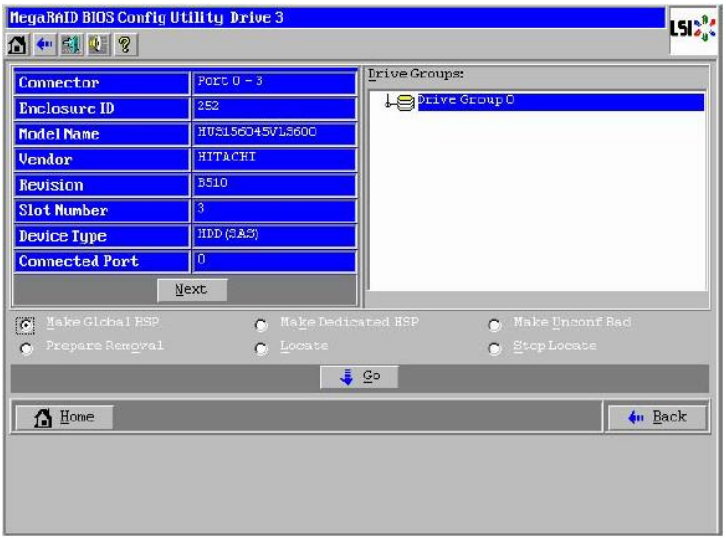
This section describes the procedure for setting hot spares (reserve disks).

Note

Be sure to configure redundant disk arrays, RAID 1, 5, 6, or 10 before setting hotspares.

1 With the main menu displayed, click a hard disk for hotspare from the hard disk list in the **Logical View / Physical View** pane.

The following screen appears:



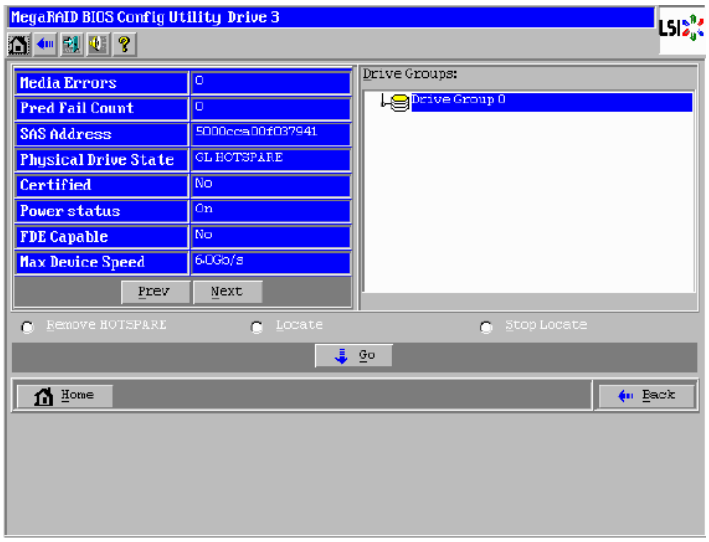
Tip

Only a hard disk whose status is **Unconfigured Good** (unused) can be selected.

2 Check **Make Global HSP**.

3 Click **Go**.

Hotspare is set to the specified hard disk.



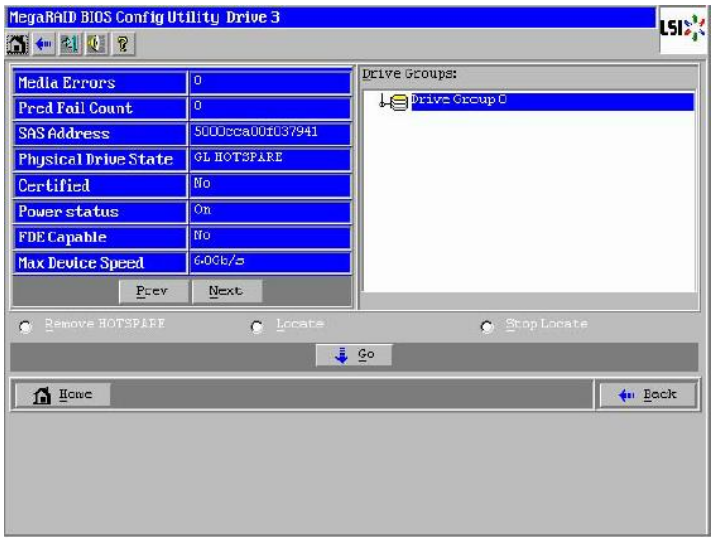
Canceling hotspares

This section describes the procedure for canceling hotspares.

1 When the main menu is displayed, click a hard disk that is set in hotspare from the list in **Logical View/Physical View**.

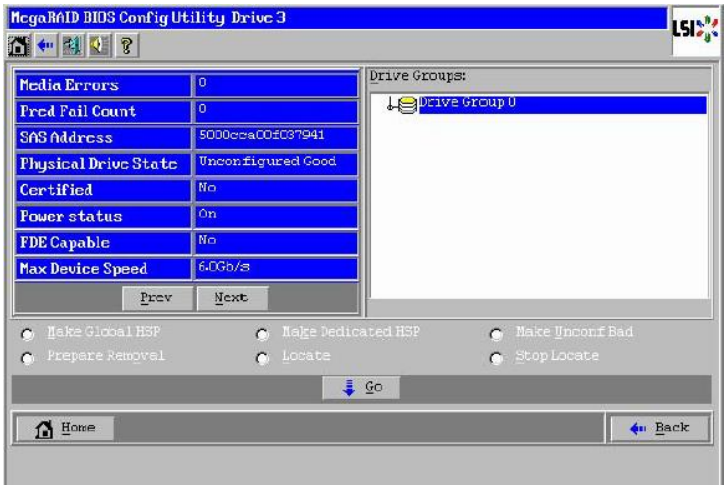
Select a hard disk with hotspare status.

The following screen appears:



2 Check **Remove HOTSPARE**, and click **Go**.

Hotspare is released.



Rebuilding disk arrays

This section describes rebuilding disk arrays when problems occurred on one hard disk in a redundant disk array configuration (RAID 1, 5, 6, 10).

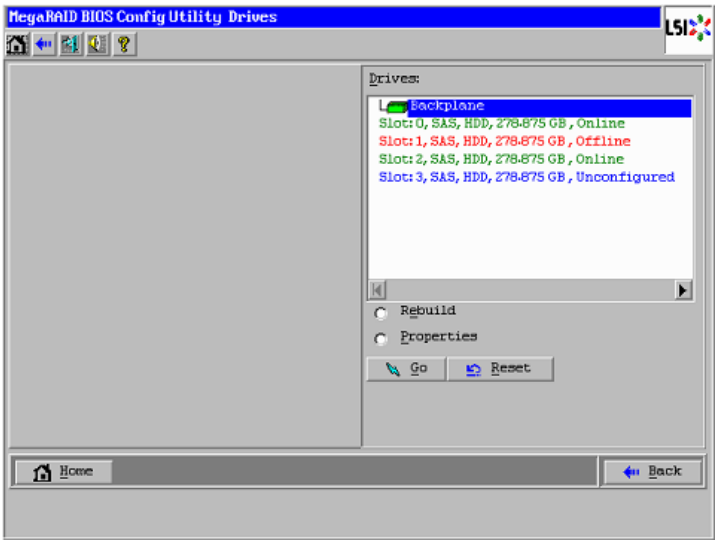


- For RAID 6, the disk array can be restored even if two hard disks fail.
- With hotspares configuration, rebuilding will work automatically when a hard disk problem occurs. Without hotspare configuration, rebuilding will work automatically after you replace the faulty hard disk in hot-plug.

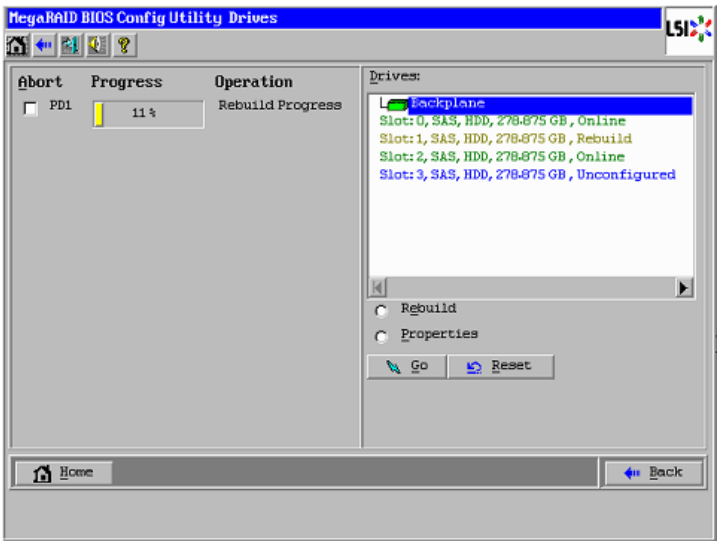
The following procedure describes manually rebuilding disk arrays when rebuilding did not work automatically.

1 Select **Drives** from the main menu.

The following screen appears:



2 Select a hard disk with the **Offline** status, check **Rebuild**, and click **Go**.
The progress of rebuilding is displayed.



3 Wait until the process is completed 100%.
A guideline for rebuilding time is shown in the table below.

RAID level	Capacity of a disk array	Rebuilding time
RAID 1	147 GB (SAS: 147 GB HDD x 2)	Approximately 50 minutes
	300 GB (SAS: 300 GB HDD x 2)	Approximately 100 minutes
RAID 5	294 GB (SAS: 147 GB HDD x 3)	Approximately 50 minutes
	600 GB (SAS: 300 GB HDD x 3)	Approximately 100 minutes
RAID 6	294 GB (SAS: 147 GB HDD x 4)	Approximately 80 minutes
	600 GB (SAS: 300 GB HDD x 4)	Approximately 160 minutes
RAID 10	294 GB (SAS: 147 GB HDD x 4)	Approximately 50 minutes
	600 GB (SAS: 300 GB HDD x 4)	Approximately 100 minutes

Tip The rebuilding time is proportional to the capacity of a disk array.

4 When rebuilding is completed 100%, click **Home** to return to the main menu.

Expanding disk array capacity

This section describes how to expand a disk array in the RAID 0, 5, or 6 disk array by adding hard disks to use.

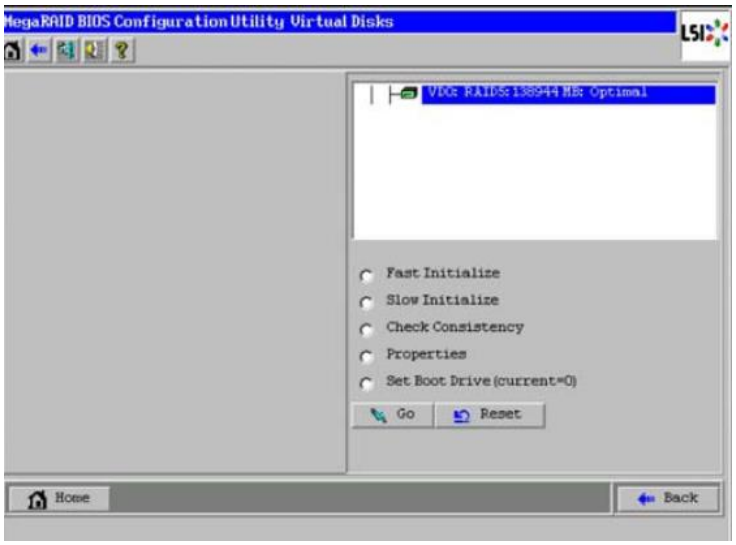
Disk array expansion can also be done from MegaRAID Storage Manager. See the *MegaRAID Storage Manager* in the DriverKit CD-ROM for how to expand disk arrays from the MegaRAID Storage Manager.



- A disk array expansion cannot be cancelled during the execution.
- Be sure to install a hard disk with **Unconfigured Good** status (unused) before expanding the capacity.

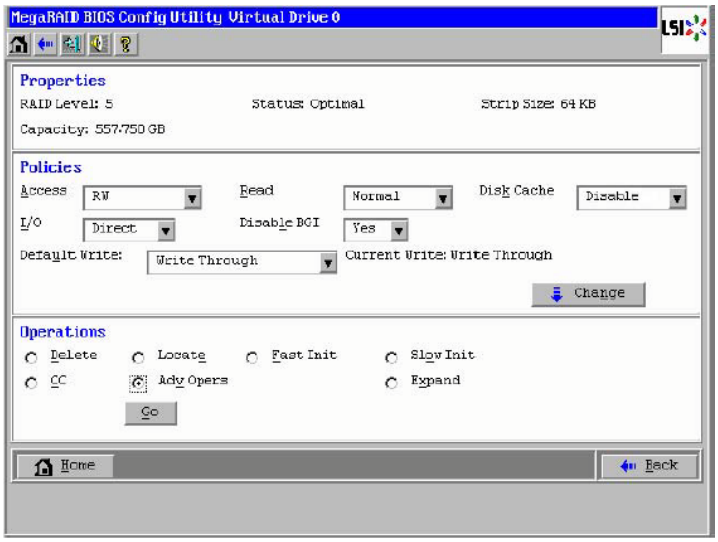
1 Select **Virtual Drives** in the main menu.

The following screen appears:



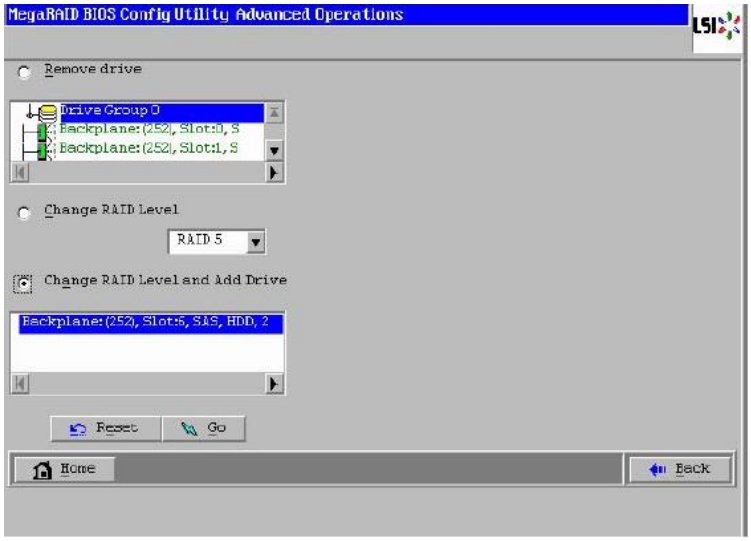
2 Select a disk array to expand the capacity from the list displayed on the upper right of the screen, check **Properties**, and click **Go**.

The following screen appears:



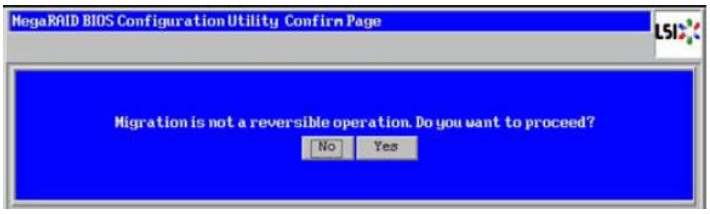
3 Check **Adv Opers** and click **Go**.

The following screen appears:



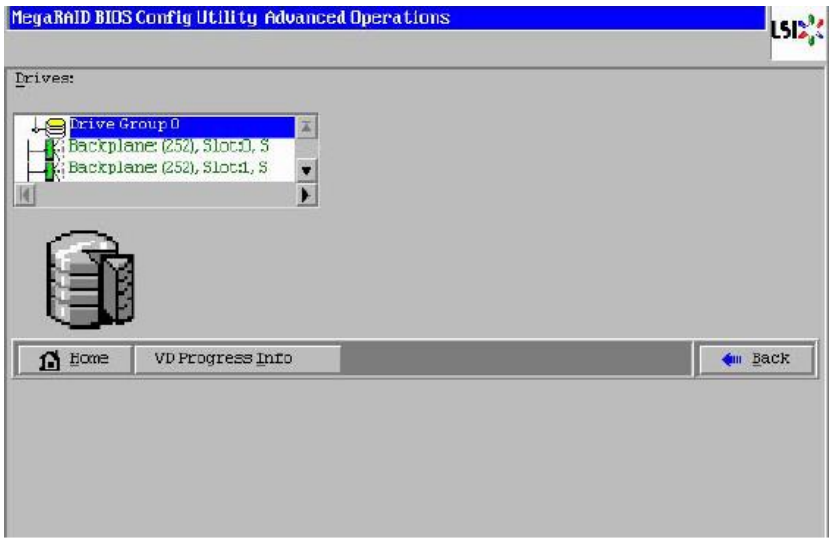
4 Check **Change RAID Level and Add Drive**, select a hard disk to use for the capacity expansion from the list displayed in the pane, and click **Go**.

Tip To select multiple hard disks, click hard disks while pressing the **Ctrl** key.



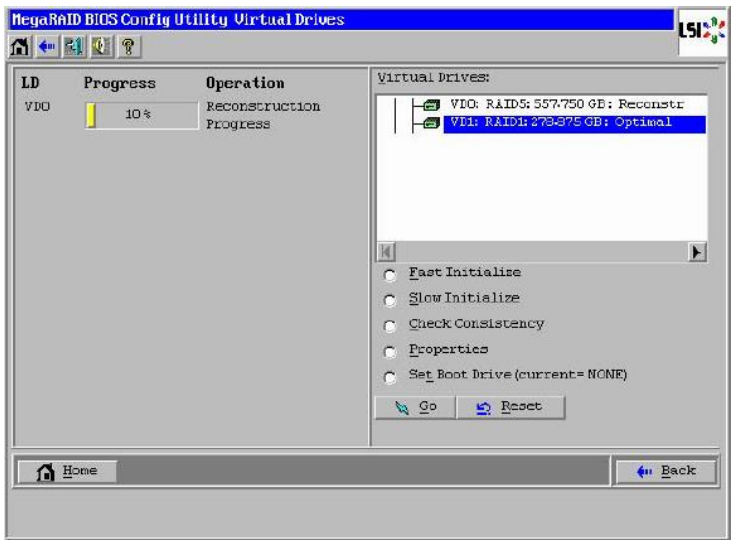
5 Click **Yes**.

The following screen appears:



6 Click **VD Progress Info** shown in the previous screen.

The progress of the capacity expansion is displayed.



7 Wait until the expansion is completed 100%.

A guideline for expanding time is shown in the table below.

RAID level	Capacity of a disk array	Rebuilding time for expansion
RAID 0	Expands “441 GB (SAS: 147 GB HDD x 3)”	Approximately 300 minutes
	Expands “900 GB (SAS: 300 GB HDD x 3)”	Approximately 600 minutes
RAID 5	Expands “294 GB (SAS: 147 GB HDD x 3)”	Approximately 240 minutes
	Expands “600 GB (SAS: 300 GB HDD x 3)”	Approximately 480 minutes
RAID 6	Expands “294 GB (SAS: 147 GB HDD x 4)”	Approximately 240 minutes
	Expands “600 GB (SAS: 300 GB HDD x 4)"	Approximately 480 minutes



The rebuilding time for expansion is proportional to the capacity of a disk array regardless of the number of hard disks to add.

8 When expansion is completed 100%, click **Home** to return to the main menu.

❑ Changing the write policy for disk arrays

This section describes the procedure for changing the write policies.

Enabling Write Cache of a disk array can improve the write performance.

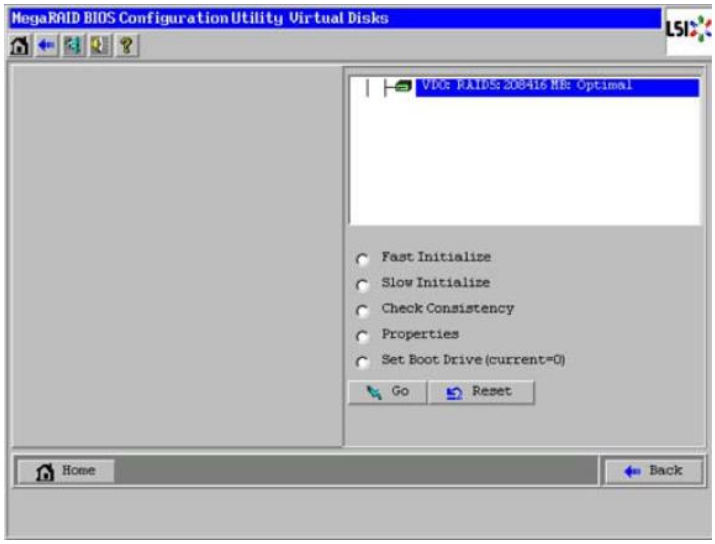
> ***NOTICE***
>
> When enabling the disk array “write cache”, connect the system equipment to a UPS. Otherwise, data in the write cache may disappear or be destroyed durig a blackout or instant power failure.

In Write Policy, “Always Write Back” can be supported only when the system equipment is connected to the UPS (uninterruptible power supply).

Even in this case, set to **Write Through** when installing the operating system. Otherwise, installation may not be properly completed.

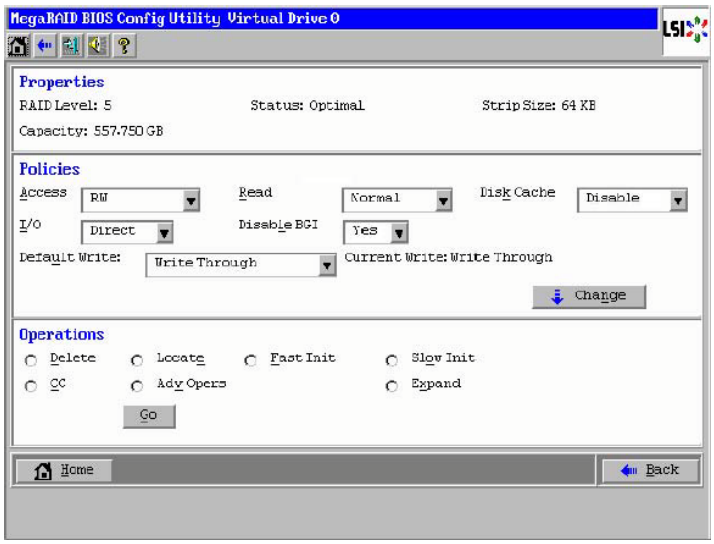
1 Select **Virtual Drives** in the main menu.

The following screen appears:



2 From the list displayed at the upper right of the screen, select a disk array for which you want to change the write policy. Check **Properties** and click **Go**.

The following screen appears:



3 Select the write policy from **Default Write** in the **Policies** pane, and click **Change**.

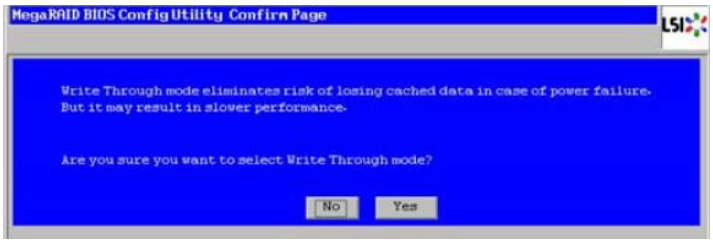
Setting value	Description
Always Write Back	Write cache is valid.
Write Through	Write cache is invalid.
Write Back with BBU	Write cache is valid only when the battery is installed.

Note

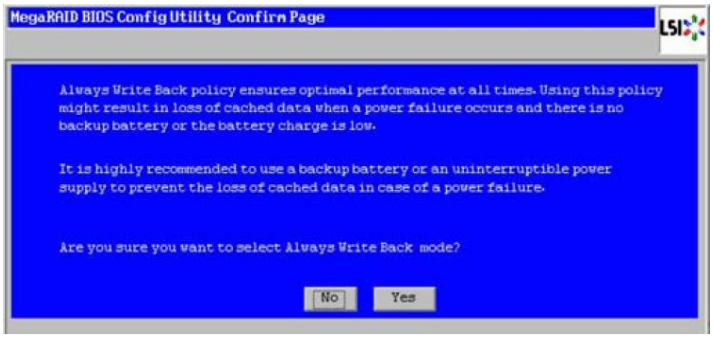
In Write Policy, operation with **Always Write Back** can be supported only when the system equipment is connected to the UPS (uninterruptible power supply). Even in this case, set **Write Through** when installing OS. Otherwise, installation may not be properly completed.

Do not select **Write Back with BBU**.

- When selecting **Write Through** in the Default write setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the Default write setting, the following screen appears. Click **Yes**.



4 Click **Home** to return to the main menu.

Tip

Set the write policy per disk array. When building multiple disk arrays, set the write policy to all disk arrays.

❑ BIOS settings for SAS internal RAID board

When using the boot from an external storage on the system equipment with the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y, change the BIOS setting: Controller BIOS setting to Disabled.

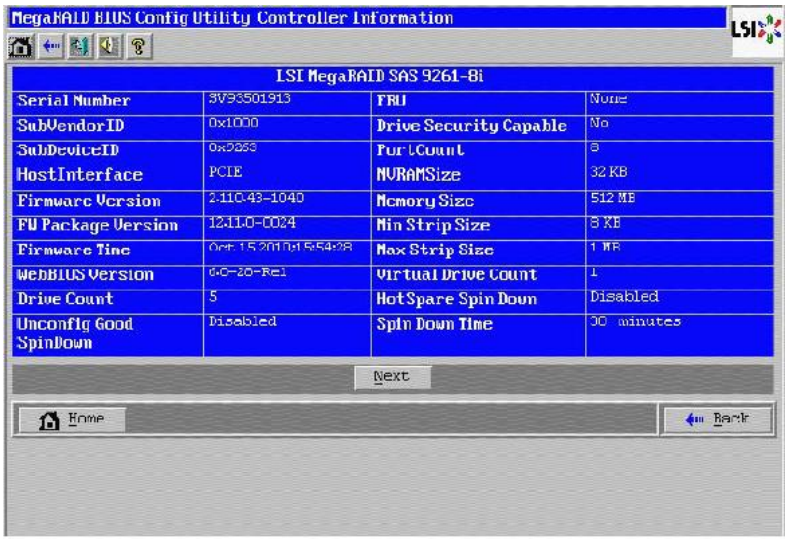
This section describes the procedure for changing the BIOS setting of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y.



When the BIOS setting: Controller BIOS setting is changed to Disabled, you cannot execute the boot from the disk array configured in the SAS internal RAID Board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y.

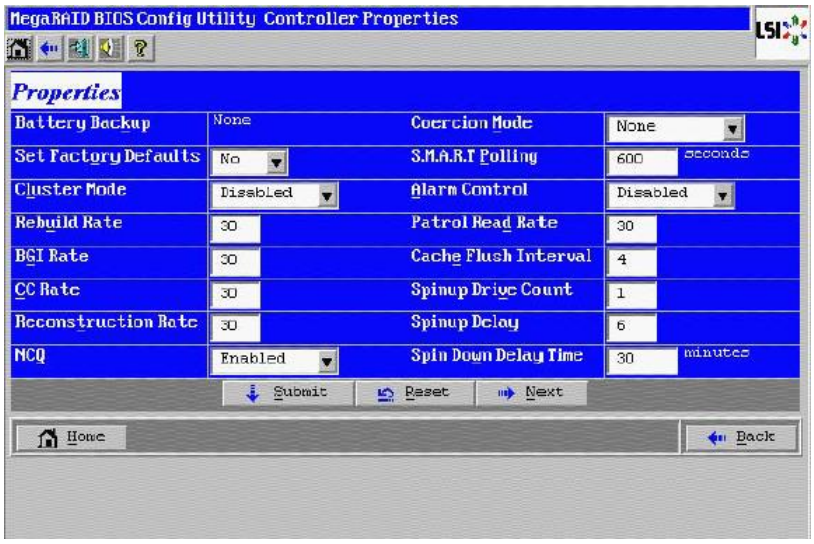
1 Select **Controller Properties** from the main menu.

The following screen appears:



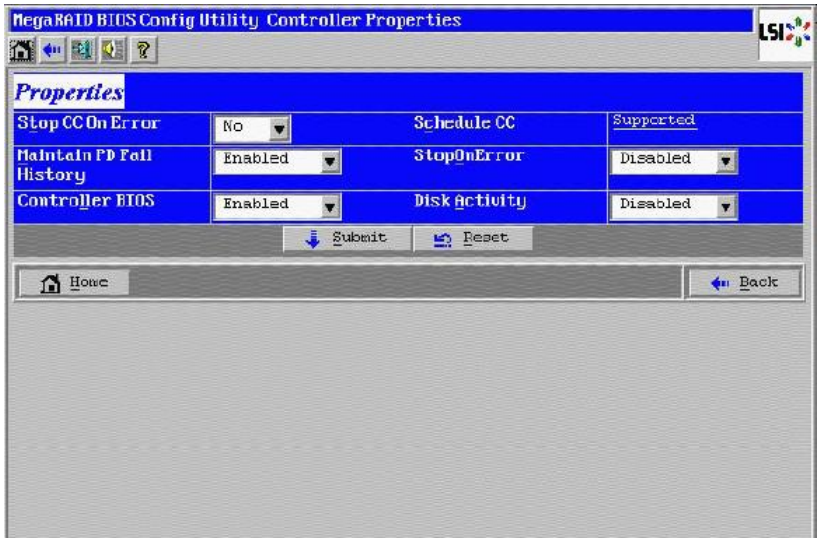
2 Click **Next**.

The following screen appears:



3 Click **Next** once more.

The following screen appears:



4 Select one of the setting values in the following table from **Controller BIOS**, and click **Submit**.

Setting value	Description
Enabled	Enables BIOS of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y. Enables the boot from the disk array.
Disabled	Disables BIOS of the SAS internal RAID board: GVX-CA2SRD2X1/GV-CA2SRD2X1-Y. Disables the boot from the disk array.

Tip Make sure to click **Submit** after changing the setting.

5 Confirm that **Controller BIOS** is set to that value.

6 Click **Home** to return to the main menu.

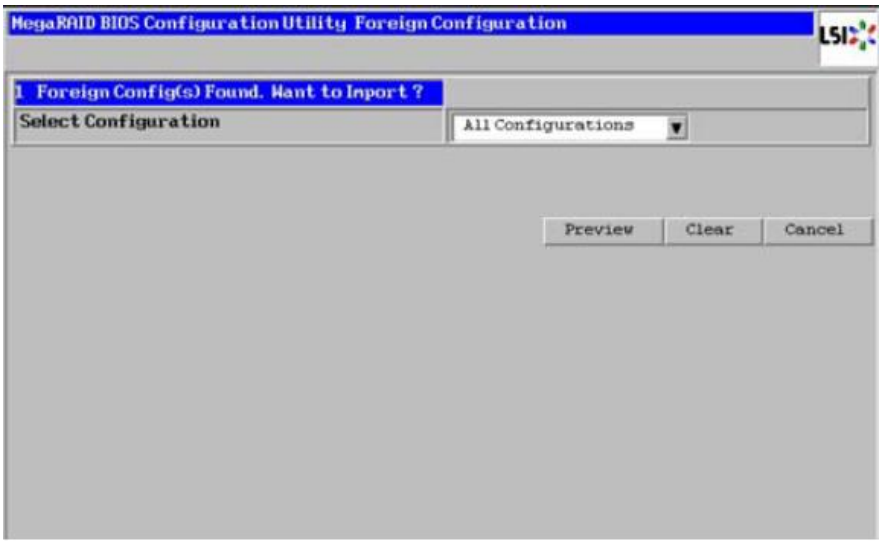
❑ Disk with foreign configuration

This section describes how to deal with a hard disk with a different configuration detected from the disk array controller board configuration.

The difference in configuration between disks may be caused by the following conditions.

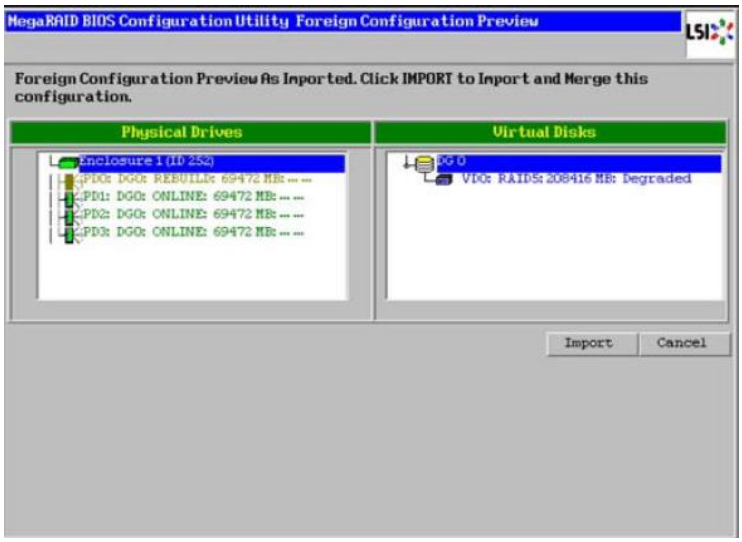
Conditions to generate foreign configuration
A disk failed and could not be recognized. Then the disk has been restored to be recognized.

1 Click **Preview**.



2 If the displayed configuration is correct, click **Import**.

If the displayed configuration is incorrect, click **Cancel**. When the screen returns to Step 1, click **Clear**.



Tip When you click **Clear**, the message “Previous foreign configuration will be lost” appears. Do you want to proceed?” is displayed. Click **Yes**, and the previous foreign configuration will be eliminated.

❑ Status

Status of the Disk Array

The following table lists the status for disk arrays.

Status indication	Description
Optimal	Normal. The disk array is perfect in function.
Partially Degraded	One hard disk fails in the RAID 6 disk array.
Degraded	One hard disk fails in the RAID 1, 5, or 10 disk array. Or two hard disks fail in the RAID 6 disk array.
Offline	The disk array is inoperable because of either failures in multiple hard disks in a redundant disk array or a failure in a hard disk in a non-redundant disk array.

Status of the hard disk

The following table lists the status for hard disks.

Status indication	Description
Online	Normal.
Offline/Failed	A fault has occurred. The hard disk is separated from the disk array due to failure.
Rebuild	Rebuilding is underway.
GL Hot Spare	This is set as a global hotspare.
DED Hot Spare	This is a dedicated hot spare.
Unconfigured GOOD	This is not used for a disk array.
Unconfigured BAD	A fault has occurred. The unrecognizable hard disk is restored to recognizable.
Missing	A fault has occurred. A "normal" hard disk has been removed.

❑ BIOS messages

The following table lists the messages for MegaRAID WebBIOS displayed during system startup.

Message	Description
Cache data was lost due to an unexpected power-off or reboot during a write operation, but the adapter has recovered. This could be due to memory problems, bad battery, or you may not have a battery installed.	If these messages are displayed even though an incorrect power-off or reboot has not been executed during write operation, contact your reseller or call maintenance personnel.
Memory/battery problems were detected. The adapter has recovered, but cached data was lost.	
Cache data was lost due to an unexpected power-off or reboot during a write operation, but the adapter has recovered. This could be due to memory problems, bad battery, or you may not have a battery installed.	
Cache data was lost, but the controller has recovered. This could be due to the fact that your controller had protected cache after an unexpected power loss and your system was without power longer than the battery backup time.	
The cache contains dirty data, but some VDs are missing or will go offline, so the cached data cannot be written to disk. If this is an unexpected error, then please power off your system and check your cables to ensure all disks are present. If you continue, the data in cache will be permanently discarded. Press 'X' to acknowledge and permanently destroy the cached data.,	
Foreign configuration(s) found on adapter. Press any key to continue or 'C' load the configuration utility, or 'F' to import foreign configuration(s) and continue.	A hard disk with a different configuration from the disk array configuration in the disk array controller was detected. See “Disk with foreign configuration”.
FW package: xxxx	This shows the firmware package version. You do not need to take any action.
The battery hardware is missing or malfunctioning, or the battery is unplugged. If you continue to boot the system, the battery-backed cache will not function. Please contact technical support for assistance. Press ‘D’ to disable this warning (if your controller does not have a battery).	Battery backup unit information is not set correctly. Press the **D** key while this message is displayed. If this key operation does not recover the situation, contact your reseller or call maintenance personnel.
The battery is currently discharged or disconnected. Verify the connection and allow 30 minutes for charging. If the battery is properly connected and it has not returned to operational state after 30 minutes of charging, contact technical support for additional assistance. Press 'D' to disable this warning (if your controller does not have a battery).	
Some configured disks have been removed from your system, or are no longer accessible. Please check your cables and also ensure all disks are present.	Some hard disks with the disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.

Message	Description
The following VDs have missing disks: X Y.. If you proceed (or load the configuration utility), these VDs will be marked OFFLINE and will be inaccessible. Please check your cables and ensure all disks are present.	Since some hard disks have been removed, the disk array is set in OFF LINE. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
A discovery error has occurred, please power cycle the system and all the enclosures attached to this system.	A disk array controller or hard disk has not been recognized correctly. When this message is displayed, contact your reseller or call maintenance personnel.
The following VDs are missing: X Y … If you proceed (or load the configuration utility), these VDs will be removed from your configuration. If you wish to use them at a later time, they will have to be imported. If you believe these VDs should be present, please power off your system and check your cables to ensure all disks are present.	Some disk array configurations are removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
All of the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your cables to ensure all disks are present.	All hard disks with disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
Press any key to continue, or 'C' to load the configuration utility.	Press the **C** key while this message is displayed, MegaRAID WebBIOS will start.
Press <Ctrl> <H> for WebBIOS.	When this message is displayed, press the **Ctrl** and **H** keys at the same time to start MegaRAID WebBIOS.
Your battery is bad or missing, and you have VDs configured for write-back mode. Because the battery is not usable, these VDs will actually run in write-through mode until the battery is replaced.	Write cache is not enabled because MegaRAID Storage Manager has set the write policy (write cache setting) to Write Back. Do not change the write cache from the MegaRAID Storage Manager any more. Change the write policy setting from MegaRAID WebBIOS referring to “Changing the write policy for disk arrays”.
Multibit ECC errors were detected on the controller. DIMM on the controller needs replacement. If you continue, data corruption can occur. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, please press 'X' to continue.	An error has occurred in the cache memory of the disk array controller. When this message is displayed, contact your reseller or call maintenance personnel.
Single-bit ECC errors were detected during the previous boot of the RAID controller. The DIMM on the controller needs replacement. Please contact technical support to resolve this issue. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, press 'X' to continue.	

Message	Description
Single-bit overflow ECC errors were detected during the previous boot of the RAID controller. The DIMM on the controller needs replacement. Please contact technical support to resolve this issue. If you continue, data corruption can occur. Press 'X' to continue or else power off the system and replace the DIMM module and reboot. If you have replaced the DIMM press 'X' to continue.	
Multibit ECC errors were detected on the RAID controller. If you continue, data corruption can occur. Please contact technical support to resolve this issue. Press 'X' to continue or else power off the system, replace the controller and reboot.	
Single-bit ECC errors were detected on the RAID controller. Please contact technical support to resolve this issue. Press 'X' to continue or else power off the system, replace the controller and reboot.	
Single-bit overflow ECC errors were detected on the RAID controller. If you continue, data corruption can occur. Please contact technical support to resolve this issue. Press 'X' to continue or else power off the system, replace the controller and reboot.	
RAID Adapter Memory Error!!! Please check the SDRAM connection. If problems persist contact Tech Support. Press Any Key to Continue...	An error occurred on the disk array controller memory. When this message is displayed, contact your reseller or call maintenance personnel.
Adapter at Baseport XXXXh is not responding. No MegaRAID Adapter installed.	Baseport XXXXh does not respond. When this message is displayed, contact your reseller or call maintenance personnel.
This is a TEST message. You may hit a key to ignore it, or wait 5 seconds. No further action is required.	When this message is displayed, contact your reseller or call maintenance personnel.
This firmware is an ALPHA version - It has not completed all validations. The validation stamp is: X Y.	When this message is displayed, contact your reseller or call maintenance personnel.
This firmware is BETA version - It has not completed all validations. The validation stamp is: X Y.	When this message is displayed, contact your reseller or call maintenance personnel.
This firmware is a TEST version - It has not completed any validation.	When this message is displayed, contact your reseller or call maintenance personnel.
Firmware version inconsistency was detected. The adapter has recovered, but cached data was lost.	When this message is displayed, contact your reseller or call maintenance personnel.
The most recent configuration command could not be committed and must be retried.	Disk array configuration information was cleared or not found.
Previous configuration cleared or missing Importing configuration created on X/Y X:Y	When this message is displayed, contact your reseller or call maintenance personnel.
An enclosure was found that contains both SAS and SATA drives, but this controller does not allow mixed drive types in a single enclosure. Please correct the problem then restart your system.	The disk array controller is operated by incorrect parameters. When this message is displayed, contact your reseller or call maintenance personnel.

Message	Description
SAS drives were detected, but this controller does not support SAS drives. Please remove the SAS drives then restart your system.	
SATA drives were detected, but this controller does not support SATA drives. Please remove the SATA drives then restart your system.	
There are X enclosures connected to connector Y, but only a maximum of Z enclosures can be connected to a single SAS connector. Please remove the extra enclosures then restart your system.	Incorrect enclosures were found. When this message is displayed, contact your reseller or call maintenance personnel.
Invalid SAS topology detected. Please check your cable configurations repair the problem, and restart your system.	When this message is displayed, contact your reseller or call maintenance personnel.
Invalid SAS Address present in serial boot ROM (SBR). Please contact your system support. Press any key to continue with Default SAS Address	When this message is displayed, contact your reseller or call maintenance personnel.
Invalid SAS Address present in MFC data. Please program valid SAS Address and restart your system.	
Your VDs that are configured for write-back are temporarily running in write-through mode. This is caused by the battery being charged, missing or bad. Please allow the battery to charge for 24 hours before evaluating the battery for replacement. The following VDs are affected: X Press any key to continue.	Set a write policy from MegaRAID WebBIOS referring to Changing the write policy for disk arrays.
Invalid memory configuration detected. Please contact your system support. System has halted.	When this message is displayed, contact your reseller or call maintenance personnel.
Entering the configuration utility in this state will result in drive configuration changes. Press 'Y' to continue loading the configuration utility or please power off your system and check your cables to ensure all disks are present and reboot.	Hard disk configuration information has been changed. When this message is displayed, contact your reseller or call maintenance personnel.
Attached Enclosure does not support in controller's Direct mapping mode. Please contact your system support. System has halted due to unsupported configuration.	Incorrect information was detected from the enclosure. When this message is displayed, contact your reseller or call maintenance personnel.
Expander Detected in controller with Direct mapping mode Reconfiguring automatically to persistent mapping mode. Automatic reboot would happen in 10 seconds.	A device (expander) not supported was detected. When this message is displayed, contact your reseller or call maintenance personnel.
Your controller's IO processor has a fault that can potentially cause data corruption. Your controller needs replacement. Please contact your system support. To continue please press 'Y' to acknowledge.	When this message is displayed, contact your reseller or call maintenance personnel.
Number of disks exceeded the maximum supported count of X disks Please remove the extra drives and reboot system to avoid losing data Press 'Y' to continue with extra drives	Incorrect hard disks were detected. When this message is displayed, contact your reseller or call maintenance personnel.

Message	Description
Number of devices exceeded the maximum limit of devices per quad Please remove the extra drives and reboot system to avoid losing data. System has halted due to unsupported configuration.	
Drive security is enabled on this controller and a pass phrase is required. Please enter the pass phrase.	Hard disk security functions are not supported. When this message is displayed, contact your reseller or call maintenance personnel.
Invalid pass phrase. Please enter the pass phrase.	
There was a drive security key error. All secure drives will be marked as foreign.	
Invalid pass phrase. If you continue, there will be a drive security key error and all secure configurations will be marked as foreign. Reboot the machine to retry the pass phrase or press any key to continue.	
Unable to communicate to electronic key management systems (EKMS). If you continue, there will be a drive security key error and all secure configurations will be marked as foreign. Please check connection with the EKMS, reboot the machine to retry the EKMS, or press any key to continue.	Hard disk security functions are not supported. When this message is displayed, contact your reseller or call maintenance personnel.
Unable to Rekey security to EKMS as not able to communicate to EKMS. If you continue, the drive security will remain in the existing security mode. Please check connection with the EKMS, reboot the machine to retry the EKMS or press any key to continue.	
The native configuration is no longer supported by the current controller settings. Please ensure that correct controller or iButton is being used. If you continue, the configuration will be marked foreign and part of it may be imported if possible. Press any key to continue.	When this message is displayed, contact your reseller or call maintenance personnel.
The battery is currently discharged or disconnected. Verify the connection and allow 30 minutes for charging. If the battery is properly connected and it has not returned to operational state after 30 minutes of charging, then contact technical support for additional assistance.	Battery backup unit information is incorrect. When this message is displayed, contact your reseller or call maintenance personnel.
The battery is currently discharged or disconnected. VDs configured in write-back mode will run in write through mode to protect your data and will return to write-back policy when the battery is operational. If VDs have not returned to write-back mode after 30 minutes of charging, then contact technical support for additional assistance. The following VDs are affected: X2 Press any key to continue.	

Message	Description
Two BBUs are connected to the adapter. This is not a supported configuration. Battery and caching operations are disabled. Remove one BBU and reboot to restore battery and caching operations. If dirty cache is lost in this boot that could have been because of dual battery presence.	
Firmware did not find valid NVDATA image. Please program valid NVDATA image and restart your system. Press any key to continue	When this message is displayed, contact your reseller or call maintenance personnel.
IR to MR Migration failed. Press any key to continue with MR defined NVDATA values	Migration is not supported. When this message is displayed, contact your reseller or call maintenance personnel.
There are offline or missing virtual drives with preserved cache. Please check the cables and ensure that all drives are present.	Logical drives are not found. When this message is displayed, contact your reseller or call maintenance personnel.
There are offline or missing virtual drives with preserved cache. Please check the cables and ensure that all drives are present. Press any key to enter the configuration utility.	
Incompatible secondary iButton present! Please insert the correct iButton and restart the system. Press any key to continue but original equipment manufacturer (OEM) specific features will not be upgraded!	When this message is displayed, contact your reseller or call maintenance personnel.
Upgrade Key Missing! An upgrade key was present on a previous power cycle, but it is not connected. This can result in inaccessible data unless it is addressed. Please re-attach the upgrade key and reboot.	The upgrade key is not supported. When this message is displayed, contact your reseller or call maintenance personnel.
A snapshot rollback is in progress on VDs X, controller cannot boot until the rollback operation completes. Press any key to enter the configuration utility.	Snapshot is not supported. When this message is displayed, contact your reseller or call maintenance personnel.
The Following VDs: X have Rollback active and corresponding Repository missing. If you continue to boot the system or enter the configuration utility, these VDs will become unusable Press any key to Continue.	
Snapshot Repository VDs X have been removed from your system or are no longer accessible. Please check your cables and ensure all disks are present. If you continue to boot the system, the snapshot related data will be lost.	

MegaRAID SAS 2208

❑ Starting and ending MegaRAID WebBIOS

Use the following procedure to start the MegaRAID WebBIOS.

1 Turn on the power supply to the system equipment.

2 When the following screen appears, press and hold the **Ctrl** key, and press the **H** key.

The MegaRAID WebBIOS is started.

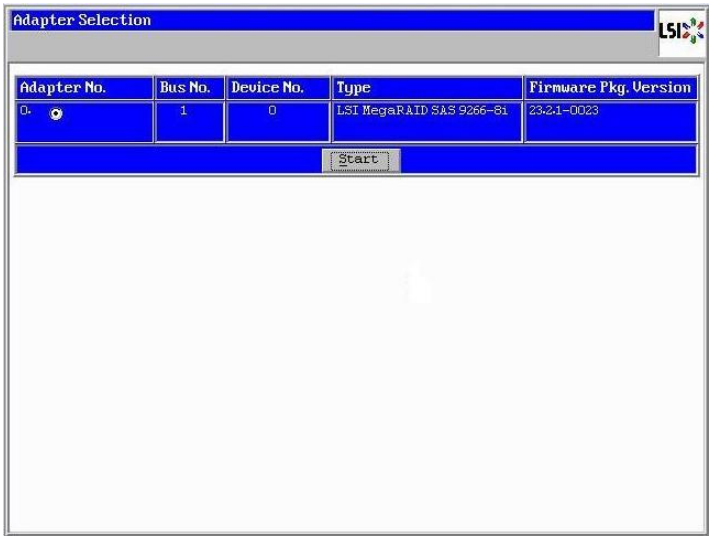
```
LSI MegaRAID SAS-MFI BIOS
Version x.xx.xx (Build xxx xx, xxxx)
Copyright(c) 2008 LSI Corporation
HA -0 (Bus x Dev x) MegaRAID SAS 8708 ERI
FW package: x.x.x-xxxx

x Virtual Drive(s) found on the host adapter.

x Virtual Drive(s) handled by BIOS
Press <Ctrl><H> for WebBIOS
```

If the operating system has been started before you press the keys, shutdown the operating system and then restart the system equipment. Check the manual for ending your operating system because some operating systems, such as Windows, require shutdown and other special operations when the particular operating system is terminated.

3 The MegaRAID WebBIOS is started and **Adapter Selection** appears.



4 Press the **Ctrl** key.

Note

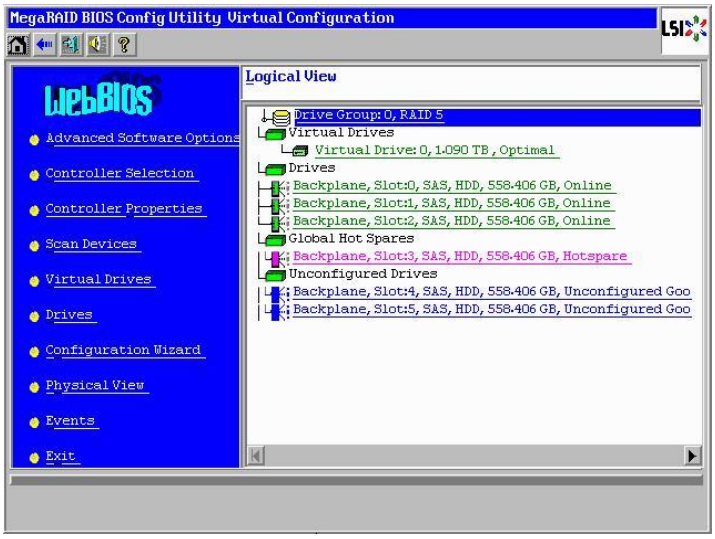
Without pressing the **Ctrl** key, your keyboard and mouse may not operate properly.

If the keyboard or mouse is not available when you operate MegaRAID WebBIOS, press the **Ctrl** key once.

5 Press **Enter** once.

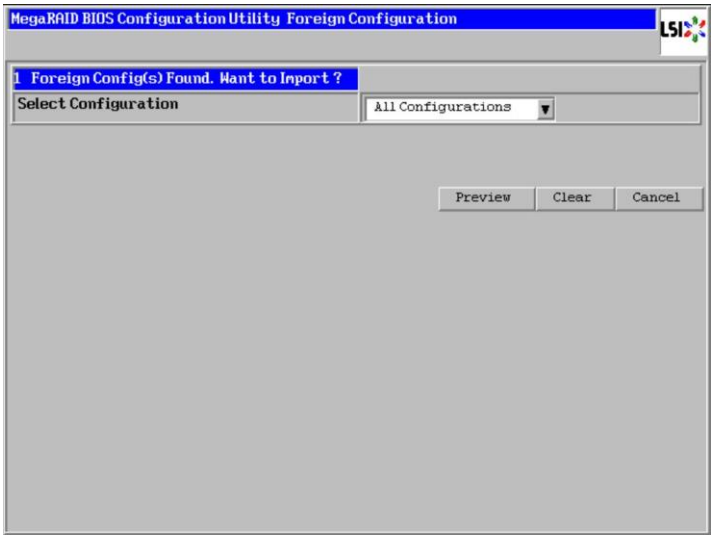
Without pressing **Enter**, the mouse will not work properly.

The main menu is displayed.



Tip

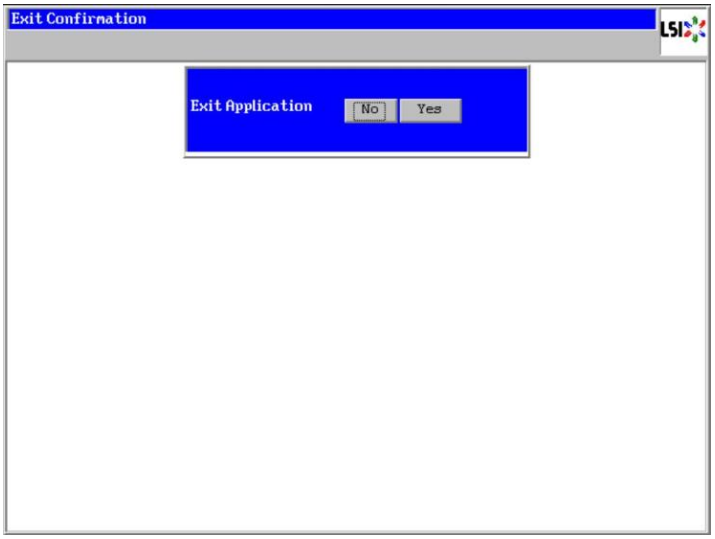
If a hard disk, which has a different disk array configuration coming from the record in the disk array controller board exists, the following screen is displayed. See “Disk with foreign configuration” for details.



Use the following procedure to end the MegaRAID WebBIOS.

1 From the main menu, click **Exit**.
The exit confirmation screen appears.

Tip When you want to return to the main menu, click Home or .



2 Click **Yes**.
Clicking **No** returns you to the main menu.

3 When the following message appears, power off the system equipment. Or, with the remote console application (Reclient), click **C+A+D** in the toolbar of the system console; with the remote console application (Java application), click **Keyboard > (Ctrl+Alt+Del)** in the toolbar or press **Alt + L** keys, to restart the system equipment.



Tip

For the remote console (Reclient), see the *Hitachi Compute Blade 2000 Remote Console Application User's Guide* contained in the remote console application CD that came with the system equipment.

For the remote console (Java application), see "Remote Console Application (Java Application)" in Chapter 3.

❑ Operation for MegaRAID WebBIOS

For MegaRAID WebBIOS, you can set individual items by using the following keys.

Connect a mouse to the remote console before starting MegaRAID WebBIOS.

Key/mouse	Operation
Mouse	Moves the mouse cursor.
Mouse - left button	- Selects an item that the mouse cursor is placed on. - Moves the cursor to an item to which the mouse cursor points. - Selects a disk array or physical hard disk.
0 to 9	Enters numerical values.
Ctrl	Selects multiple disk arrays or hard disks.
Del, Back Space	Deletes an entered value.

❑ Key operation for MegaRAID WebBIOS

This section describes how to operate the MegaRAID WebBIOS only with the keyboard.

Operating MegaRAID WebBIOS with keyboard

You can set the following items for MegaRAID WebBIOS using the keyboard.

Key	Operation
Tab	Moves the cursor in order. *1
Shift + Tab *2	Moves the cursor in reverse order.
Enter, Space	- Selects the item that the cursor is put on. - Determines an item setting. - Determines a disk array or physical hard disk.
[↑], [↓]	- Selects a disk array or physical hard disk. - Selects a setting value.
Shift	Selects multiple disk arrays or hard disks.
0 to 9	Inputs a numerical value.
Del, Back Space	Deletes an entered value.

*1 The item selected by the cursor is encircled by the dotted line.

*2 **Shift + Tab** is to press the **Tab** key while pressing the **Shift** key.



It may be hard to find the cursor on some screens. Press the **Tab** key or **Shift + Tab** keys to move the cursor so you can locate it.

Screen composition for MegaRAID WebBIOS

The main menu of the MegaRAID WebBIOS utility includes **Menu Icon**, which is not used in operation with the keyboard.

Operation in MegaRAID WebBIOS setting/disk array configuration

When operating MegaRAID WebBIOS only with the keyboard, replace the mouse with the keyboard as follows:

- Click (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.
- Place a check mark in (an object).

  Put the cursor on (the object) and press **Enter** or the **Space** key.

Execute a specific operation in setting or configuring a disk array, as follows:

- Selecting **Menu > Logical View > Physical View** in the main menu:

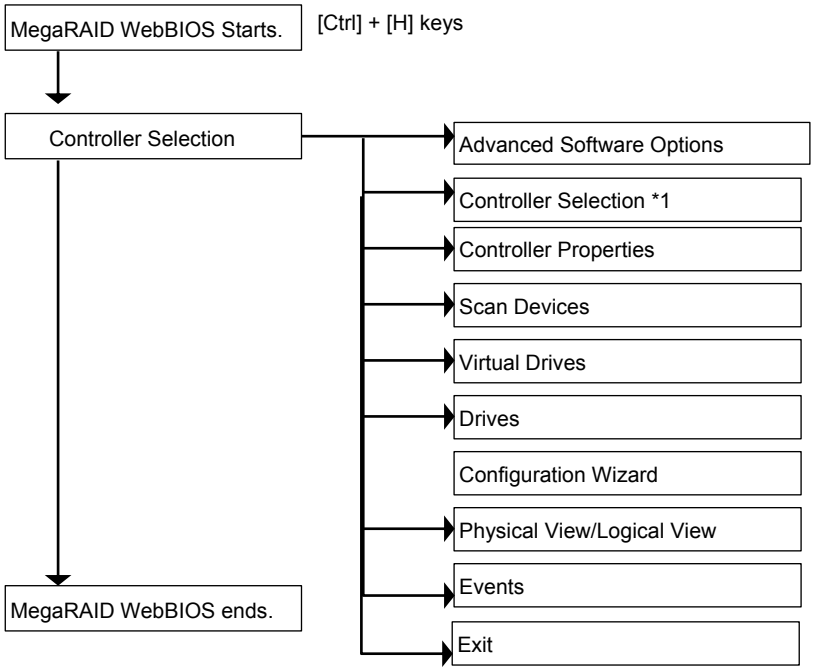
  Press the **Tab** key or press the **Tab** key while pressing the **Shift** key to move the cursor among **Menu**, **Logical View**, and **Physical View**.
  - When displaying the main menu, press the **Tab** key seven times to move the cursor to **Controller Selection** that is selected.
  - Move the cursor to **Events** or **Exit** using the **Tab** key. With the cursor on **Events** or **Exit**, press the **Tab** key once, and the cursor moves to **Logical View** or **Physical View** that is selected on the right on the screen.
  - With the cursor on **Logical View** or **Physical View**, press the **Tab** key twice, and the cursor moves to that is selected on the upper left of the screen.



- You can select a hard disk or disk array using [↑] and [↓] keys on the selection screen of **Logical View** or **Physical View**.
- Setting items in each menu.
  To change a setting value, put the cursor on the setting item box and select a new setting value using [↑] and [↓] keys or enter the setting value using the numerical keys.
- Selecting multiple hard disks in a disk array configuration.
  Press and hold the **Shift** key and select hard disks using [↑] and [↓] keys, and then press **Enter** or **Space** key.

❑ Configuration of MegaRAID WebBIOS

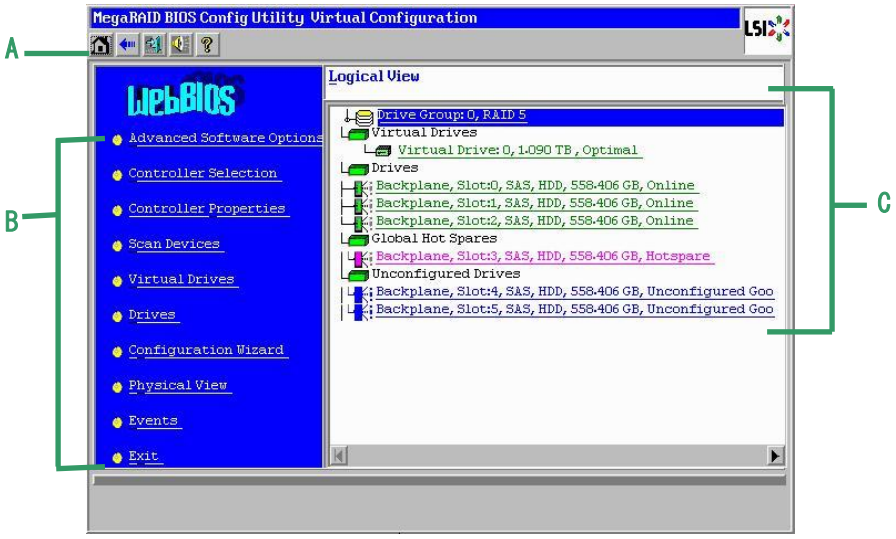
The MegaRAID WebBIOS is configured as shown below.



*1 “Adapter Selection” is displayed on the Controller Selection window.

❑ Screen configuration of MegaRAID WebBIOS

The screen configuration of MegaRAID WebBIOS is shown below.



A Menu icon

The following table shows the icons that are available.

Icon at the upper left on the screen	Operation from an icon click
	Return to the main menu.
	Return to the previous screen
	End the utility.
	Temporarily stop ringing the buzzer on the disk array controller board. (This function is not supported.)
	Display the version of MegaRAID WebBIOS,

B Menu

Menu items for MegaRAID WebBIOS are displayed. Click each item to go to the respective menu screen.

C Logical view/physical view

Hard disks or disk arrays connected to the disk array controller are displayed.

Tip

Click a hard disk from disks displayed in **Logical View** or **Physical View**, and the same screen is displayed as when you select **Drives > Properties** from the menu.

Select a disk array from disks displayed in **Logical View**, and the same screen is displayed as when you select **Virtual Drives > Properties** from the menu.

❑ Setting items for MegaRAID WebBIOS

This section describes the setting items and values for MegaRAID WebBIOS.

- The same alphanumeric characters are used to associate the setup screen and each of the items.
- In the table, the underlined values are default values. Those in brackets [ ] are recommended values.

  Example:

  [Enabled (valid)]/Disabled (invalid): "Enabled" is the Default and also the recommended value.

  [Enabled (valid)]/Disabled (invalid): "Disabled" is the Default value; and "Enabled" is the recommended value, which requires a setting change.

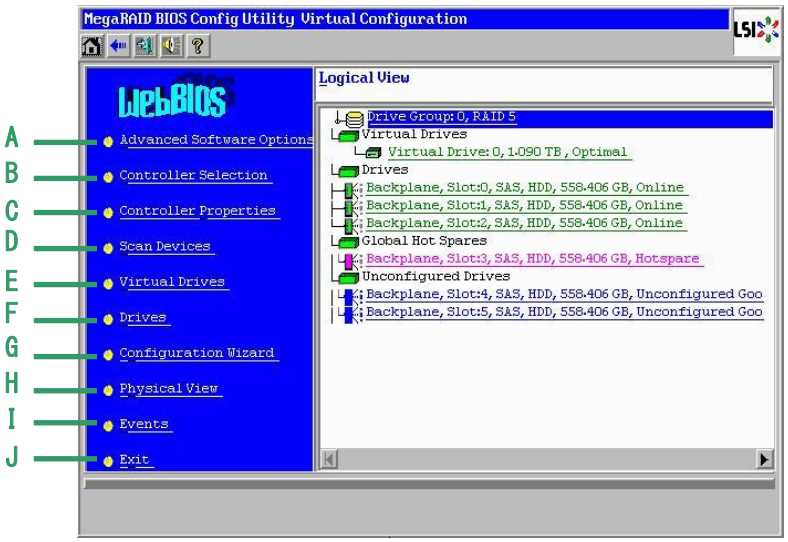
  When you need to change the setting from the Default to the recommended value, the recommended value is emphasized in red.

Note

Unless otherwise specified, use the recommended values for all setting items. If you set non-recommended values, the equipment would not be supported and might not operate properly.

Main menu

Start MegaRAID WebBIOS, and the following main menu appears.



Menu		Content	Setting/display value
A	Advanced Software Options	Setting advanced functions	-
B	Controller Selection *1	Selecting the disk array controller to be operated	-
C	Controller Properties	Viewing and setting the hardware information on the disk array controller board	See Controller properties: Menu for setting the disk array controller board.
D	Scan Devices	Scanning the installed devices	-
E	Virtual Drives	Viewing and setting the disk array (logical drive) information	See Virtual Drives: Viewing and setting disk array information.
F	Drives	Viewing and setting the hard disk (physical drive) information	See Drives: Viewing physical hard disk information.
G	Configuration Wizard	Building or formatting disk arrays	See Building disk arrays.
H	Physical View/Logical View	Switching display modes	See Switching the display mode.
I	Events	Displaying events	-
J	Exit	Ending the MegaRAID WebBIOS	See Ending Procedure.

*1 Adapter Selection is displayed on the Controller Selection screen.

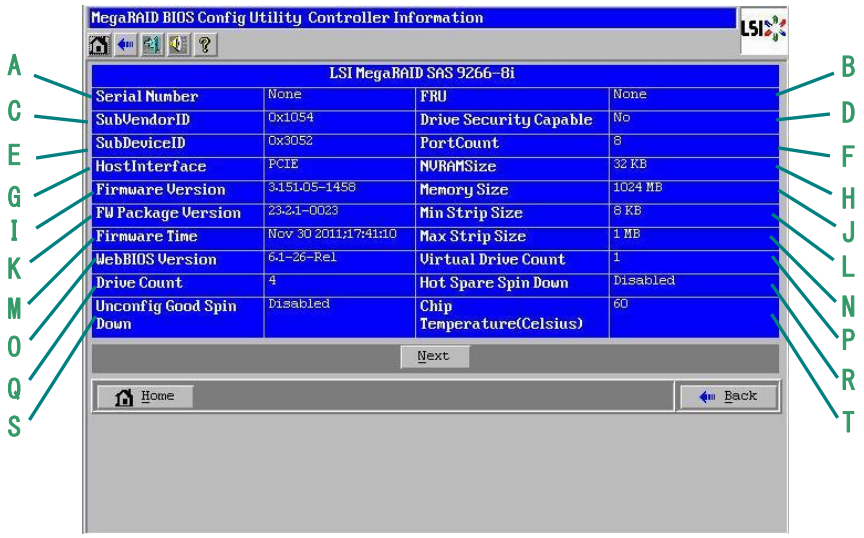
Tip

Do not use **Advanced Software Options**] and **Events** because they are not supported.

Controller properties: Menu for setting the disk array controller board

You can display and set the hardware information about the disk array controller board.

Select **Controller Properties** from the main menu. The following screen appears:



Display item		What is displayed
A	Serial Number	Serial number
B	FRU	Board name per maintenance
C	SubVendorID	Sub-vendor ID
D	Drive Security Capable	Encryption function: Enable or Disable
E	SubDeviceID	Sub-device ID
F	PortCount	Number of ports installed
G	HostInterface	Host interface
H	NVRAM Size	Size of NVRAM installed
I	Firmware Version	Firmware version
J	Memory Size	Size of memory installed
K	FW Package Version	Firmware package version
L	Min Stripe Size	Minimum stripe size
M	Firmware Time	Current time at which the firmware acquires
N	Max Stripe Size	Maximum stripe size
O	WebBIOS Version	MegaRAID WebBIOS version
P	Virtual Drive Count	Exisiting number of array configurations (logical devices)
Q	Disk Count	Number of physical devices installed
R	Hot Spare Spin Down	Power capping mode set to a hard disk with hopspare
S	Unconfig Good Spin Down	Power capping mode set to unused hard disks
T	ChipS Temperature (Celsius)	Chip temperature in Celsius

Tip

You cannot change the settings for those items displayed here.

Properties: Controller properties submenu 1

Click **Next** in the **Controller Properties** screen, and the following screen appears.



Display item		What is displayed
A	Global Hot spare for Emergency	Whether or not to rebuild a different type of drive for global hot spare.
B	Unconfig Good for Emergency	Whether or not to rebuild a different type of unconfigured physical drive.
C	Emergency for SMARTer	Whether or not to apply SMART copy back to a different type of physical drive for hotspare.
D	Shield State Supported	Diagnostics for physical drives *1
E	SSD Disk Cache Setting	SSD cache setting value.
F	Metadata Size	Metadata size of the disk array controller.

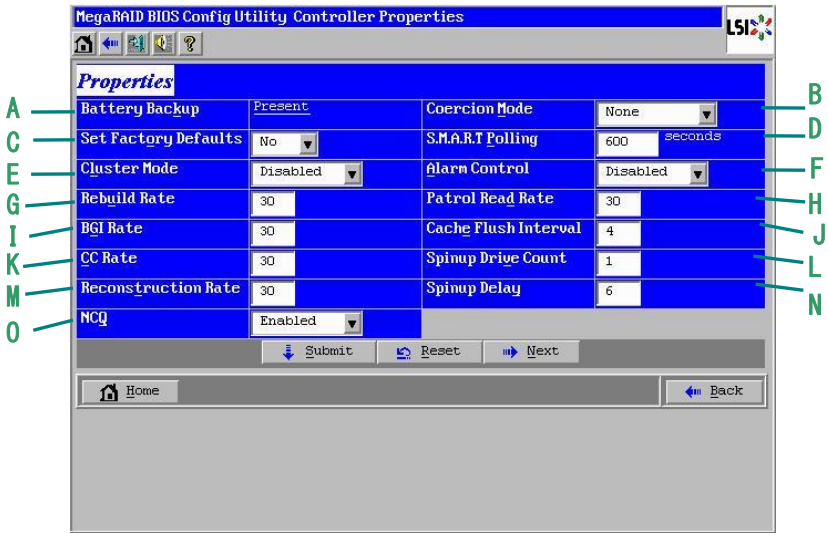
*1: Diagnostics for physical drives is not supported.

Tip

Those values shown in this screen cannot be changed.

Properties: Controller properties submenu 2

Click **Next** in the **Properties: Controller properties submenu 1** screen, and the following screen appears.



Display item		Display/content	Setting/display value **
A	Battery Backup *1	Cache backup module mount status.	None/Present (See Battery module: BBU setting submenu.)
B	Coercion Mode *2	Setting the capacity control for the physical hard disk used for disk array building	[None (using the entire capacity)] / 128 MB-way (using a capacity as a multiple of 128 MB) / 1 GB-way (using a capacity as a multiple of 1 GB)
C	Set Factory Defaults *3	Returning all the settings to their Defaults values	—
D	S.M.A.R.T Polling *4	Setting the interval of S.M.A.R.T. reporting	0 to 65535 / 300 / [600]
E	Cluster Mode *5	Setting the cluster mode	[Disabled (invalid)] / Enabled (valid)
F	Alarm Control	Sounding the buzzer on the controller in the event of a fault at a connected device	[Disabled (not sounding)] / Enabled (sounding) / Silence (stop sounding temporarily)
G	Rebuild Rate *5	Priority of rebuilding	0 to 100 / [30]
H	Patrol Read Rate *5	Priority of patrol reading	0 to 100 / [30]
I	BGI Rate *5	Priority of background initializing	0 to 100 / [30] (BGI: background initializing)
J	Cache Flush Interval *5	Flash timing for write-cache data	1 to 255 / [4]
K	CC Rate *5	Priority of integrity inspection	0 to 100 / [30]
L	Spinup Drive Count *5	Number of hard disk motors started at system startup	0 to 8 / [4]
M	Reconstruction Rate *5	Priority of capacity expansion	0 to 100 / [30]
N	Spinup Delay *5	Timing for hard disk motors started at system startup	0 to xxx / [6]
O	NCQ *5	Setting the NCQ command	[Enabled] / Disabled (NCQ: native command queuing)

*1 If with a cache backup module installed, **Present** is shown and **Battery Module: BBU** setting submenu is displayed.

*2 This can be changed only when no disk arrays have been set at all.

*3 Do not use **Set Factory Defaults**. This setting must be changed to the recommended values.

*4 Change the value to the recommended value.

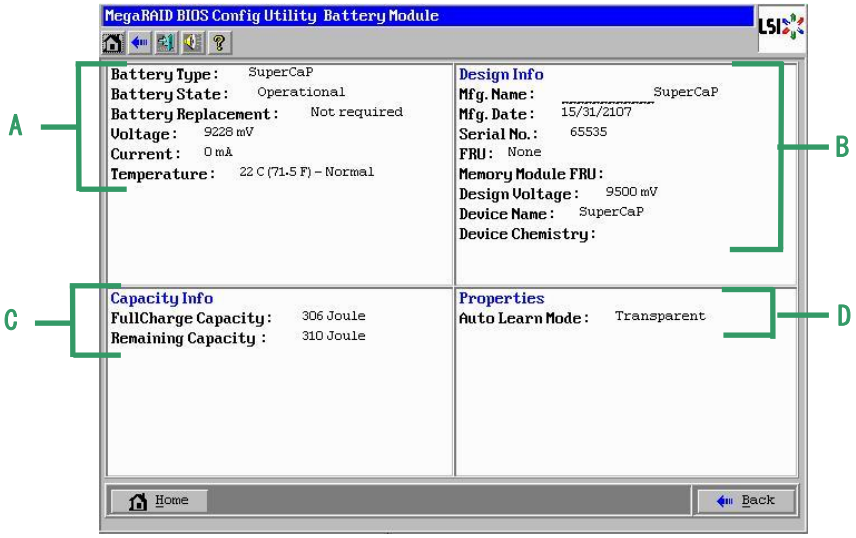
*5 Always use the Default setting.



- Place the mouse cursor on a setting item and left-click the mouse to change the setting values. Or, left-click the mouse to move the cursor and enter a value from the keyboard. Click **Submit** after the setting.
- Values of **Spin Drive Count** and **Spin Delay** are fixed.

Battery module: BBU setting submenu

Click **Battery Backup > Present** in the **Properties: Controller properties submenu 2** screen, and the following screen appears.

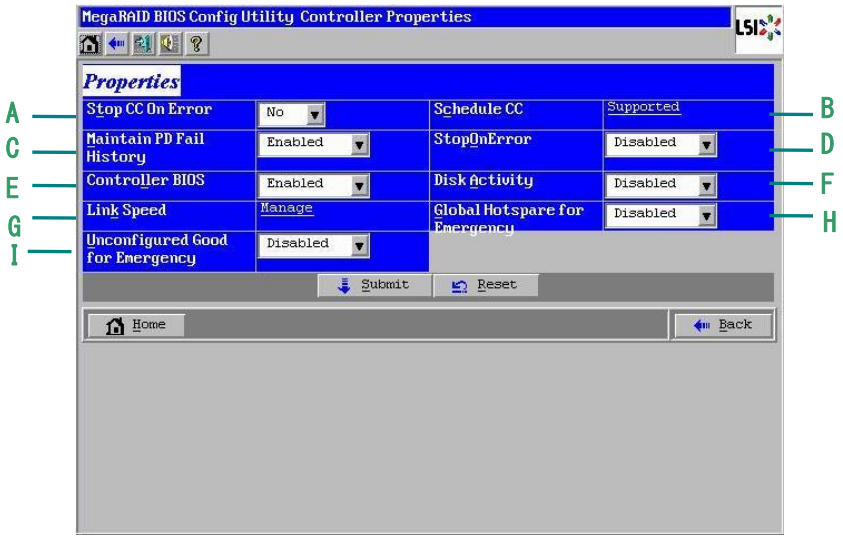


Display item		Display/content	Setting/display value **
A	Battery type	A type of the battery	Displayed only
	Battery State	A state of the battery	Displayed only
	Battery Replacement	Whether or not to need battery replacement.	Displayed only
	Voltage	Voltage amount	Displayed only
	current	Current amount	Displayed only
	Temperature	Temperature	Displayed only
B	Mfg. Name	Product name	Displayed only
	Mfg. Date	Date of manufacture	Displayed only
	Serial No.	Serial number	Displayed only
	FRU	Cache backup module name per maintenance	Displayed only
	Memory Module FRU	Memory module name per maintenance	Displayed only
	Design Voltage	Design voltage amount	Displayed only
	Device Name	Device name	Displayed only
	Device Chemistry	Device element	Displayed only
C	FullCharge Capacity	Maximum electrostatic capacitance	Displayed only
	Remaining Capacity	Remaining electrostatic capacitance	Displayed only
D	Auto Learn Mode	Automatic diagnostics	Displayed only

Properties: Controller properties submenu 3

Click **Next** in the **Properties: Controller properties submenu2** screen, and the following screen appears.

Stop CC On Error, **Schedule CC**, **Maintain PD Fail History**, and **Disk Activity** are not supported. Do not set those items.



Setting item		Description	Setting/display value **
A	Stop CC On Error *1	Sets an operation when an error is detected at the consistency check.	[No (continuous operation)] / Yes (stops the consistency check.)
B	Schedule CC *1	Sets a consistency check schedule.	When clicking [Supported], the screen moves to “Schedule CC Page: Schedule Consistency Check setting submenu”.
C	Maintain PD Fail History *1	Sets whether or not a failed hard disk can be used.	[Enabled (Registers failed hard disk information.)] / Disabled (Not register failed hard disk information.)
D	Stop On Error *2	Sets whether or not to boot the OS when an error is detected at the consistency check.	[Disabled)] / Enabled
E	Controller BIOS	Sets the disk array controller BIOS	[Enabled)] / Disabled
F	Disc Activity *1	Sets hard disk LED switching.	[Disabled)] / Enabled
G	Link Speed	Sets the physical drive link speed.	Click [Manage] to go to Link Speed: Link Speed submenu.
H	Global Hot spare for Emergency *1	Sets whether or not to rebuild a different type of physical drive for global hot spare.	[Disabled)] / Enabled
I	Unconfigured for Emergency *1	Sets whether or not to rebuild an unconfigured physical drive.	[Disabled)] / Enabled

*1 Do not set this item, which is not supported.

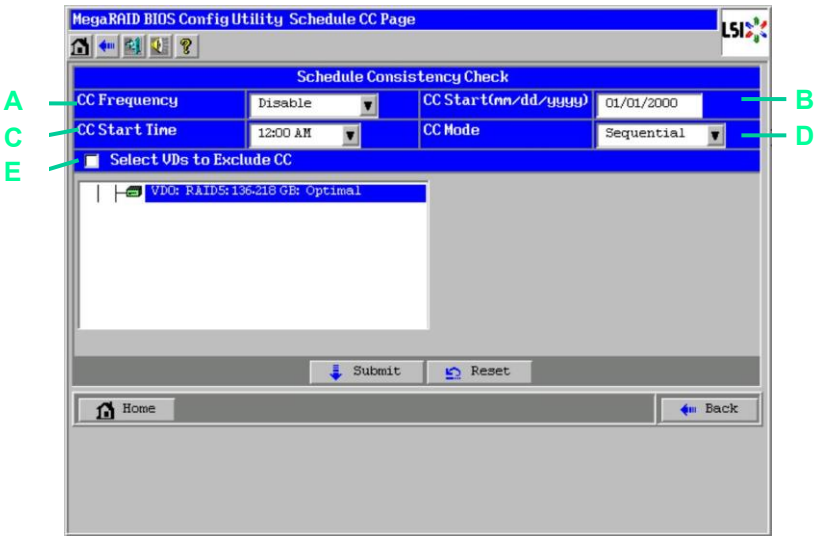
*2 Make sure to use this item with the default setting.

Schedule CC Page: Schedule Consistency Check setting submenu

Click **Supported** of Schedule CC in the **Properties: Controller Properties submenu 2** screen, and the following screen appears.

Note

The following items are not supported. Do not set these items.

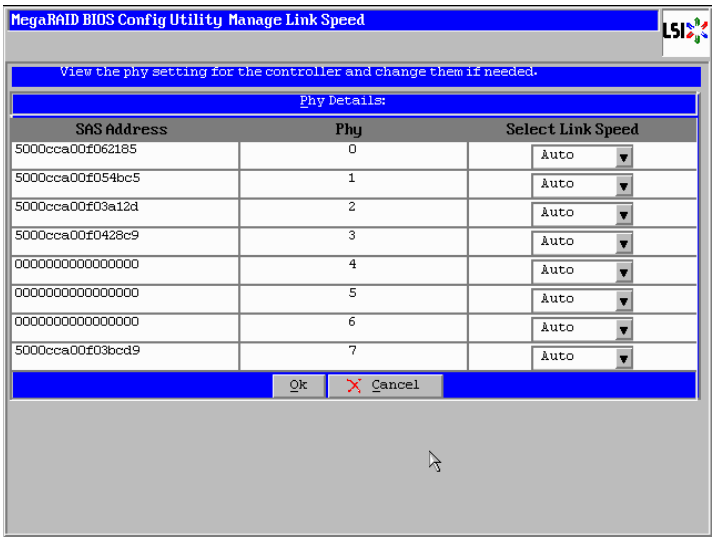


Setting item		Description	Setting/display value **
A	CC Frequency	Sets the CC schedule function: Enable or Disable	[Disable (invalid schedule)] / Continuous / Hourly / Daily / Weekly / Monthly
B	CC Start (mm/dd/yyyy)	Sets on what date the consistency check starts.	[01/01/2000]/Choose any date. *1
C	CC Start Time	Sets on what time the consistency check starts.	[12:00 AM]/.03:00 AM / Choose any date.*1
D	CC Mode	Sets if the consistency check is executed on multiple disk arrays.	[Sequential (a consistency check per array)] / Concurrent (a consistency check on multiple arrays)
E	Select VDs to Execute CC	Specifies a disk array on which the consistency check is executed.	Choose any array configuration.

*1 This item is automatically set by disabling CC Frequency.

Link Speed: Link Speed submenu

Click **Link Speed > Manage** of Schedule CC in the **Properties: Controller Properties submenu3** screen, and the following screen appears. This system, however, does not support the Link Speed submenu. Use those default values as shown below for all items.

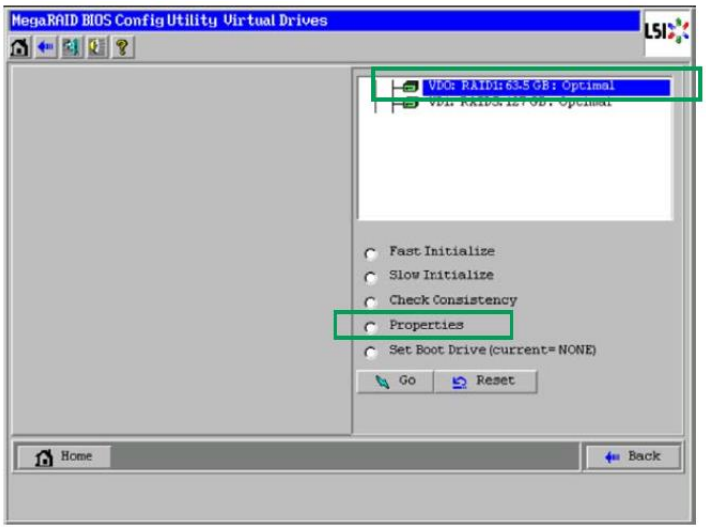


Setting item		Description	Setting/display value **
A	Select Link Speed	Sets the speed to link to physical drives	[Auto] / 1.5 Gbps/ 3 Gbps/ 6 Gbps

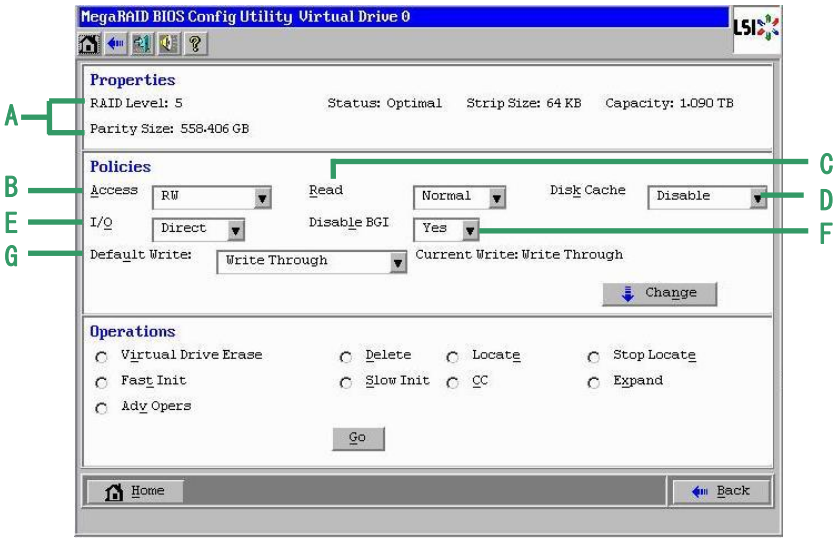
Virtual Drives: Viewing and setting disk array information

You can view and change the information on the disk array (logical drive) that is already set.

Select **Virtual Drives** in the main menu, and the following screen appears:



Select a disk array for viewing information and changing the setting from the list on the upper right of the screen. Check **Properties** and then click **Go**, and the disk array properties screen appears.



NOTICE

When enabling the write cache of the disk array, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and become corrupted.

Display item		What is displayed	Setting/display value **
A	RAID Level	RAID level	-
	Status	Status of the disk array	-
	Strip Size	Stripe size of the disk array	-
	Capacity	Size of the disk array	-
	Parity Size *1	Size of the parity	-
B	Access	Access mode	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
C	Read	Read policy	[Normal (no advance reading)] / Ahead (always advance reading) / Adaptive (advance reading only in the event of sequential access)
D	Disk Cache	Setting the cache installed in a physical hard disk	[Disable (cache: not used)] / [Enable (cache: used) / Unchanged (based on the hard disk setting)]
E	I/O	Setting the read-cache operation	[Direct (reading from the cache at a cache hit)] / [Cached (always reading from the cache)]
F	Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
G	Default Write *2 *3	Setting the write cache	Without cache backup module installed * 4: [Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.) With cache backup module installed * 5: Write Through (write-cache invalid)/ Always Write Back (write-cache valid)/[Write Back With BBU (Write cache is valid only when a cache backup module is installed.)]

*1 This item is shown with RAID Level 5 or 6.

*2 **Default Write** supports setting in **Always Write Back** only when the system equipment without a cache backup module installed is connected to UPS. Even so, set **Write through** when installing OS. Otherwise, the installation may not finish properly. Do not set **Write Back with BBU**.

*3 For the equipment with a cache backup module installed, make sure to set **Write Back With BBU** for Default Write. If not, write performance may slow down.

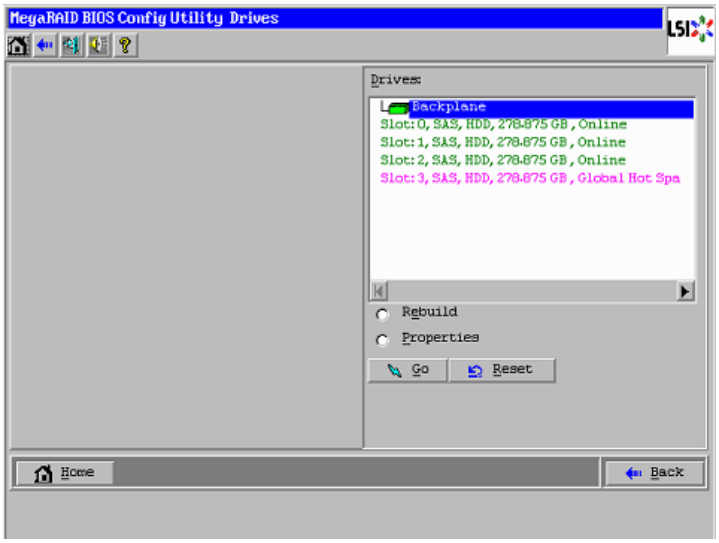
*4 **None** is shown for Battery Backup in Properties: Controller properties submenu 2.

*5 **Present** is shown for Battery Backup in Properties: Controller properties submenu 2.

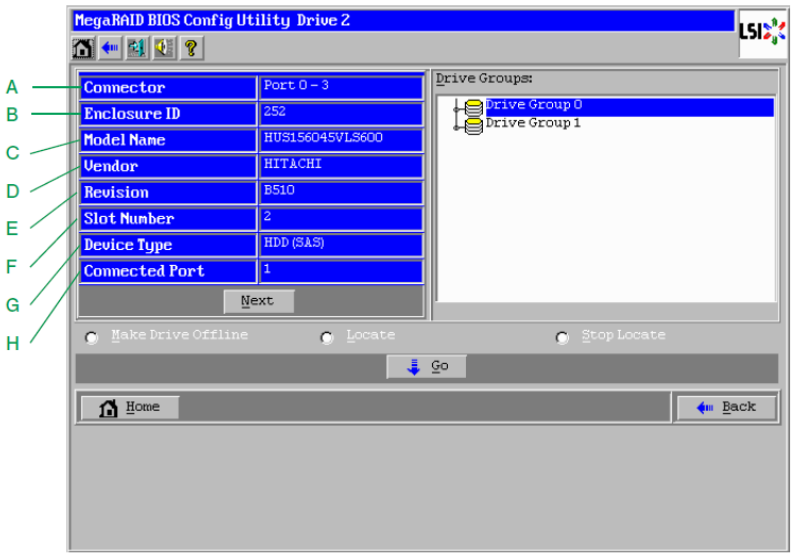
Drives: Viewing physical hard disk information

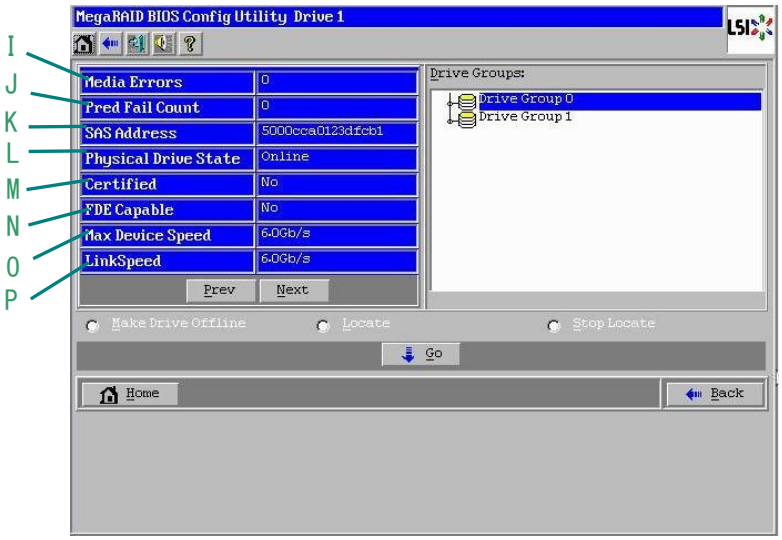
Here you display the information on the physical hard disk in the physical drive connected to the disk array controller.

Select **Drives** in the main menu, and the following screen appears:

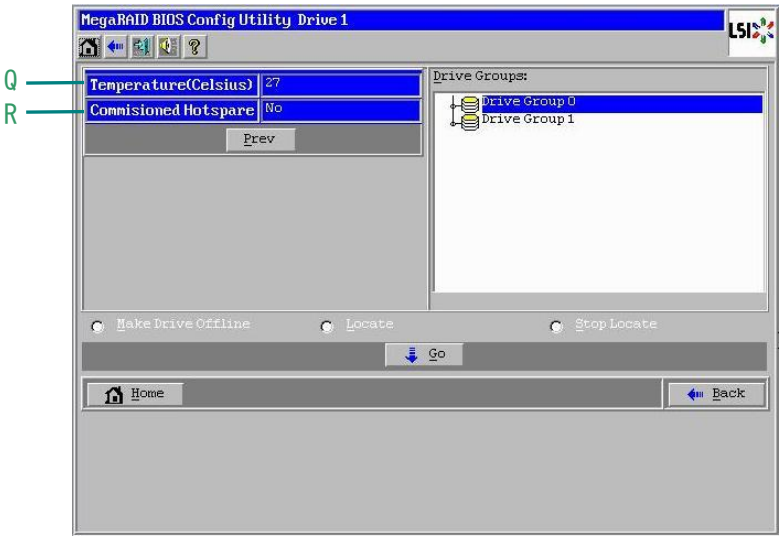


Select a disk array for viewing and setting information from the list on the upper right of the screen. Check **Properties** and then click **Go**. The hard disk properties screen appears.





When clicking **Next**, you can view the following screen.



When clicking **Prev**, you can return to the previous screen.

Display item		What is displayed
A	Connector	Disk array controller board connector connected
B	Enclosure ID	ID number of the enclosure device connected
C	Model Name	Disk model name
D	Vendor	Vendor name
E	Revision	Firmware version
F	Slot Number	Number of the slot installed
G	Device Type	Device type
H	Connected Port	Port number of the disk array controller board connected
I	Media Errors	Number of media errors detected
J	Pred Fail Count	Number of S.M.A.R.T. warnings reported

Display item		What is displayed
K	SAS Address	SAS address
L	Physical Drive State	Physical hard disk status
M	Certified	Certification
N	FDE Capable	Full Disk Encryption: Capable or No
O	Max Device Speed	The maximum connection speed
P	Link Speed	Link speed
Q	Temperature (Celsius)	Hard disk temperature
R	Commissioned Hotspare	Fault tolerance by Hotspare

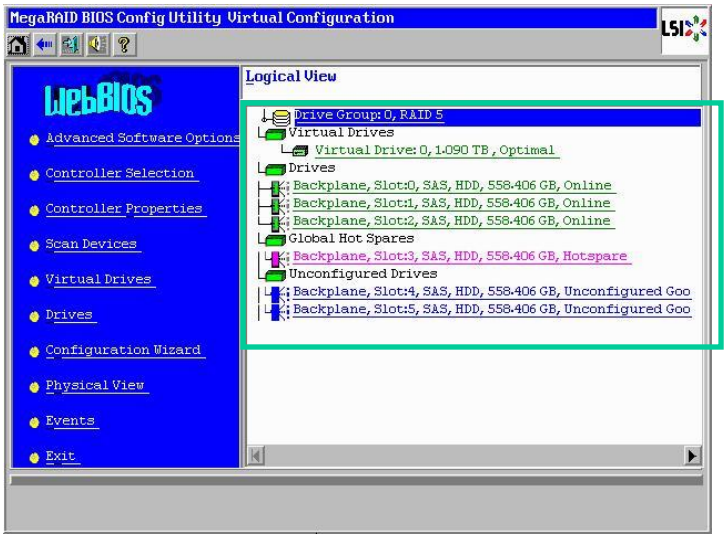


- Items described in the table above cannot be changed.
- For the status of the physical hard disk, see "Status".
- **Media Errors** and **Pred Fail Count** are cleared when the system is powered off or rebooted.

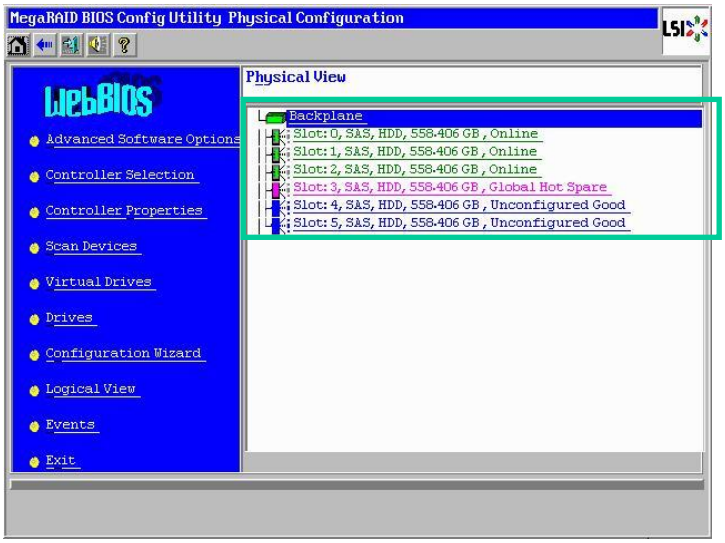
❑ Switching the display mode

This section describes switching disk array display modes in the main menu.

There are two types of display mode: **Logical Vi**ew and **Physical View**.
The Logical View mode displays a list of disk array configurations that are already set, physical hard disks comprising a disk array configuration, and hot spare information.
The Physical View mode displays a list of physical hard disks.



Logical View mode:
Disk array/Physical hard disks/Global hot spare



Physical View mode:
List of physical hard disks

Tip

- The Logical View mode is applied when the MegaRAID WebBIOS is started.
- To switch to the physical view mode, click **Physical View** in the Logical View mode from the main menu.
- To switch to the logical view mode, click **Logical View** in the Physical View mode from the main menu.

❑ Building disk arrays

This section describes the procedure for building disk arrays.

The building of disk arrays should be entirely performed from the Configuration Wizard.

> ***NOTICE***
>
> You must not change the disk array during system operations. If you do, all data will be lost from those disks due to change in the disk array.

Note

Make sure to set each item to the recommended value unless other specific directions are given, otherwise, the system may not properly operate. We are not responsible for a malfunction due to any settings except our recommended values.

Building disk arrays for RAID 0, 1, 5, and 6

This section describes the procedure for building new disk arrays.

The following procedure is for building disk arrays for RAID 0, 1, 5 and 6.

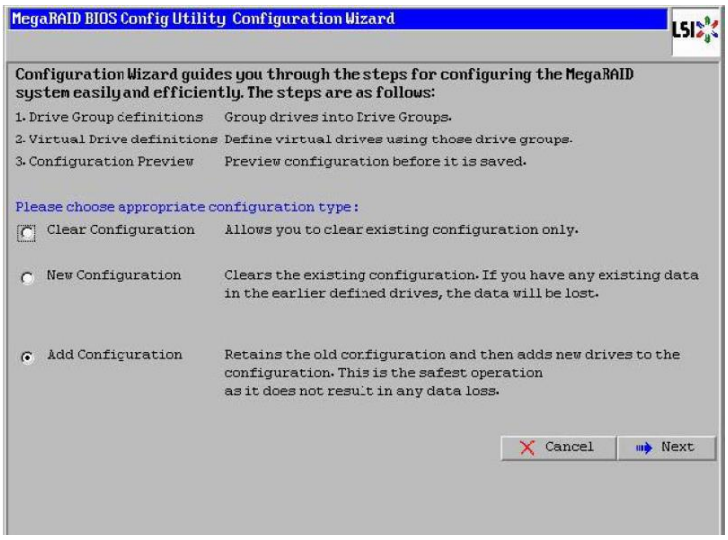
> ***NOTICE***
>
> RAID0 configuration (single hard disk configuration) has no redundancy. Thus, if the hard disk fails, all data will be lost.
>
> It is recommended that you use the system with RAID1/RAID5/RAID6/ RAID10 configuration to ensure data redundancy and improve resistance to failure.

Tip

To build RAID 10, see "Building disk arrays for RAID 10".
For information about how to set hotspare, see "Setting hotspares."

1 Select **Configuration Wizard** from the main menu.

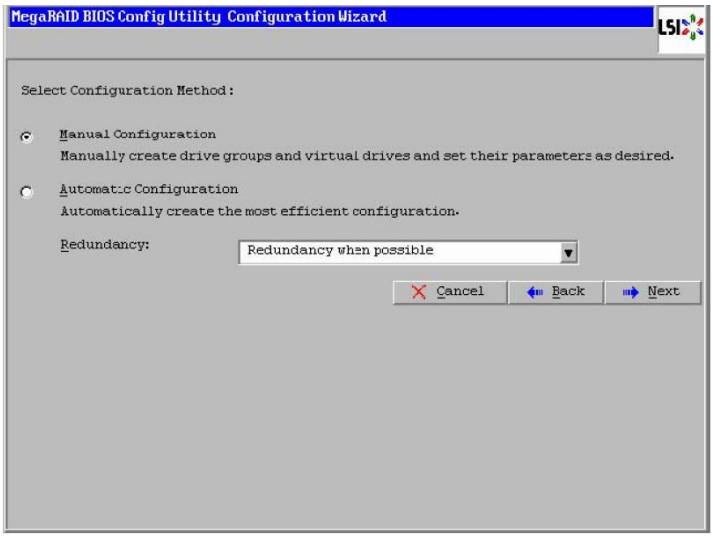
The following screen appears:



NOTICE

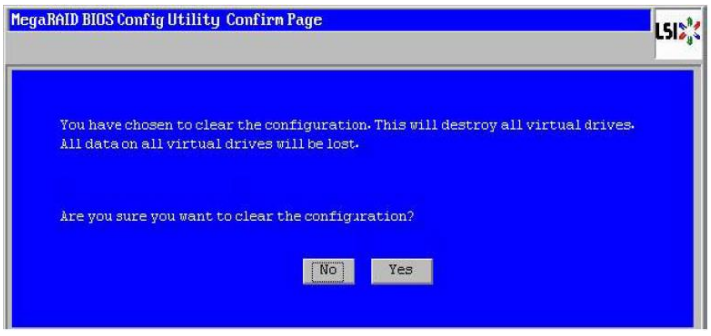
If you select **New Configuration**, all data in those hard disks including the disk array information will be lost. Backup your required data before selecting **New Configuration**.

2 Check **New Configuration** or **Add Configuration** and click **Next**.
The following screen appears:



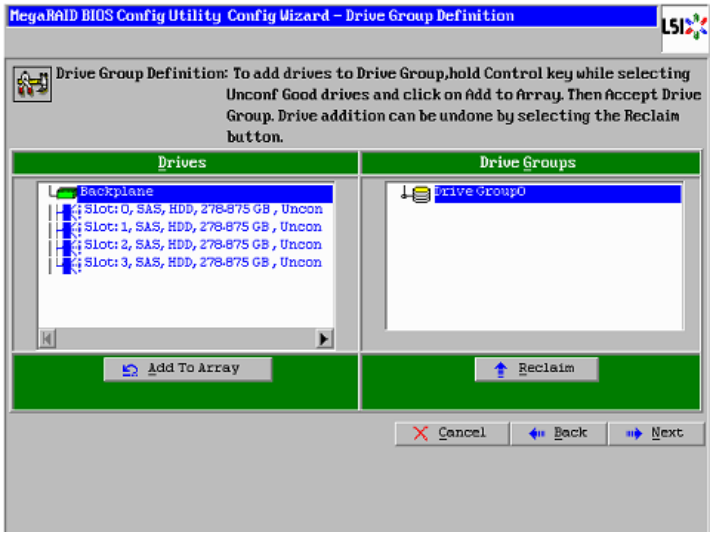
Tip

- Existing disk groups and disk arrays will remain when you select **Add Configuration**. **Add Configuration** should be selected when you want to add disk arrays to an existing disk group or to build disk arrays using an additional hard disk.
- If you select **New Configuration**, you lose existing disk groups and disk arrays. This should be selected when you discard existing drive groups and disk arrays to build a new one.
- If you select **New Configuration**, the following screen appears. Clicking **Yes** allows you to build a disk array.



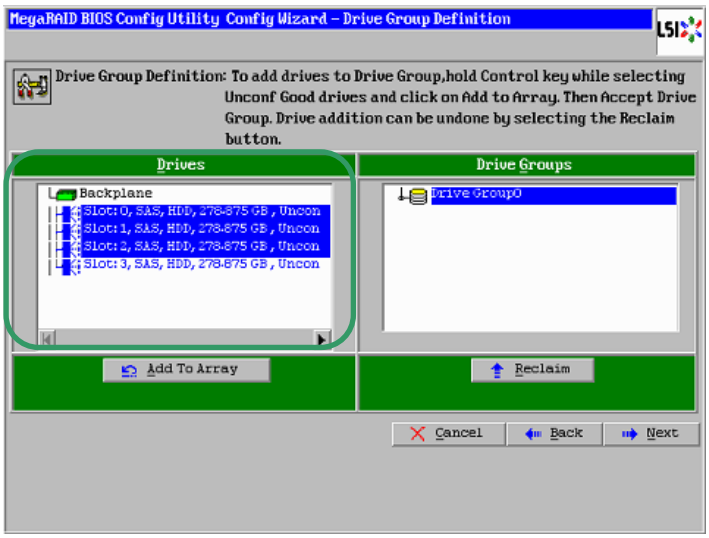
3 Check **Manual Configuration** and click **Next**.

The following screen appears:



4 Select a hard disk to be used for building a disk array.

When building a disk array with hard disks on status of **Unconfigured Good** (unused), select hard disks in the **Drives** pane.
When adding a disk array to an existing drive group, go to step 7 without selecting a hard disk.



The number of hard disks required varies depending on the RAID level to be set. The following table summarizes the number of hard disks required.

RAID level	Number of hard disks required
RAID 0	1 or more
RAID 1	2
RAID 5	3 or more
RAID 6	4 or more

Note

RAID 6 with 3 hard disks and RAID 1 with 3 or more hard disks are not supported. If you set this, the system might not operate properly.

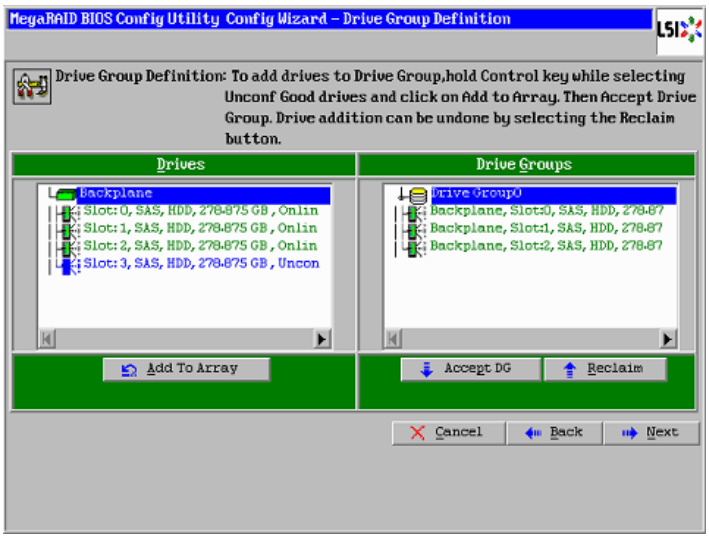
Tip

You can select only a hard disk whose status is **Unconfigured Good** (unused).

To select multiple hard disks, click them while pressing the **Ctrl** key.

5 After selecting all hard disks for building a disk array, click **Add to Array**.

Status of those selected hard disks is **Online** as shown in the **Drives** pane.

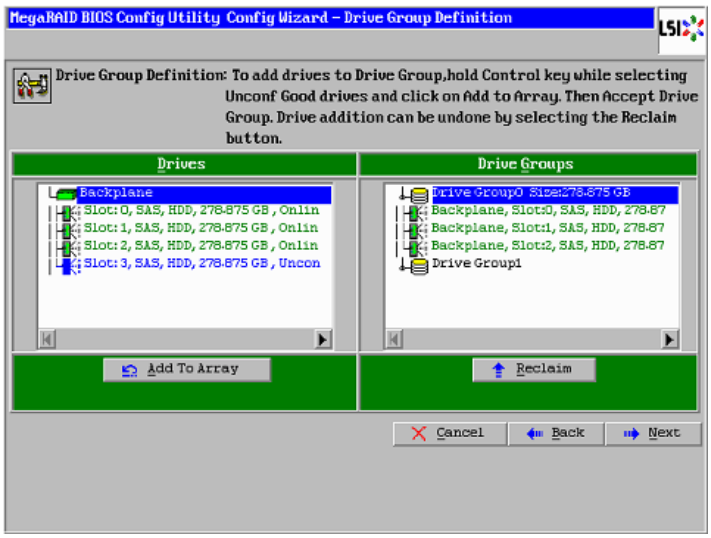


Tip

To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

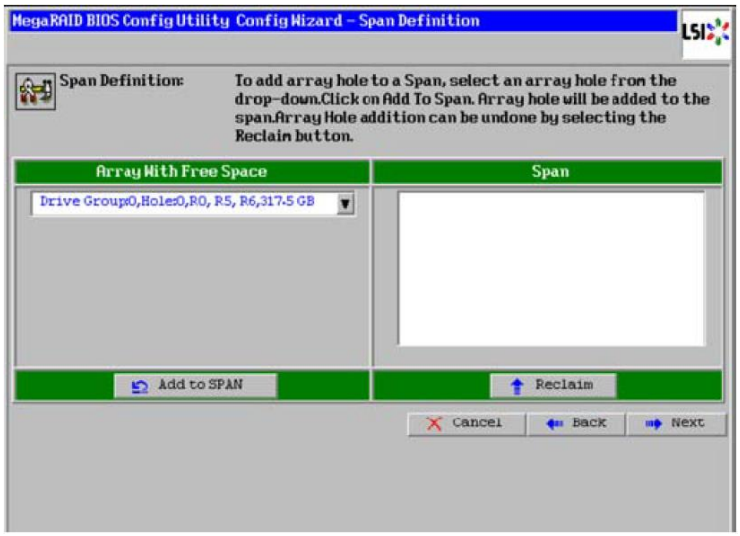
6 Click **Accept DG**.

The following screen appears:



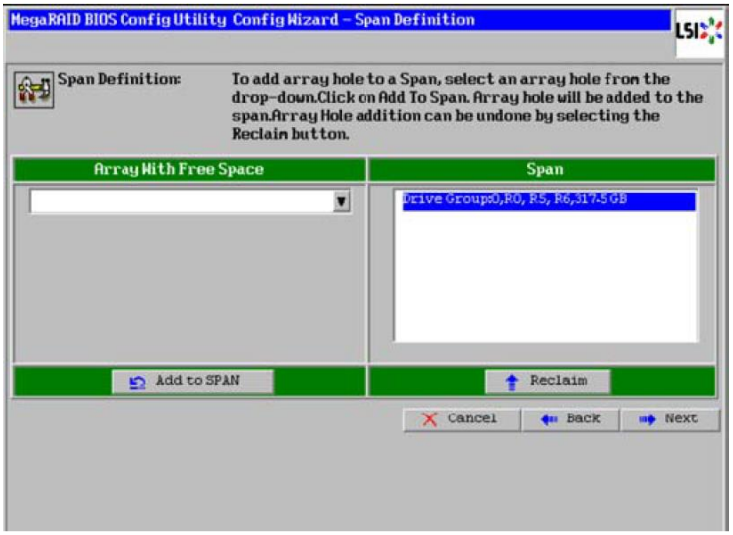
7 Click **Next**.

The following screen appears: Select the target drive group from the pull-down menu of **Array With Free Space**.



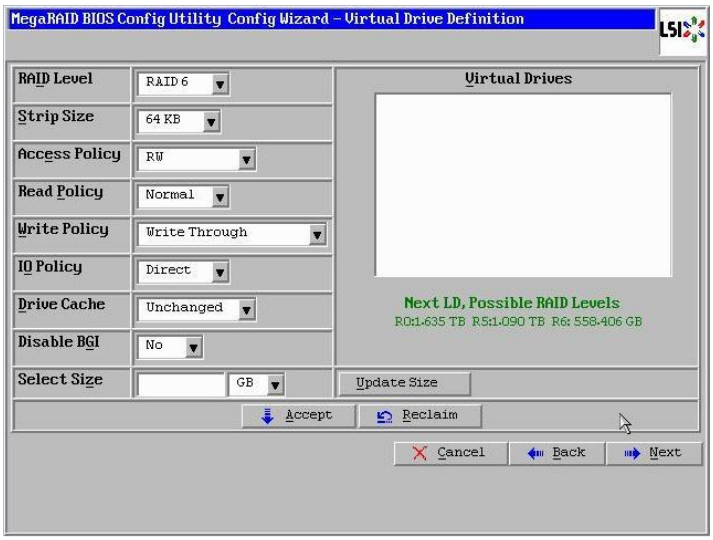
8 Click **Add to SPAN**.

The following screen appears:



9 Click **Next**.

The following screen appears:



10 Specify the RAID level, stripe size, read policy, write policy, and disk array size.

> ***NOTICE***
>
> When enabling the write cache of the disk array with the equipment that has no cache backup module installed, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Set each item to the values in the following table.

Item	Content	Setting value **
RAID Level *1 *2	RAID Level	Specify any level.
Stripe Size *3	Stripe size (only RAID 0 and 5)	8 KB / 16 KB / 32 KB / [64 KB] / 128 KB / 256 KB / 512 KB / 1 MB
Access Policy	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advance reading)] / Ahead (always advance reading)
Write Policy *4 *5	Write policy	Without cache backup module installed * 7: [Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.) With cache backup module installed * 8: Write Through (write-cache invalid)/ Always Write Back (write-cache valid)/[Write Back With BBU (Write cache is valid only when a cache backup module is installed.)]
IO Policy	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)
Drive Cache	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)

Item	Content	Setting value **
Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *6	Size of a disk array	Enter a value up to the maximum capacity value. The lowest available value is 64 KB.

*1 RAID 6 with three hard disks and RAID 1 with three or more hard disks are not supported.

*2 When you add a disk array to an existing drive group, the RAID level cannot be changed.

*3 For RAID 1, set 64KB by Default.

*4 In Write Policy, **Write Back** can be set only when the system equipment without a cache backup module installed is already connected to the UPS (uninterruptible power supply). Confirm that the checkmark is removed from **Wrthru for BAD BBU** at that time. Even in this case, set **Write Through** when the operating system is installed, otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays. Do not select **Write Back with BBU**.

*5 When the equipment has installed a cache backup module, make sure to set **Write Back With BBU** for Write Policy. If not, write performance may slow down.

*6 Maximum capacity size that can be set is shown under **Next LD, Possible RAID Levels** at the right of the screen. Type a new value up to the maximum capacity value for your RAID level. Delete the exisiting value before typing a new numeric value. When specifying the maximum capacity value, click **Update Size**.

*7 **None** is shown for Battery Backup in Properties: Controller properties submenu 2.

*8 **Present** is shown for Battery Backup in Properties: Controller properties submenu 2.



When a drive group contains multiple disk arrays, specify the same setting values on all disk arrays in the drive group.

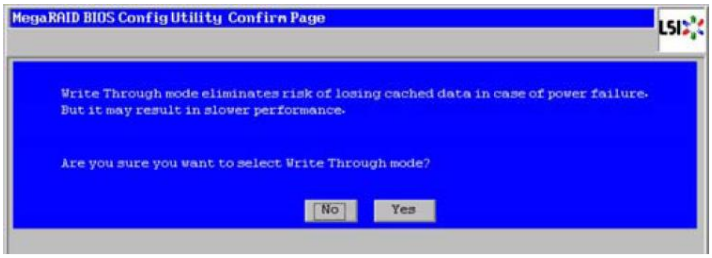


- When you configure a disk array to install an OS and enter a value larger than 2 TB, the OS will only recognize up to 2 TB.
- If you specify a larger disk array size than the maximum capacity, **Unacceptable size** appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

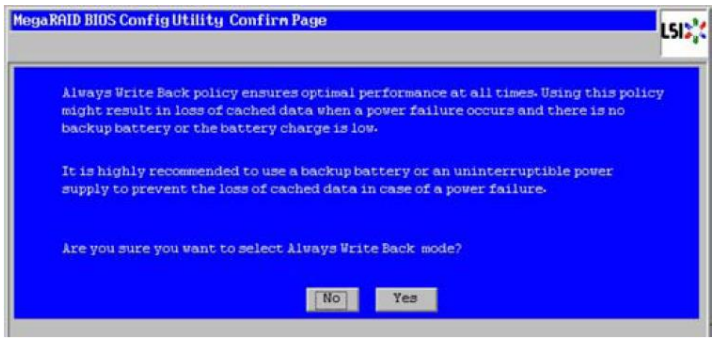
11 Click **Accept** .

One of the following screens appears.

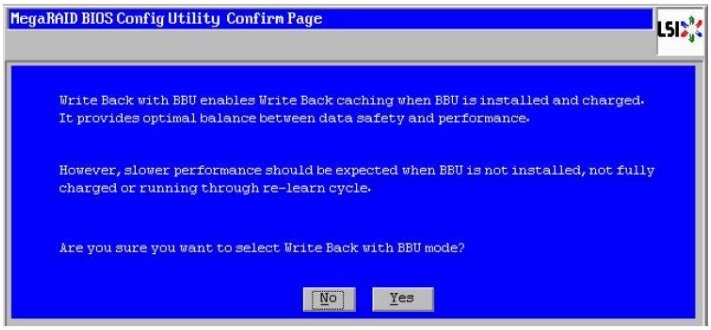
- When selecting **Write Through** in the write policy setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the write policy setting, the following screen appears. Click **Yes**.



- When selecting **Write Back with BBU** in the write policy setting, the following screen appears. Click **Yes**.



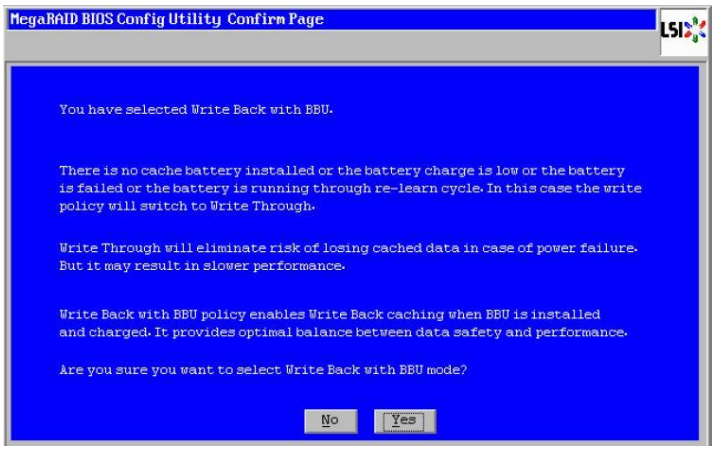
Tip

When Write Back with BBU is set as Write policy to the equipment without a cache backup module installed (*1), click **No** in the following screen. Clicking **No** returns to the screen shown in Step 9 and then set it again.

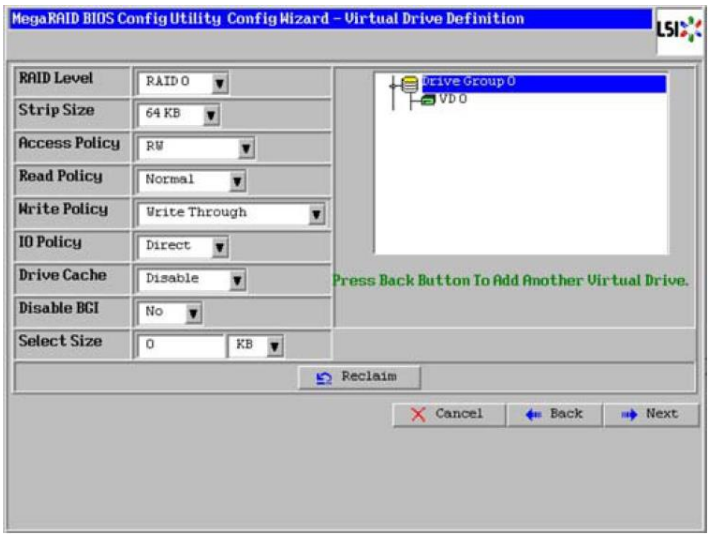
When Write Back with BBU is set as Write policy to the equipment with a cache backup module installed (*2) and the cache backup module status is checked, the following screen appears. Click **Yes**.

(*1): **None** is shown for Battery Backup in the **Properties: Controller properties submenu 2**.

(*2): **Present** is shown for Battery Backup in **Properties: Controller properties submenu 2**.

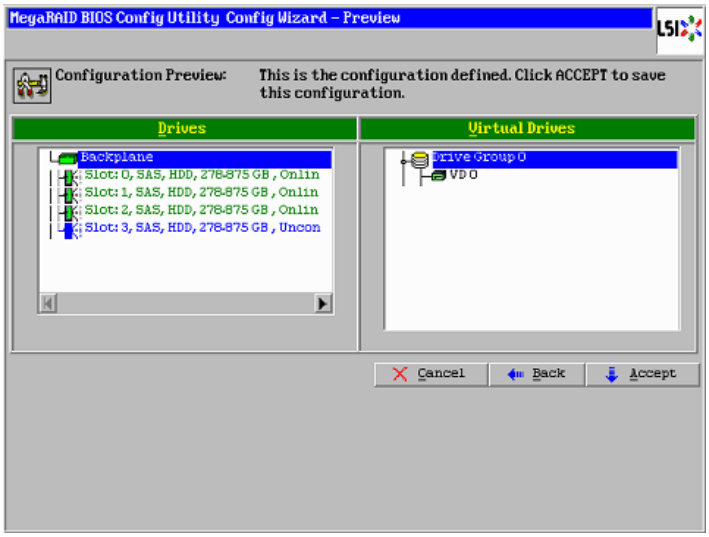


The following screen appears after **Yes** is clicked.



12 Click **Next**.

The following screen appears:



13 Click **Accept**.

The following screen appears:



14 Click **Yes**.

The following screen appears:



15 Click **No**.

The screen returns to the main menu.

16 Initialize the disk array that you have built referring to “Initializing disk arrays”.

Building disk arrays for RAID 10

The following procedure is for building disk arrays for RAID 10.

The following table summarizes the number of hard disks required for building RAID 10.

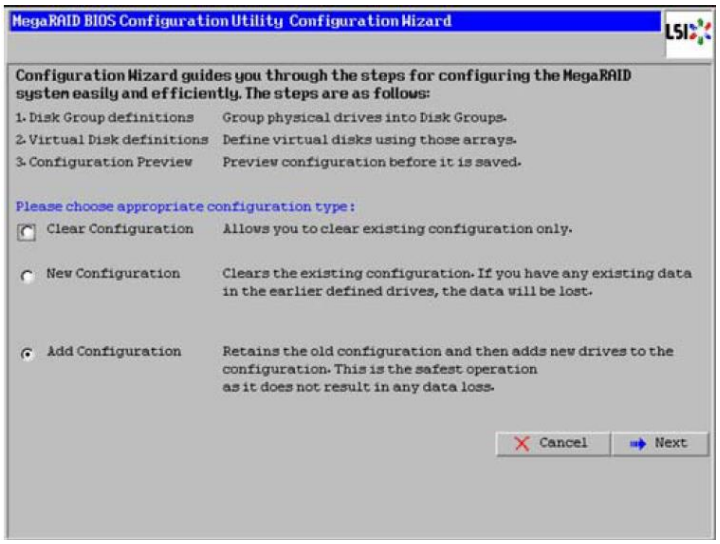
RAID level	Number of hard disks required
RAID 10	4

Tip

See Setting hotspares for how to set hotspare.

1 Select **Configuration Wizard** from the main menu.

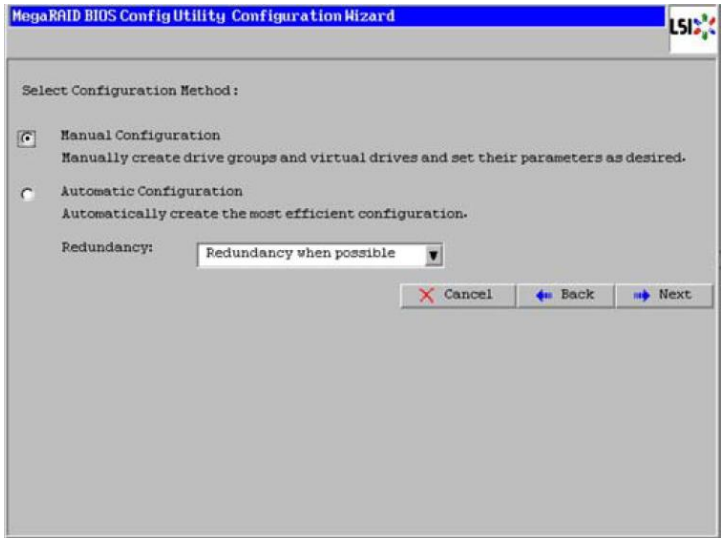
The following screen appears:



NOTICE

If you select **New Configuration**, all data in those hard disks including the disk array information will be lost. Back up your required data before selecting **New Configuration**.

2 Check **New Configuration** or **Add Configuration**, and click **Next**.
The following screen appears:



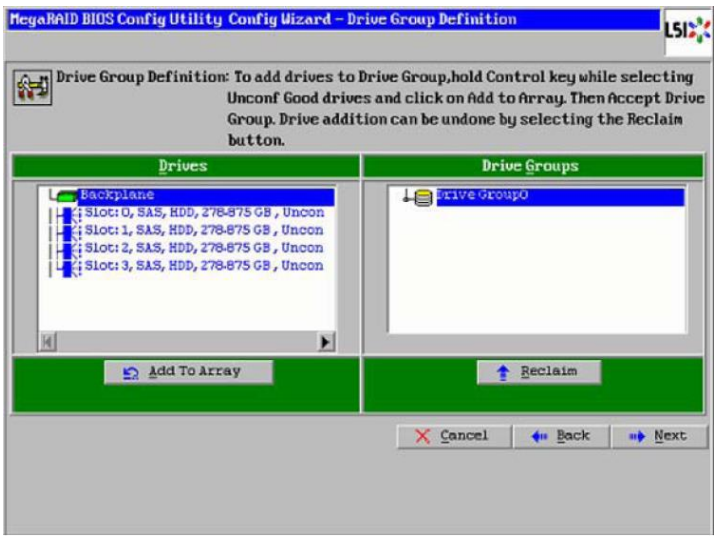
Tip

- Existing drive groups and disk arrays will remain when you select **Add Configuration**. **Add Configuration** should be selected when you want to add disk arrays to an existing drive group, or to build disk arrays using an additional hard disk.
- If you select **New Configuration**, you lose existing drive groups and disk arrays. This should be selected when you discard existing drive groups and disk array to build a new one.
- If you select **New Configuration**, the following screen appears. Clicking **Yes** allows you to build a disk array.



3 Check **Manual Configuration** and click **Next**.

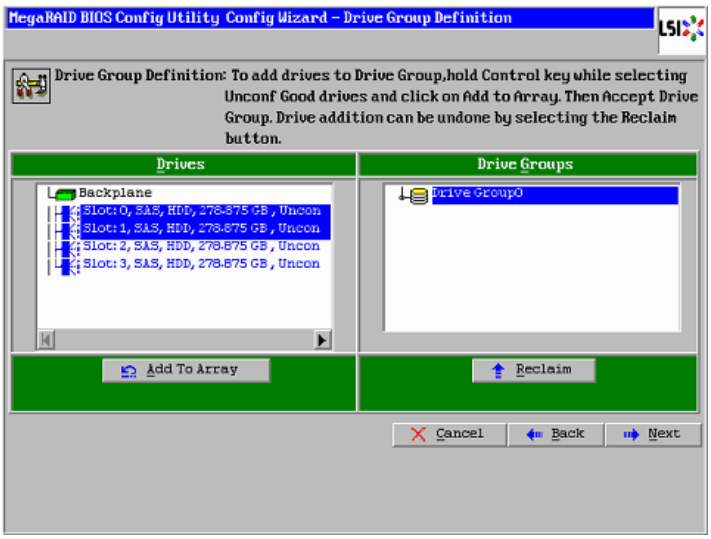
The following screen appears:



4 Select hard disks to use for building a disk array.

When building a disk array with hard disks with **Unconfigured Good** (unused), select two hard disks in the **Drives** pane.

When adding a disk array to an existing drive group, go to step 7 without selecting a hard disk.

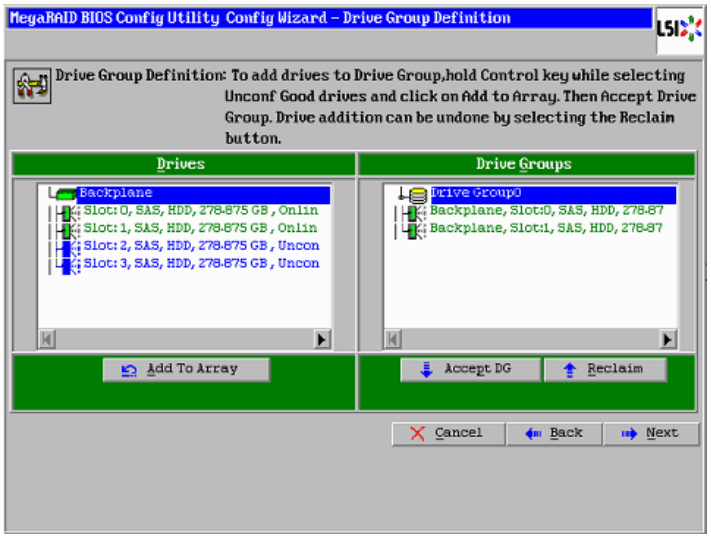


Tip

You can select only a hard disk whose status is **Unconfigured Good** (unused).

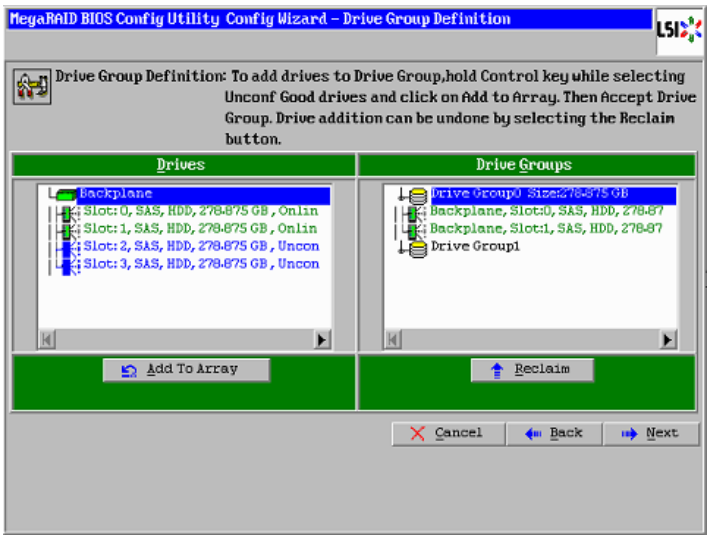
To select multiple hard disks, click them while pressing the **Ctrl** key.

5 After selecting two hard disks for building a disk array, click **Add to Array**.
Status of those selected hard disks is **Online** as shown in the **Drives** pane.



Tip To release a hard disk from **Online**, select the hard disk and click **Reclaim**.

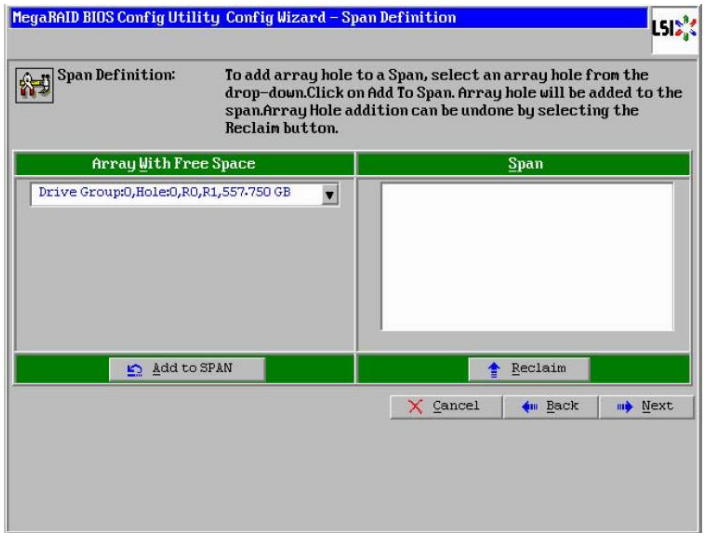
6 Click **Accept DG**.
The following screen appears:



7 When building a disk array with hard disks on status of **Unconfigured Good** (unused), repeat steps 4, 5, and 6 until selecting all hard disks to use for RAID 10, and then click **Next.**

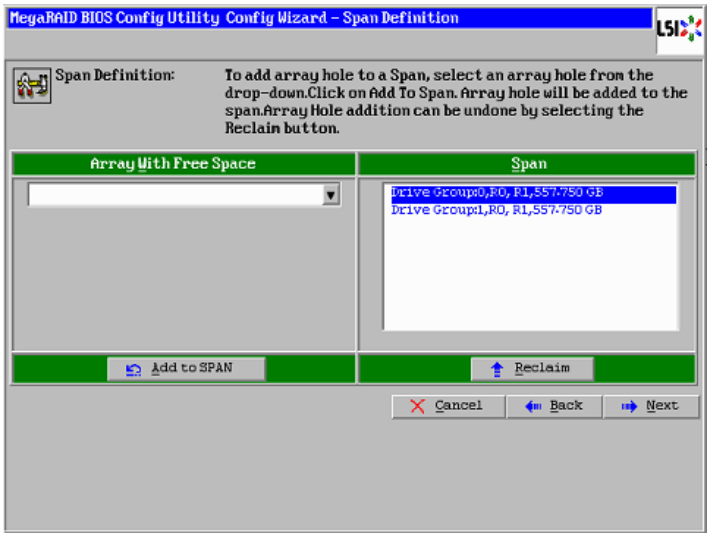
When adding a disk array to the existing drive group, just click **Next**.

The following screen appears:



8 When building a disk array with hard disks on status of “Unconfigured Good” (unused), select the all drive groups added in step 7 by repeating steps 4 through 6 from the **Array With Free Space** menu, and then click **Add to SPAN**.

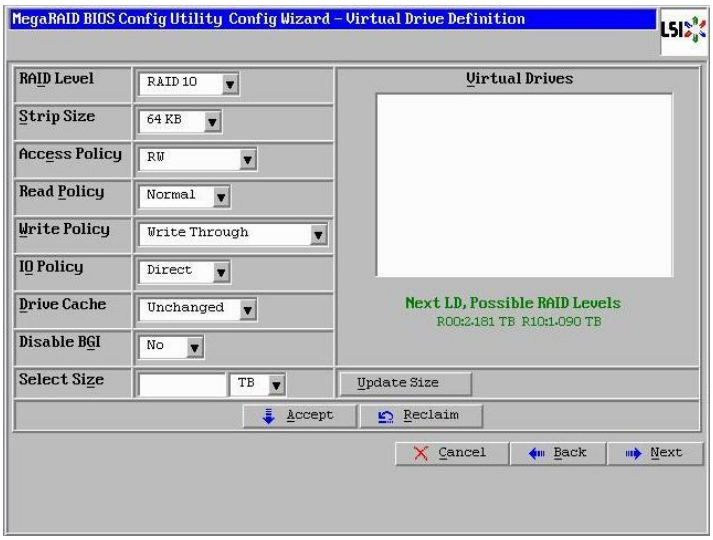
When adding a disk array to an existing drive group, select the target drive group from the **Array With Free Space** pane, and click **Add to SPAN**.



Tip When adding a disk array to existing drive groups, you can select all target drive groups by clicking one of the target drive groups and then **Add to SPAN**.

9 Click **Next**.

The following screen appears:



10 With all the RAID disk array configurations selected, specify RAID level, stripe size, read policy, write policy, and disk array size.

> ***NOTICE***
>
> When enabling the write cache of the disk array with the equipment that has no cache backup module installed, connect the system equipment to UPS. When you use the equipment without connecting to the UPS, data can disappear and be corrupted.

Set each item to the following value.

Item	Content	Setting value **
RAID Level	RAID Level	[RAID 10]
Stripe Size	Stripe size	8 KB / 16 KB / 32 KB / [64 KB] / 128 KB / 256 KB / 512 KB / 1 MB
Access Policy	Access policy	[RW (reading and writing)] / Read Only (reading only) / Blocked (access denied)
Read Policy	Read policy	[Normal (no advanced reading)] / Ahead (always advanced reading)
Write Policy *1 *2	Write policy	Without cache backup module installed * 4: [Write Through (write cache invalid)] / Always Write Back (write-cache valid) / Write Back with BBU (Write cache is valid only when the battery is installed.) With cache backup module installed * 5: Write Through (write-cache invalid)/ Always Write Back (write-cache valid)/[Write Back With BBU (Write cache is valid only when a cache backup module is installed.)]
IO Policy	Read-cache operation	[Direct (reading from the cache at a cache hit)] / Cached (always reading from the cache)

Item	Content	Setting value **
Drive Cache	Setting the hard disk cache	[Disable (setting invalid)] / Enable (setting valid) / No change (depending on the hard disk setting)
Disable BGI	Setting the background initializing	No (background initializing valid) / [Yes (background initializing invalid)]
Select Size *2 *3	Size of a disk array	Enter a value up to the maximum capacity value. The lowest available value is 64 KB..

*1 In Write Policy, **Always Write Back** can be set only when the system equipment without a cache backup module installed is already connected to the UPS (uninterruptible power supply). Even in this case, set **Write Through** when the operating system is installed, otherwise, installation may not be properly completed. Change the setting after installing the OS referring to Changing the write policy for disk arrays. Do not use **Write Back with BBU**.

*2 When the equipment has installed a cache backup module, make sure to set **Write Back With BBU** for Write Policy. If not, write performance may slow down.

*3 The maximum Select Size to be set is shown under **Next LD**, **Possible RAID Levels** on the right pane. Type a value up to the maximum size for the RAID level that you set. Delete a value from the text box before typing another value. When specifying the maximum size, click **Update Size**.

*4 **None** is shown for Battery Backup in Properties: Controller properties submenu 2.

*5 **Present** is shown for Battery Backup in Properties: Controller properties submenu 2.



When a drive group contains multiple disk arrays, specify the same setting values on all disk arrays in the drive group.

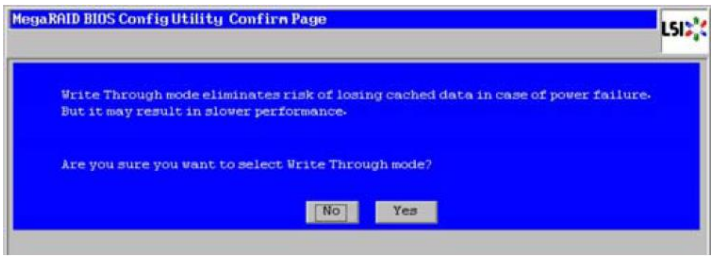


- When you configure a disk array to install an OS and put a value larger than 2 TB, the OS can recognize up to 2 TB.
- If you specify a larger disk array size than the maximum capacity, **Unacceptable size** appears on the screen and all the setting items are initialized. You need to set all items again including the correct size.

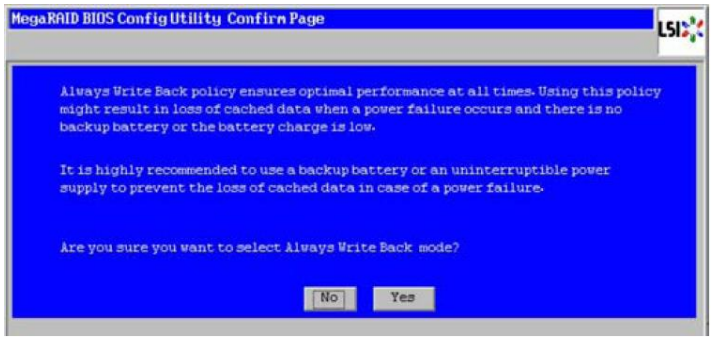
11 Click **Accept**.

One of the following screens appears.

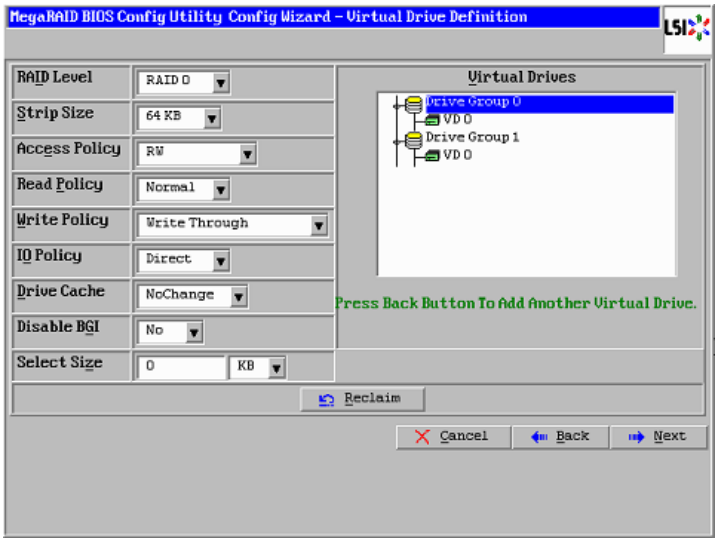
- When selecting **Write Through** in the write policy setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the write policy setting, the following screen appears. Click **Yes**.

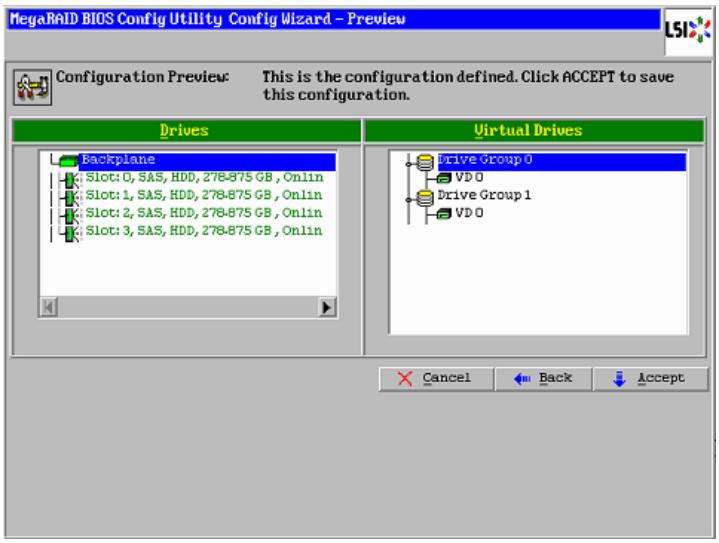


The following screen appears after **Yes** is clicked.



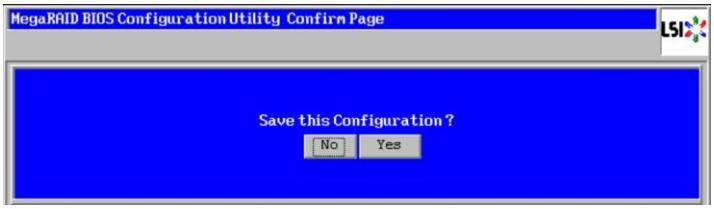
12 Click **Next**.

The following screen appears:



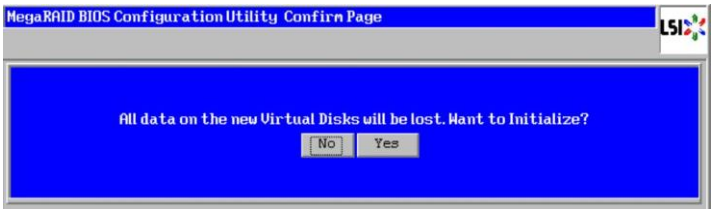
13 Click **Accept**.

The following screen appears:



14 Click **Yes**.

The following screen appears:



15 Click **No**.

The screen returns to the main menu.

16 Initialize the disk array that you have built referring to “Initializing disk arrays”.

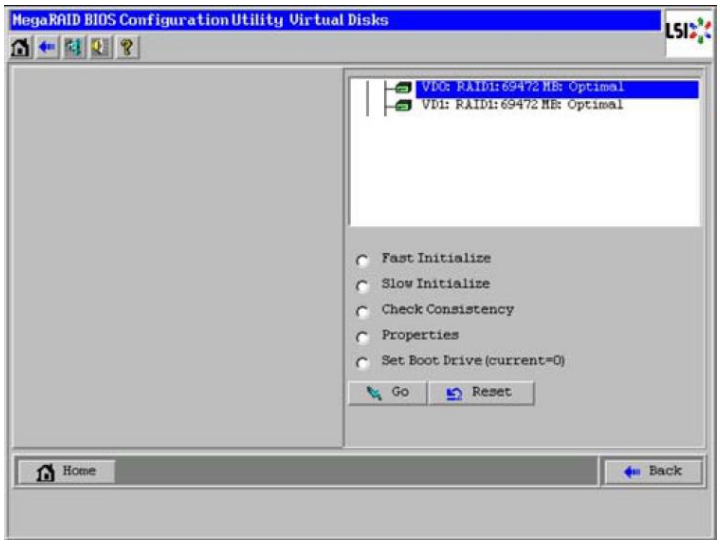
Initializing disk arrays

This section describes the procedure for initializing disk arrays.

> **NOTICE**
>
> When a disk array is initialized, all data in those hard disks including the disk array information will be lost. Back up your required data before initializing a disk array.

1 Select **Virtual Drives** from the main menu.

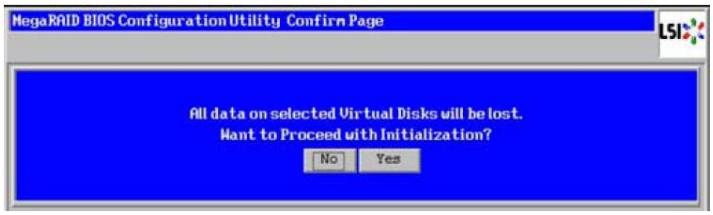
The following screen appears:



2 From the list of disk arrays displayed in the frame at the upper right, select a disk array configuration to initialize.

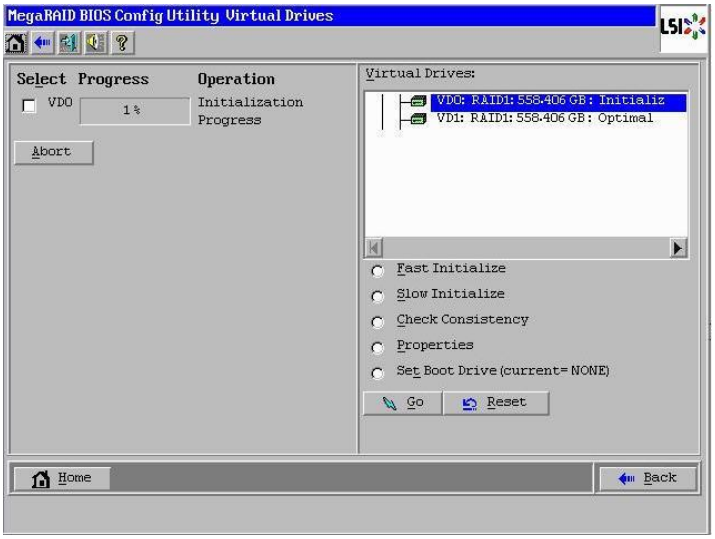
3 Check **Slow Initialize** and click **Go**.

The following screen appears:



4 Click **Yes**.

The progress of initialization is displayed.



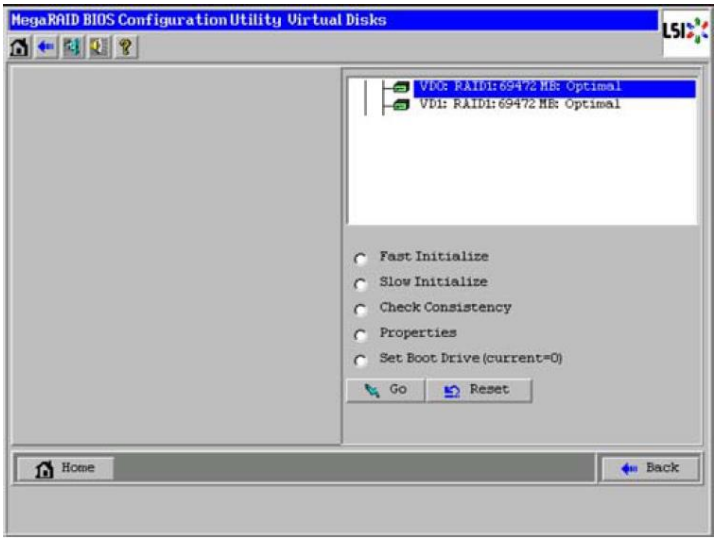
5 Wait until the processing is completed 100%.

A guideline of initialization time is shown in the table below.

Single hard disk capacity	Initialization time
147 GB (SAS HDD)	Approximately 20 minutes
300 GB (SAS HDD)	Approximately 40minutes
600 GB (SAS HDD	Approximately 80 minutes
900 GB (SAS HDD)	Approximately 120 minutes
200 GB (SAS SSD)	Approximately 20 minutes

Tip The initialization time varies depending on the single hard disk capacity regardless of the RAID level or disk array capacity.

6 When initialization is completed 100%, click **Home** to return to the main menu.



Deleting disk arrays

This section describes the procedure for deleting disk arrays.

> ***NOTICE***
>
> When a disk array is deleted, all data in those hard disks including the disk array information will be lost. Back up your required data before deleting a disk array.

Deleting all disk arrays simultaneously

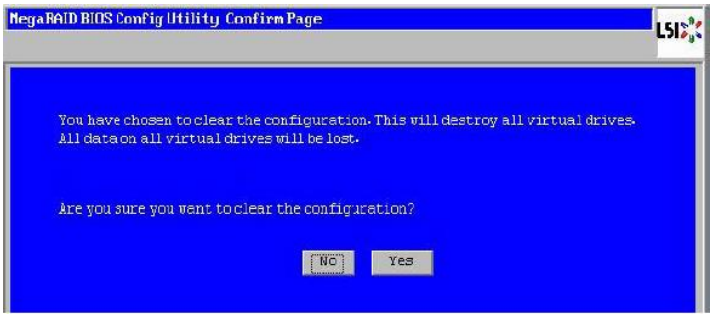
1 Select **Configuration Wizard** from the main menu.

The following screen appears:



2 Check **Clear Configuration** and click **Next.**

The following screen appears:

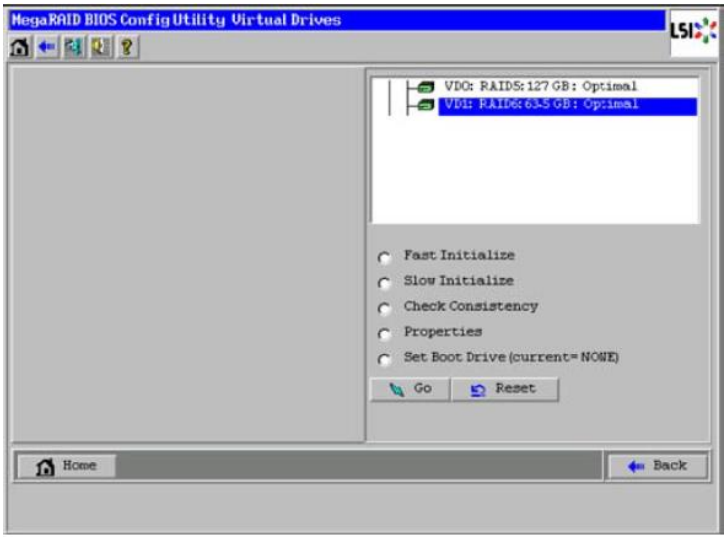


3 Click **Yes**.

Deleting disk arrays selectively

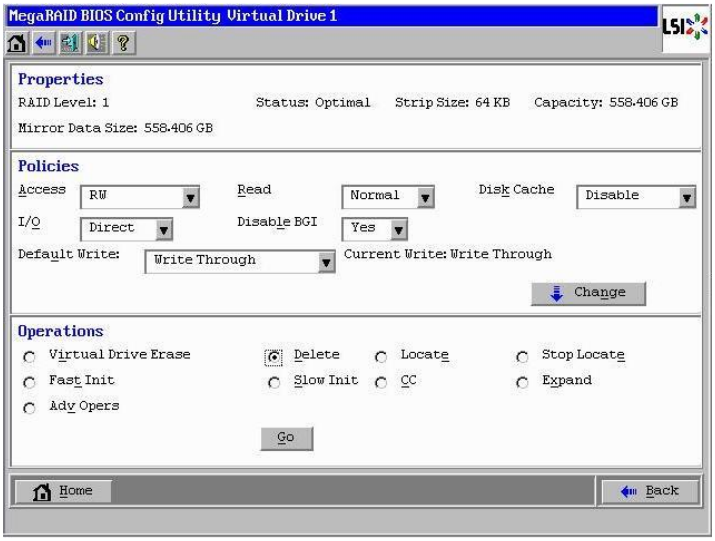
1 Select **Virtual Drives** from the main menu.

The following screen appears:



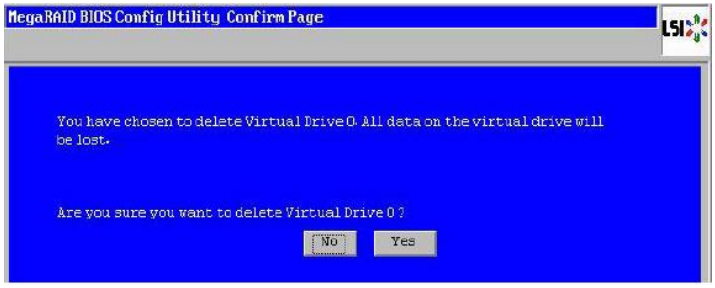
2 From the list displayed at the upper right of the screen, select a disk array that you want to delete. Then check "Properties", and click **Go**.

The following screen appears:



3 Check **Delete** and click **Go**.

The following screen appears:



4 Click **Yes**.

Checking disk arrays for consistency

This section describes how to check the consistency of disk arrays.

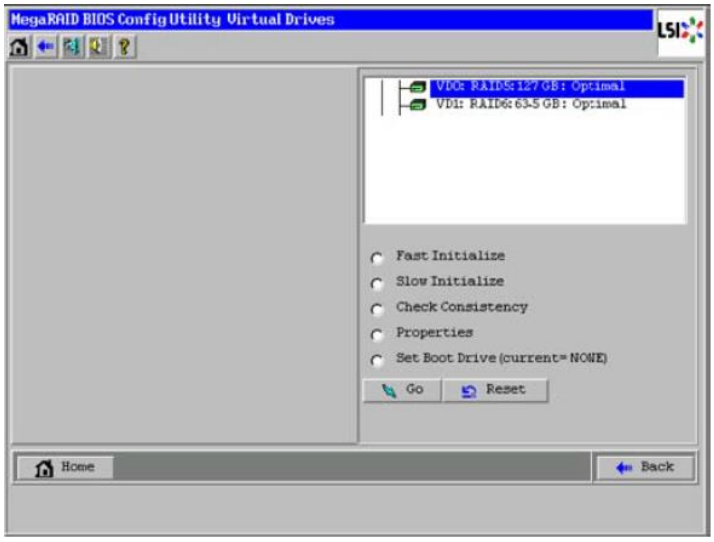
Consistency check can be done from MegaRAID Storage Manager. See the *MegaRAID Storage Manager* in the DriverKit CD-ROM for how to check consistency from the MegaRAID Storage Manager.

Tip

Consistency check on disk arrays can be executed only for RAID 1, 5, 6, and 10.

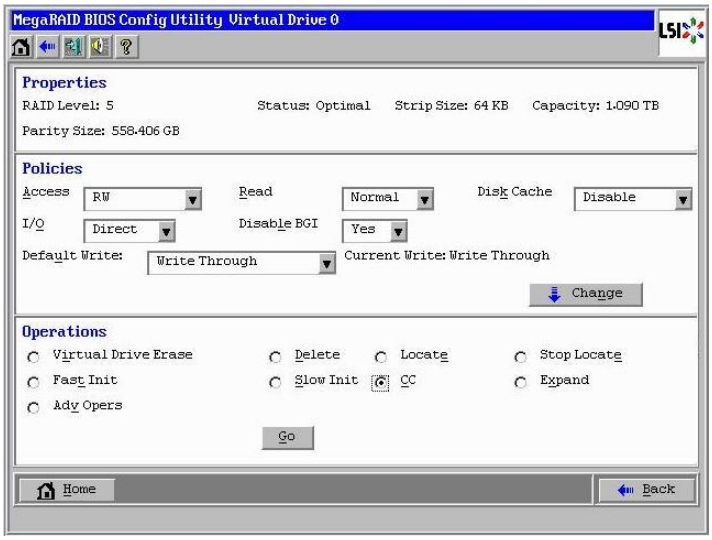
1 Select **Virtual Drives** from the main menu.

The following screen appears:



2 From the list displayed at the upper right of the screen, select a disk array that you want to check the consistency. Check **Properties** and click **Go**.

The following screen appears:



3 Check **CC** and click **Go**.

The progress of consistency check is displayed.



4 Wait until the process is completed 100%.

5 When the consistency check is completed 100%, click **Home** to return to the main menu.

Setting hotspares

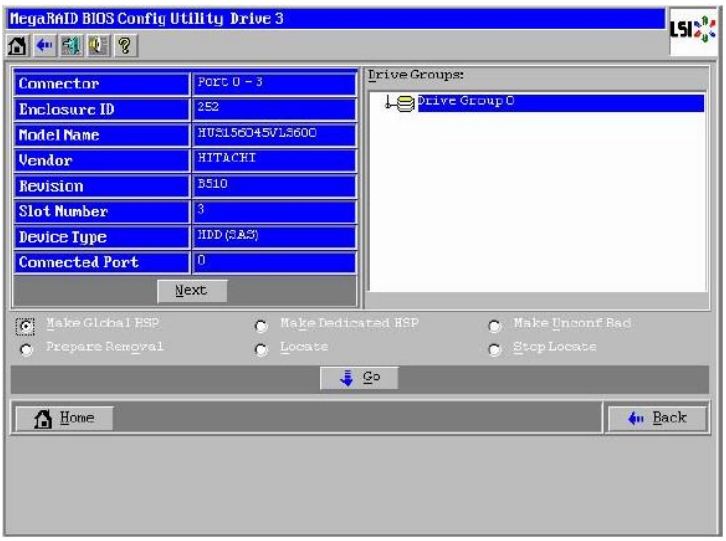
This section describes the procedure for setting hotspares (reserve disks).

Note

- Reserve disk consists of a Global hotspare effective for all logical drives configured and a dedicated hotspare effective for a specified logical drive. Select one for your purpose.
- Be sure to configure redundant disk arrays, RAID 1, 5, 6, or 10 before setting hotspares.
- Install a hard disk in the logical drive consisting of hard disks. Install an SSD in the logical drive consisting of SSDs. You cannot set a disk as a reserve disk different from those configured the logical drive.

1 With the main menu displayed, click a hard disk for hotspare from the hard disk list in the **Logical View / Physical View** pane.

The following screen appears:



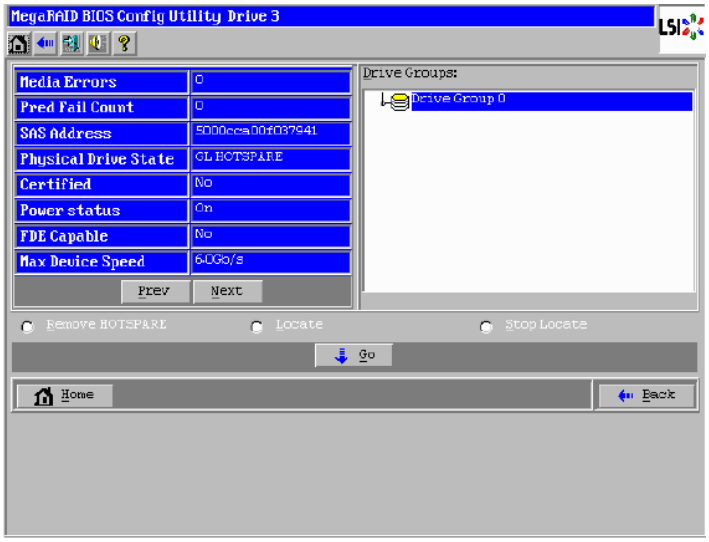
Tip

Only a hard disk whose status is **Unconfigured Good** (unused) can be selected.

2 To set the disk to Global hotspare, check **Make Global HSP**.
To set the disk to Dedicated hotspare, select a logical drive group from the right pane for hotspare and then check **Make Global HSP**.

3 Click **Go**.

Hotspare is set to the specified hard disk.



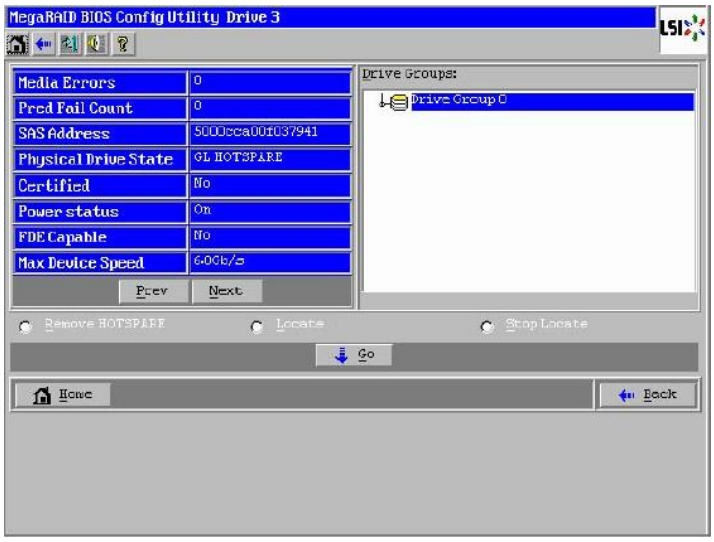
Canceling hotspares

This section describes the procedure for canceling hotspares.

1 When the main menu is displayed, click a hard disk that is set in hotspare from the list in **Logical View/Physical View**.

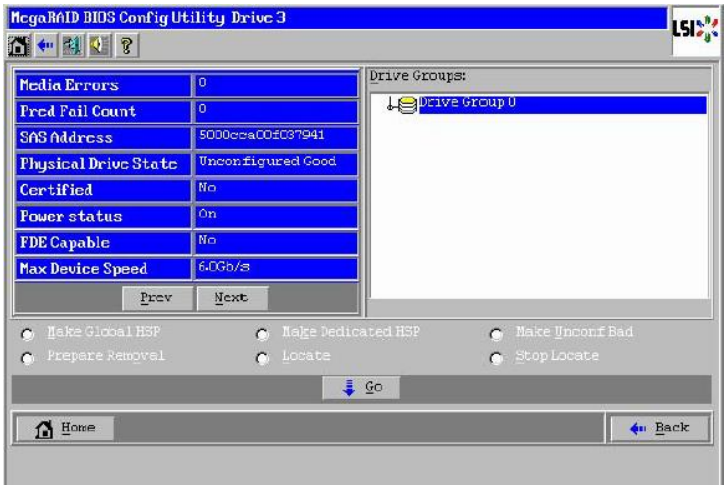
Select a hard disk with hotspare status.

The following screen appears:



2 Check **Remove HOTSPARE** and click **Go**.

Hotspare is released.



Rebuilding disk arrays

The following procedure is for rebuilding disk arrays when a problem occurs on a hard disk in a redundant disk array configuration (RAID 1, 5, 6,10).

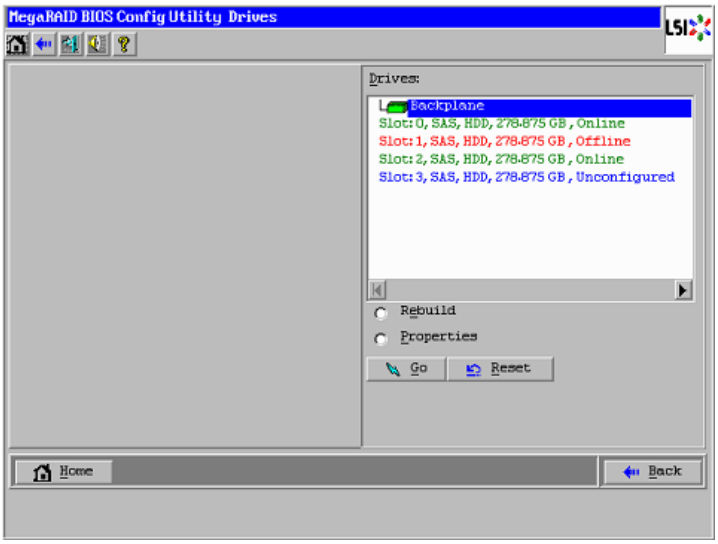


- For RAID 6, the disk array can be restored even if two hard disks fail.
- With hotspares configuration, rebuilding will work automatically when a hard disk problem occurs. Without hotspare configuration, rebuilding will work automatically after you replace the faulty hard disk in hot-plug.

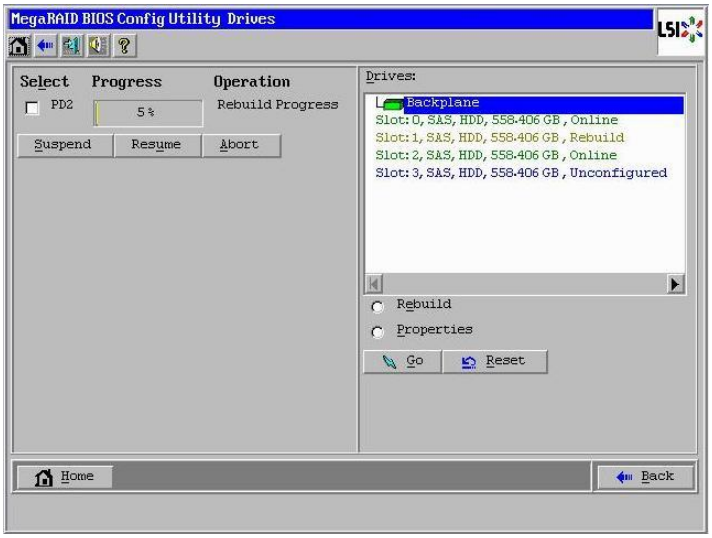
The following is a procedure for manually rebuilding where an automatic rebuild did not work.

1 Select **Drives** from the main menu.

The following screen appears:



2 Select a hard disk with the **Offline** status, check **Rebuild**, and click **Go**.
The rebuilding progress is displayed.



3 Wait until the processing is completed 100%.
A guideline for rebuilding time is shown in the table below.

RAID level	Capacity of a disk array	Rebuilding time
RAID 1	300 GB (SAS: 300 GB HDD x 2)	Approximately 40 minutes
	200 GB (SAS: 200 GB SSD x 2)	Approximately 10 minutes
RAID 5	600 GB (SAS: 300 GB HDD x 3)	Approximately 40 minutes
	400 GB (SAS: 200 GB SSD x 3)	Approximately 10 minutes
RAID 6	600 GB (SAS: 300 GB HDD x 4)	Approximately 40 minutes
	400 GB (SAS: 200 GB SSD x 4)	Approximately 10 minutes
RAID 10	600 GB (SAS: 300 GB HDD x 4)	Approximately 40 minutes
	400 GB (SAS: 200 GB SSD x 4)	Approximately 10 minutes

Tip The rebuilding time is proportional to the capacity of a disk array.

4 When rebuilding is completed 100%, click **Home** to return to the main menu.

Expanding disk array capacity

This section describes how to expand a disk array in a RAID 0, 5, or 6 disk array by adding hard disks to use.

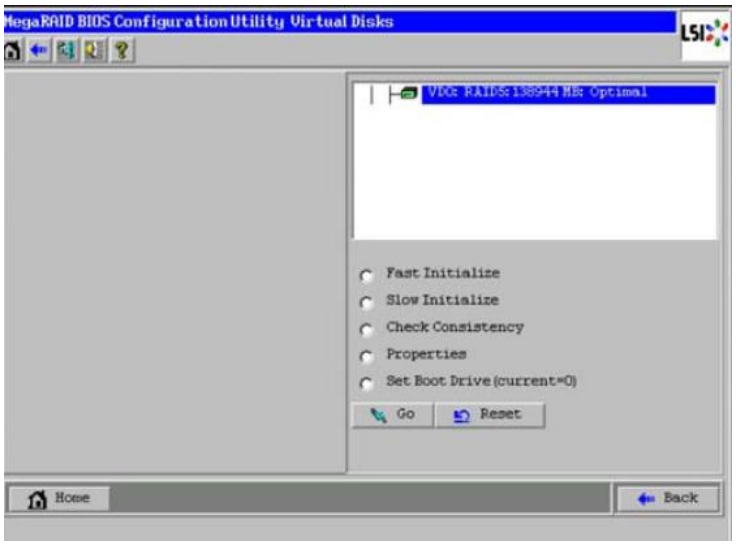
Disk array expansion can also be done from MegaRAID Storage Manager. See *MegaRAID Storage Manager* in the DriverKit CD-ROM for information about how to expand disk arrays from the MegaRAID Storage Manager.



- A disk array expansion cannot be cancelled during the execution.
- Be sure to install a hard disk with **Unconfigured Good** status (unused) before expanding the capacity.

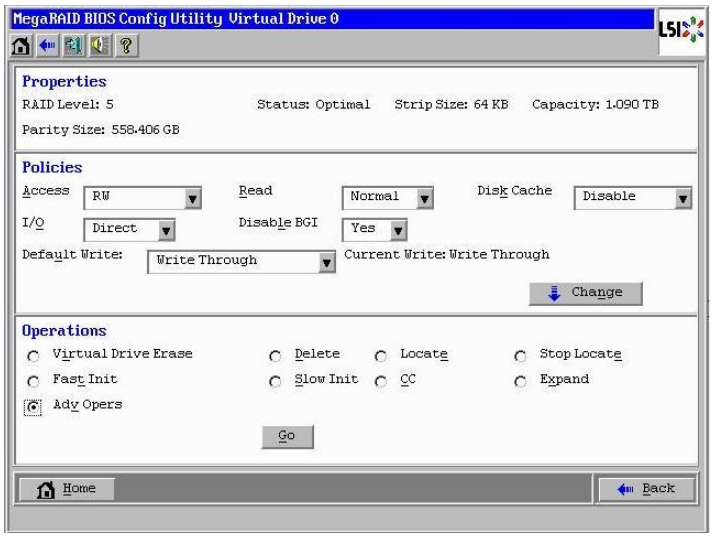
1 Select **Virtual Drives** in the main menu.

The following screen appears:



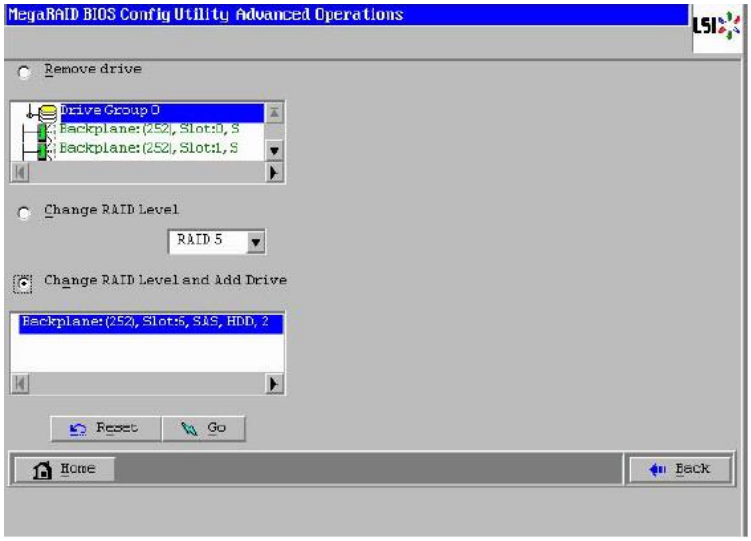
2 Select a disk array to expand the capacity from the list displayed on the upper right of the screen. Check **Properties** and click **Go**.

The following screen appears:



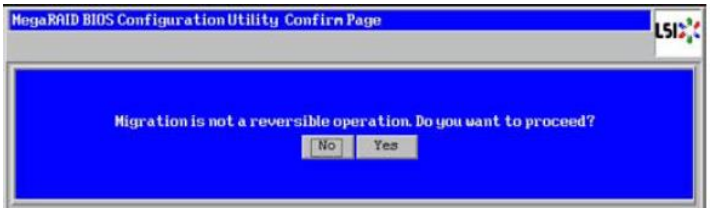
3 Check **Adv Opers** and click **Go**.

The following screen appears:



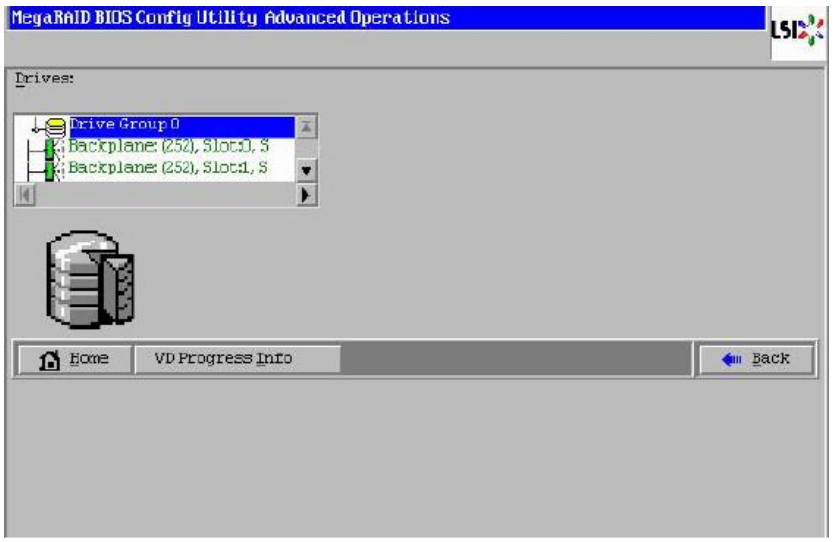
4 Check **Change RAID Level and Add Drive**, select a hard disk to use for the capacity expansion from the list displayed in the pane, and click **Go**.

Tip To select multiple hard disks, click hard disks while pressing the **Ctrl** key.



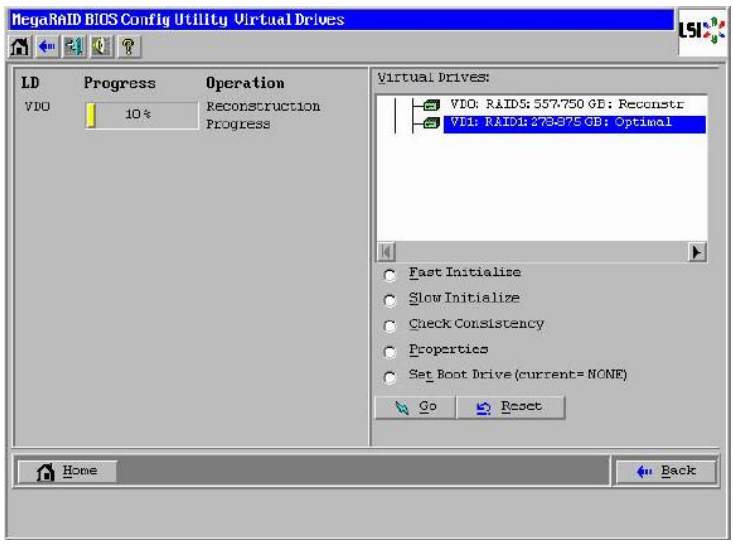
5 Click **Yes**.

The following screen appears:



6 Click **VD Progress Info** shown in the screen above.

The progress of the capacity expansion is displayed.



7 Wait until the expansion is completed 100%.

A guideline for expansion time is shown in the table below.

RAID level	Capacity of a disk array	Rebuilding time for expansion
RAID 0	900 GB (SAS: 300 GB HDD x 3)	Approximately 210 minutes
	600 GB (SAS: 200 GB SSD x 3)	Approximately 70 minutes
RAID 5	600 GB (SAS: 300 GB HDD x 3)	Approximately 160 minutes
	400 GB (SAS: 200 GB SSD x 3)	Approximately 60 minutes
RAID 6	600 GB (SAS: 300 GB HDD x 4)	Approximately 170 minutes
	400 GB (SAS: 200 GB SSD x 4)"	Approximately 60 minutes



The rebuilding time for expansion is proportional to the capacity of a disk array regardless of the number of hard disks to add.

8 When expansion is completed 100%, click **Home** to return to the main menu.

❑ Changing the write policy for disk arrays

This section describes the procedure for changing the write policies.

Enabling Write Cache of a disk array can improve the write performance.

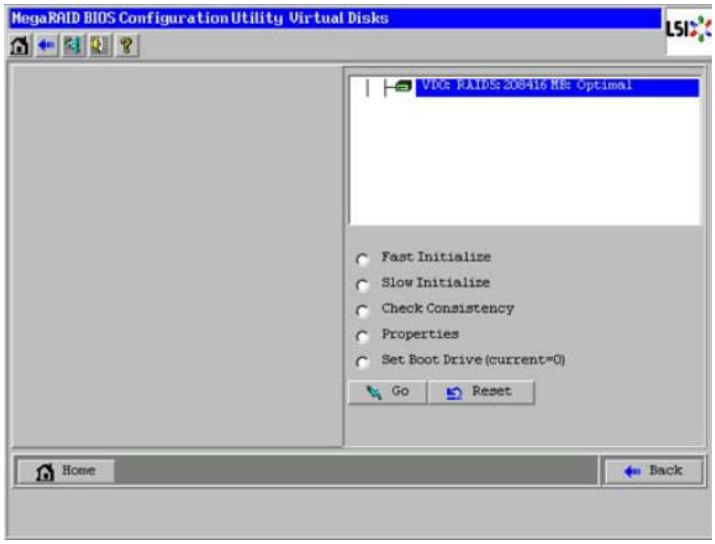
> ***NOTICE***
>
> When enabling the disk array "write cache" with the equipment that has no cache backup module installed, connect the system equipment to UPS. Otherwise, data in the write cache may disappear or be destroyed during a blackout or instant power failure.

Note

- In Write Policy for the equipment that has no cache backup module installed, **Always Write Back** can be supported only when the system equipment is connected to the UPS (uninterruptible power supply).
  Even in this case, set to **Write Through** when installing the operating system. Otherwise, installation may not be properly completed.
- When the equipment has a cache backup module installed, make sure to set **Write Back With BBU** for Write Policy. If not, write performance may slow down.

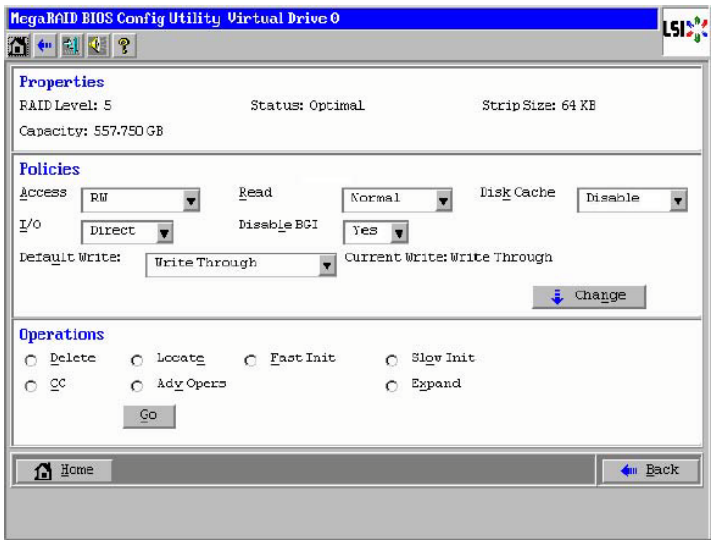
1 Select **Virtual Drives** in the main menu.

The following screen appears:



2 From the list displayed at the upper right of the screen, select a disk array for which you want to change the write policy. Check **Properties** and click **Go**.

The following screen appears:



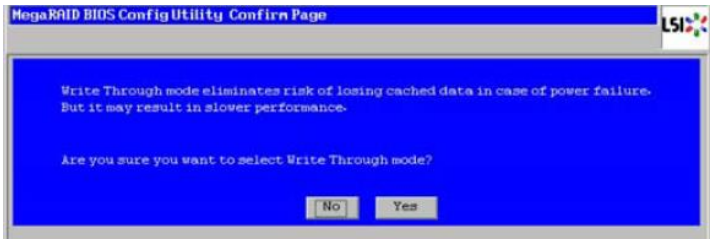
3 Select the write policy from **Default Write** in the **Policies** pane, and click **Change**.

Setting value	Description
Always Write Back	Write cache is valid.
Write Through	Write cache is invalid.
Write Back with BBU	Write cache is valid only when a cache backup module is installed.

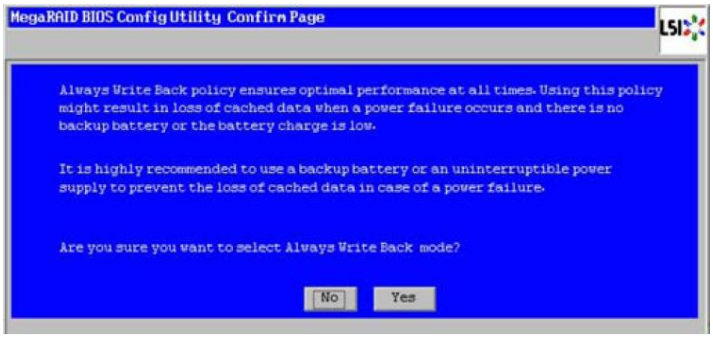
Note

- In Write Policy for the equipment that has no cache backup module installed, operation with **Always Write Back** can be supported only when the system equipment is connected to the UPS (uninterruptible power supply). Even in this case, set **Write Through** when installing OS. Otherwise, installation may not be properly completed.
- When the equipment has a cache backup module installed, Make sure to set **Write Back With BBU** for Write Policy. If not, write performance may slow down.

- When selecting **Write Through** in the Default write setting, the following screen appears. Click **Yes**.



- When selecting **Always Write Back** in the Default write setting, the following screen appears. Click **Yes**.



4 Click **Home** to return to the main menu.

Tip

Set the write policy per disk array. When building multiple disk arrays, set the write policy to all disk arrays.

❑ BIOS settings for SAS internal RAID controller

When using the boot from an external storage on the system equipment with the SAS RAID controller: MegaRAID SAS 2208, change the BIOS setting: Controller BIOS setting to Disabled.

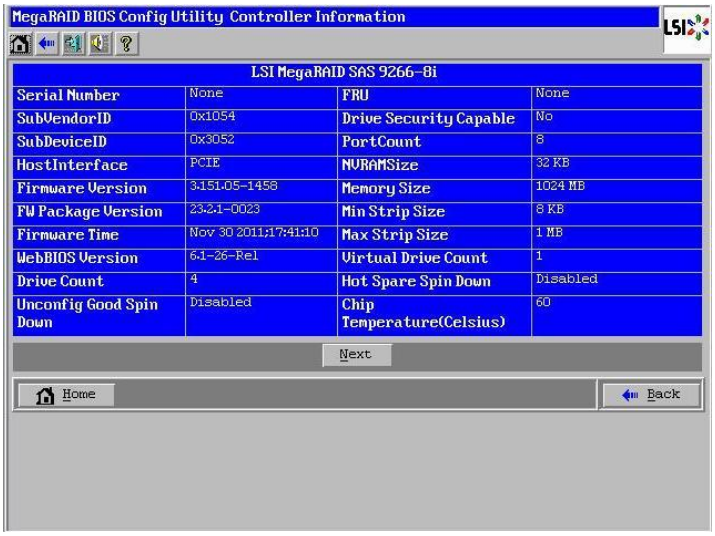
This section describes the procedure for changing the BIOS setting of the SAS RAID controller: MegaRAID SAS 2208.

Tip

When changing the BIOS setting: Controller BIOS setting is changed to Disabled, you cannot execute the boot from the disk array configured in the SAS RAID Controller: MegaRAID SAS 2208.

1 Select **Controller Properties** from the main menu.

The following screen appears:



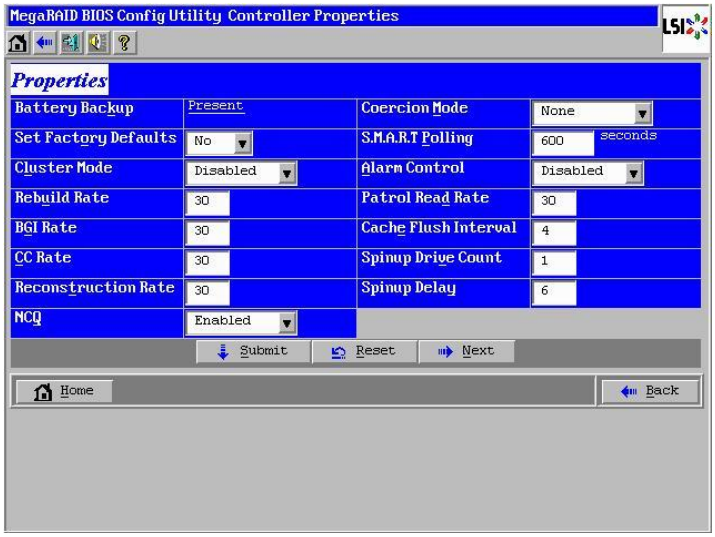
2 Click **Next**.

The following screen appears:



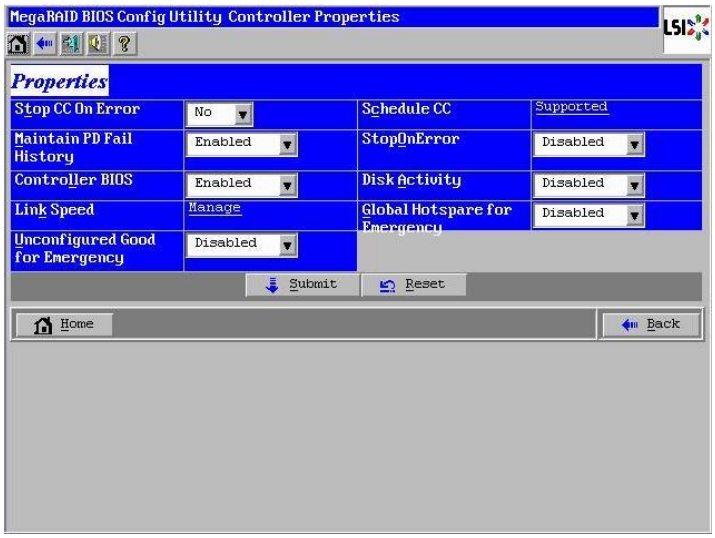
3 Click **Next**.

The following screen appears:



4 Click **Next** once more.

The following screen appears:



5 Select one of the setting values in the table below from **Controller BIOS**, and then click **Submit**.

Setting value	Description
Enabled	Enables BIOS of the SAS RAID controller: MegaRAID SAS 2208. Enables the boot from the disk array.
Disabled	Disables BIOS of the SAS RAID controller: MegaRAID SAS 2208. Disables the boot from the disk array.

Tip Make sure to click **Submit** after changing the setting.

5 Confirm that **Controller BIOS** is set to that value.

6 Click **Home** to return to the main menu.

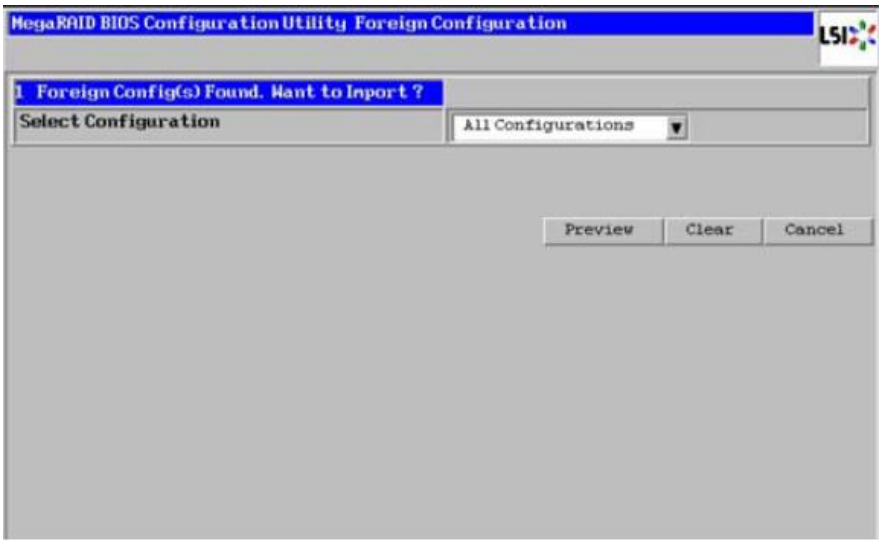
❑ Disk with foreign configuration

This section describes how to deal with a hard disk with a different configuration detected from the disk array controller board configuration.

A difference in configuration between disks may be caused by the following conditions.

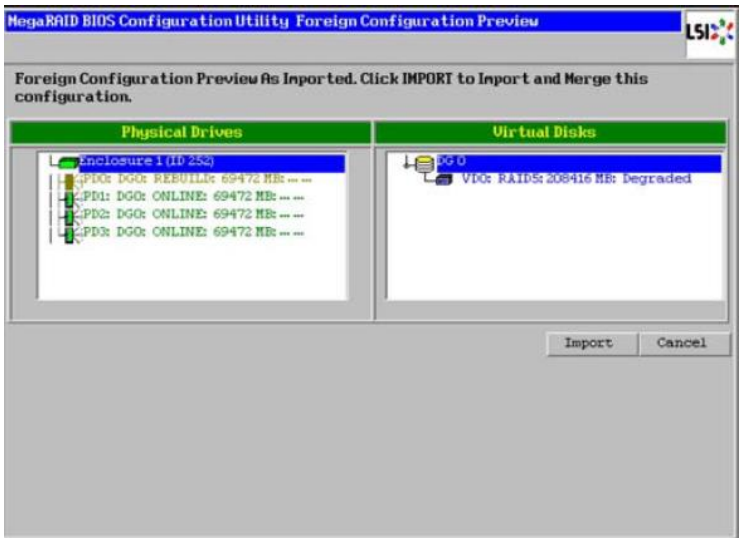
Conditions to generate foreign configuration
A disk failed and could not be recognized. Then the disk has been restored to be recognized.
A disk that had been used in another system unit with a foreign configuration contained was used.

1 Click **Preview**.



2 If the displayed configuration is correct, click **Import**.

If the displayed configuration is incorrect, click **Cancel**. When the screen returns to Step 1, click **Clear**.



Tip When you click **Clear**, a message “Previous foreign configuration will be lost. Do you want to proceed?” is displayed. Click **Yes**, and the previous foreign configuration will be eliminated.

❑ Status

Status of the disk array

The following table lists the status for disk arrays.

Status indication	Description
Optimal	Normal. The disk array is perfect in function.
Partially Degraded	One hard disk fails in the RAID 6 disk array.
Degraded	One hard disk fails in the RAID 1, 5, or 10 disk array. Or two hard disks fail in the RAID 6 disk array.
Offline	The disk array is inoperable because of either failures in multiple hard disks in a redundant disk array or a failure in a hard disk in a non-redundant disk array.

Status of the hard disk

The following table lists the status for hard disks.

Status indication	Description
Online	Normal.
Offline/Failed	A fault has occurred. The hard disk is separated from the disk array due to failure.
Rebuild	Rebuilding is underway.
Global Hot Spare	This is set as a global hotspare.
Dedicated Hot Spare	This is a dedicated hot spare.
Unconfigured GOOD	This is not used for a disk array.
Unconfigured BAD	A fault has occurred. The unrecognizable hard disk is restored to recognizable.
Missing	A fault has occurred. A "normal" hard disk has been removed.

❑ BIOS messages

The following table lists the messages for MegaRAID WebBIOS displayed at system startup.

	Message	Description
1	Cache data was lost because of an unexpected power-off or reboot during a write operation, but the adapter has recovered. This could be because of memory problems, bad battery, or you may not have a battery installed. Press any key to continue or press C to load the configuration utility.	If these messages are displayed even though an incorrect power-off or reboot has not been executed during write operation, contact your reseller or call maintenance personnel.
2	The memory/battery problems were detected. The adapter was recovered, but cached data was lost. Press any key to continue or press C to load the configuration utility.	
3	Cache data was lost, but the controller has recovered. This could be due to the fact that your controller had protected cache after an unexpected power loss and your system was without power longer than the battery backup time. Press any key to continue or press C to load the configuration utility.	
4	The cache contains dirty data, but some VDs are missing. The cached data cannot be written to the disk. If this is an unexpected error, then power off your system and check your cables to ensure all disks are present. If you continue, the data in the cache will be permanently discarded. Press X to acknowledge and permanently destroy the cached data.	
5	Foreign configurations found on adapter. Press any key to continue or press C to load the configuration utility.	A hard disk with a different configuration from the disk array configuration in the disk array controller was detected. See Disk with foreign configuration.
6	FW package	This shows the firmware package version. You do not need to take any action.
7	The battery hardware is missing or malfunctioning, the battery is unplugged, or the battery could be fully discharged. If you continue to boot the system, the battery-backed cache will not function. If the battery is connected and has been allowed to charge for 30 minutes and if this message continues to appear, contact technical support for assistance. Press D to disable this warning (if your controller does not have a battery).	Cache backup module information is not set correctly. Press the **D** key while this message is displayed. If this key operation does not recover the situation, contact your reseller or call maintenance personnel.
8	The battery hardware is missing or malfunctioning, the battery is unplugged, or the battery could be fully discharged. If you continue to boot the system, the battery-backed cache will not function. If the battery is connected and has been allowed to charge for 30 minutes, and if this message continues to appear, contact technical support for assistance.	

	Message	Description
9	Some configured disks have been removed from your system, or are no longer accessible. Check your cables and also ensure all disks are present. Press any key to continue or press C to load the configuration utility.	Some hard disks with the disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
10	The following VDs have missing disks: - If you proceed (or load the configuration utility), these VDs will be marked OFFLINE and will be inaccessible. - Check your cables and ensure all disks are present. Press any key to continue or press C to load the configuration utility.	Since some hard disks have been removed, the disk array is set in OFFLINE. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
11	A discovery error has occurred. Power-cycle the system and all the enclosures attached to this system.	A disk array controller or hard disk has not been recognized correctly. When this message is displayed, contact your reseller or call maintenance personnel.
12	The following VDs are missing: If you proceed (or load the configuration utility), these VDs will be removed from your configuration. If you wish to use them at a later time, they will have to be imported. If you decide these VDs should be present, power off your system and check your cables to ensure all disks are present. Press any key to continue or press C to load the configuration utility.	Some disk array configurations are removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
13	The following VDs are missing complete spans. If you proceed (or load the configuration utility), these VDs will be removed from your configuration and the remaining drives marked as foreign. If you wish to use them at a later time, restore the missing spans and use foreign import to recover the VDs. If you believe these VDs should be present, please power off your system and check your cables to ensure all disks are present. Press any key to continue, or 'C' to load the configuration utility.	
14	All of the disks from your previous configuration are gone. If this is an unexpected message, then power off your system and check your cables to ensure all disks are present. Press any key to continue or press C to load the configuration utility.	All hard disks with disk array configuration information have been removed. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.
15	Your battery is either charging, bad, or missing, and you have VDs configured for write-back mode. Because the battery is not currently usable, these VDs will actually run in the write-through mode until the battery is fully charged or replaced if it is bad or missing. Press any key to continue.	Cache backup module information is not correct. When this message is displayed even if the device is installed properly, contact your reseller or call maintenance personnel.

	Message	Description
16	Multibit Error Check and Correct (ECC) errors were detected on the RAID controller. The DIMM on the controller needs replacement. Contact technical support to resolve this issue. If you continue, data corruption can occur. Press X to continue, or power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, press X to continue.	Errors have occurred in the cache memory of the disk array controller. When this message is displayed, contact your reseller or call maintenance personnel.
17	Single-bit ECC errors were detected during the previous boot of the RAID controller. The DIMM on the controller needs replacement. Contact technical support to resolve this issue. Press X to continue, or power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, press X to continue.	
18	Single-bit overflow ECC errors were detected during the previous boot of the RAID controller. The DIMM on the controller needs replacement. Contact technical support to resolve this issue. If you continue, data corruption can occur. Press X to continue, or power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, press X to continue	
19	Single-bit overflow ECC errors were detected during the previous boot of the controller. The DIMM on the controller needs replacement. If you continue, data corruption can occur. Press X to continue, or power off the system and replace the DIMM module and reboot. If you have replaced the DIMM, press X to continue	
20	Multibit ECC errors were detected on the RAID controller. If you continue, data corruption can occur. Contact technical support to resolve this issue. Press X to continue, or power off the system, replace the controller and reboot.	
21	Multiple Single-bit ECC errors were detected during the previous boot of the controller. The DIMM on the controller needs replacement. If you continue, data corruption can occur. Press X to continue or power off the system, replace the DIMM module, and reboot. If you have replaced the DIMM, press X to continue.	
22	Single-bit overflow ECC errors were detected on the RAID controller. If you continue, data corruption can occur. Contact technical support to resolve this issue. Press X to continue or power off the system, replace the controller and reboot.	
23	Memory Error. Please check the SDRAM connection. If problems persist contact Technical Support.	An error occurred on the disk array controller memory. When this message is displayed, contact your reseller or call maintenance personnel.
24	Memory Error. Detected Unsupported RAID Controller Memory. Contact Technical support.	
25	Unrecoverable Error. Please check the SDRAM connection. If problems persist contact Technical Support.	

	Message	Description
26	This is a TEST message. Press any key to ignore it, or wait 5 seconds. No further action is required. Press any key to continue, or press C to load the configuration utility.	When this message is displayed, contact your reseller or call maintenance personnel.
27	This firmware is an ALPHA version. It has not completed all validation.	When this message is displayed, contact your reseller or call maintenance personnel.
28	This firmware is a BETA version. It has not completed all validation.	When this message is displayed, contact your reseller or call maintenance personnel.
29	This firmware is a TEST version. It has not completed any validation.	When this message is displayed, contact your reseller or call maintenance personnel.
30	The firmware version inconsistency was detected. The adapter was recovered, but cached data was lost. Press any key to continue or press C to load the configuration utility.	When this message is displayed, contact your reseller or call maintenance personnel.
31	Firmware Failed Validation. Adapter needs to be reflashed.	
32	The most recent configuration command could not be committed and must be retried. Press any key to continue, or press C to load the configuration utility.	Disk array configuration information was cleared or not found. When this message is displayed, contact your reseller or call maintenance personnel.
33	Previous configuration cleared or missing. Importing configuration created on X/Y X:Y. Press any key to continue or press C to load the configuration utility.	
34	An enclosure was found that contains both SAS and SATA drives, but this controller does not allow mixed drive types in a single enclosure. Correct the problem and restart your system. Press any key to continue or press C to load the configuration utility.	The disk array controller is operated by incorrect parameters. When this message is displayed, contact your reseller or call maintenance personnel.
35	SAS drives were detected, but this controller does not support SAS drives. Remove the SAS drives and restart your system. Press any key to continue or press C to load the configuration utility.	
36	SATA drives were detected, but this controller does not support SATA drives. Remove the SATA drives, and restart your system. Press any key to continue or press C to load the configuration utility.	
37	Raid Key Missing. Please check the Raid Key connection. If problems persist contact Technical Support.	
38	Raid Key Authentication Error. Please check the RAID Key installed for this solution. If problems persist contact Technical Support.	
39	Raid Key OEM Authentication Error. Install the correct RAID key for this System. If problems persist, contact Technical Support.	
40	There are more enclosures connected to the port than what is allowed for a single SAS port. Remove the extra enclosures, and then restart your system.	Incorrect enclosures are detected. When this message is displayed, contact your reseller or call maintenance personnel.

	Message	Description
41	Invalid SAS topology detected. Check your cable configurations, repair the problem, and restart your system.	When this message is displayed, contact your reseller or call maintenance personnel.
42	Invalid SAS Address present in SBR. Contact your system support. Press any key to continue with the default SAS address.	When this message is displayed, contact your reseller or call maintenance personnel.
43	Invalid SAS Address present in MFC data. Program the valid SAS Address, and restart your system.	
44	Invalid memory configuration detected. Contact your system support. System has halted.	When this message is displayed, contact your reseller or call maintenance personnel.
45	Entering the configuration utility in this state will result in drive configuration changes. Press Y to continue loading the configuration utility or power off your system and check your cables to ensure that all the disks are present, and then restart.	Hard disk configuration information has been changed. When this message is displayed, contact your reseller or call maintenance personnel.
46	External Enclosure does not support in controller's Direct mapping mode. Contact your system support. System has halted due to unsupported configuration.	Incorrect information was detected from the enclosure. When this message is displayed, contact your reseller or call maintenance personnel.
47	Expander Detected in controller with Direct mapping mode. Reconfiguring automatically to persistent mapping mode. Automatic reboot would happen in 10 seconds.	An unsupported device (expander) is detected. When this message is displayed, contact your reseller or call maintenance personnel.
48	The controller's I/O processor has a fault that can potentially cause data corruption. Your controller needs replacement. Contact your system support. Press Y to acknowledge.	The processor of the controller is faulty. When this message is displayed, contact your reseller or call maintenance personnel.
49	Number of disks exceeded the maximum supported count of X disks. Remove the extra drives and reboot the system to avoid losing data Press Y to continue with extra drives.	Improper hard disks are detected. When this message is displayed, contact your reseller or call maintenance personnel.
50	Number of devices exceeded the maximum limit of devices per quad. Remove the extra drives and reboot the system to avoid losing data. System has halted due to unsupported configuration.	
51	Drive security is enabled on this controller and a pass phrase is required. Please enter the pass phrase.	Hard disk security functions are not supported. When this message is displayed, contact your reseller or call maintenance personnel.
52	Invalid pass phrase. Please enter the pass phrase.	
53	There was a drive security key error. All secure drives will be marked as foreign. Press any key to continue, or C to load the configuration utility.	
54	Invalid pass phrase. If you continue, there will be a drive security key error and all secure configurations will be marked as foreign. Reboot the machine to retry the pass phrase or press any key to continue.	

	Message	Description
55	Unable to communicate to EKMS. If you continue, there will be a drive security key error and all secure configurations will be marked as foreign. Please check connection with the EKMS, reboot the machine to retry the EKMS or press any key to continue.	
56	Unable to change security to EKMS as not able to communicate to EKMS. If you continue, the drive security will remain to existing security mode. Please check connection with the EKMS, reboot the machine to retry the EKMS or press any key to continue	
57	DKM existing key request failed; existing secure configurations will be labeled foreign and will not be accessible. Reboot server to retry.	
58	DKM new key request failed; controller security mode transition was not successful. Reboot server to retry request, or press any key to continue.	
59	The native configuration is no longer supported by the current controller settings. Please ensure that correct controller, iButton or key vault is being used. If you continue, the configuration will be marked foreign and part of it may be imported if possible. Press any key to continue.	The native configuration is not supported by the current disk array controller settings. When this message is displayed, contact your reseller or call maintenance personnel.
60	The battery is currently discharged or disconnected. Verify the connection and allow 30 minutes for charging. If the battery is properly connected and it has not returned to operational state after 30 minutes of charging, contact Technical Support for additional assistance. Press D to disable this warning (if your controller does not have a battery).	Cache backup module information is incorrect. When this message is displayed, contact your reseller or call maintenance personnel.
61	The battery is currently discharged or disconnected. VDs configured in write-back mode will run in write-through mode to protect your data, and will return to write-back policy when the battery is operational. If VDs have not returned to write-back mode after 30 minutes of charging then Contact Technical support for additional assistance. The following VD is affected: X. Press any key to continue.	
62	Two BBUs are connected to the adapter. This is not a supported configuration. Battery and caching operations are disabled. Remove one BBU and reboot to restore battery and caching operations. If dirty cache is lost in this boot, that could have been because of dual battery presence.	
63	Firmware did not find valid NVDATA image. Program valid NVDATA image and restart your system. Press any key to continue.	Valid setting files are not found. When this message is displayed, contact your reseller or call maintenance personnel.
64	IR to MR Migration failed. Press any key to continue with MR defined NVDATA values	Migration is not supported. When this message is displayed, contact your reseller or call maintenance personnel.

	Message	Description
65	There are offline or missing virtual drives with preserved cache. Check the cables and ensure that all drives are present. Press any key to enter the configuration utility.	No virtual drive is found. When this message is displayed, contact your reseller or call maintenance personnel.
66	Incompatible secondary iButton present! Please insert the correct iButton and restart the system. Press any key to continue but OEM-specific features will not be upgraded.	iButton is incorrect. When this message is displayed, contact your reseller or call maintenance personnel.
67	Upgrade Key Missing! An upgrade key was present on a previous power cycle, but it is not connected. This can result in inaccessible data unless it is addressed. Reattach the upgrade key and reboot.	Any upgrade key is not supported. When this message is displayed, contact your reseller or call maintenance personnel.
68	FW Flash in Progress. Please Reset system after X minutes.	Firmware is being written. Restart the system X minutes later.
69	Serial Boot ROM (SBR) device is corrupt or bad. Please contact Technical Support.	A Serial Boot ROM (SBR) is faulty. When this message is displayed, contact your reseller or call maintenance personnel.

High-performance Server Blade settings (X57A1/X57A2 models)

This section describes the high-performance server blade setup with the Web console.

See High-performance server blade setup menu (X57A1/X57A2 models) for information about how to start/finish the BIOS setup menu.

Initial settings with server blade web console

A server blade can be managed remotely by using the server blade Web console.

This section describes how to do the initial settings of the server blade via the server blade Web console.

The following items require initial settings:

- User account configuration
- LPAR manager boot settings
- Mouse mode settings for the remote console
- BMC time settings

❑ Connection

For connection, see Connection, Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models). You can connect to the server blade Web console in the same way as standard server blades.

❑ Login

Start the web browser of the console terminal. See Login in Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for information about login. You can log in to the server blade Web console in the same way as standard server blades.

❑ User account configuration

Set a user account to remotely operate server blades.

See User account configuration in Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for how to set user accounts. You can configure the user account in the same way as standard server blades.

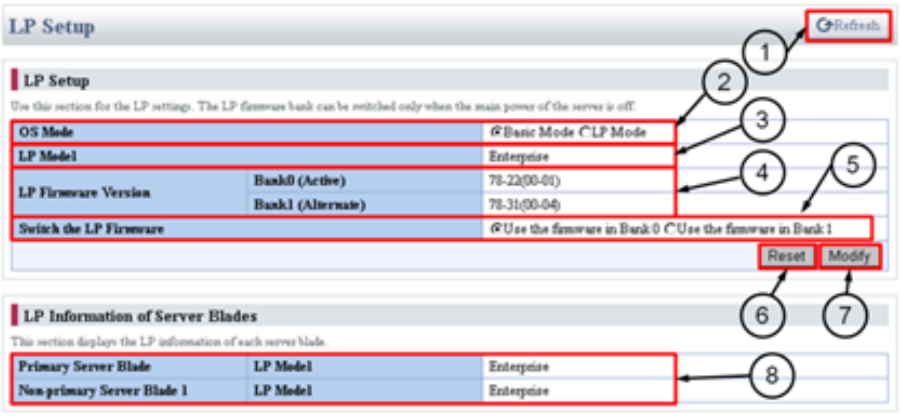
❑ LPAR manager boot settings

Configure the LPAR manager boot settings.

Select **Server Operation** in the upper tabs and then select **LP Setup** in the tree menu on the left to display the following screen.

If you do not use LPAR manager, set **OS Mode** to **Basic Mode**, which is the Default setting.

If you use LPAR manager, set it to **LP** Mode.



#	Item	Description
1	Refresh	Reloads the information.
2	OS Mode	Basic Mode: Select this not to use LPAR manager. LP Mode: Select this to use LPAR manager.
3	LP Model	Displays the LP model string.
4	LP Firmware Version	Bank0, Bank1: Displays LP firmware version of each bank. Active: shows the firmware bank currently selected. Alternate: shows the firmware bank not currently selected. When firmware exists, its version is shown. When no firmware exists, N/A is shown.
5	Switch the LP Firmware	Selects which bank (Bank0 or Bank1) is to be used for next LP boot. Switching banks is executed at the next power-on or reset.
6	Reset	Cancels the edited settings.
7	Modify	Validates the edited settings and moves to the confirmation screen.

#	Item	Description
8	LP Information of Server Blades	Shows LP model name for each server blade in the server partition.



See ‘LP mode setting’ in “LPAR manager boot” in Chapter 12.

❑ Mouse mode settings for the remote console

Set a mouse mode to operate the server blade with the remote console application.

See Mouse mode settings for the remote console in Standard Server Blade Settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for how to set the mouse mode.

❑ BMC time settings

Set the time of the server blade BMC (Baseboard Management Controller).

See BMC time settings in Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for how to set the BMC time.

❑ Logout

Click **Logout** on the right end of the screen to log out of the server blade Web console.

Server blade web console function

This section describes the functions of the server blade Web console.

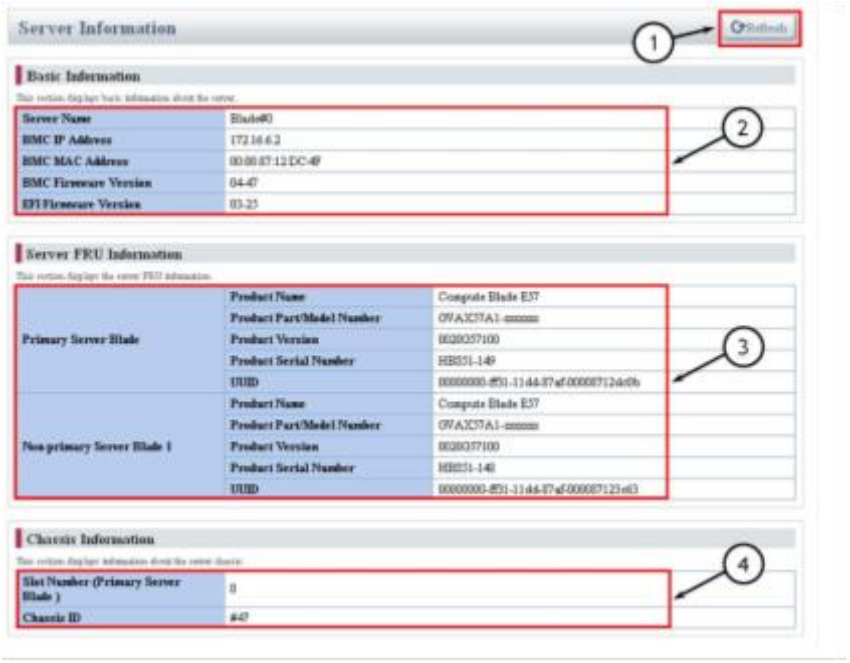
See “Server blade web console function” in Standard server blade settings (X55A1/X55A2/X55R3/X55S3/X55R4 models) for the function list and required roles.

Server Operation tab

Using the Server Operation tab, you can display information about server blade, control the power status, and configure the boot settings of the server blade.

❑ Server information

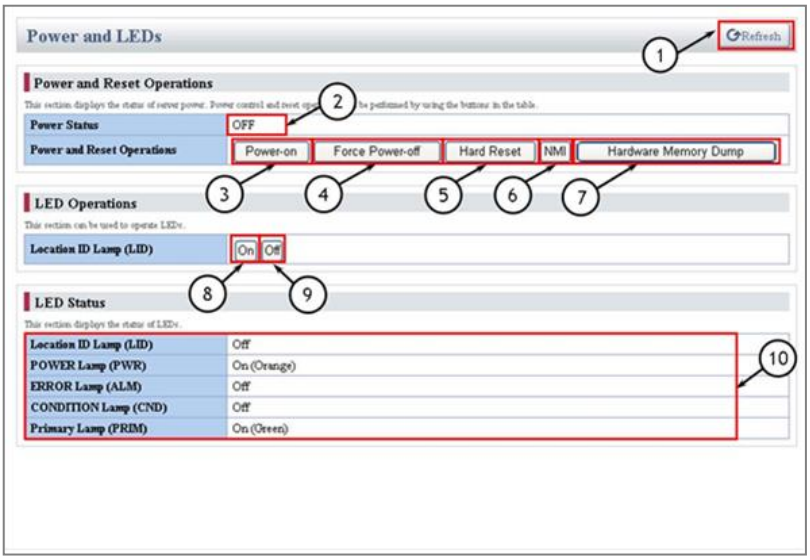
The following screen shows the server blade information.



#	Item	Description
1	Refresh	Reloads the information.
2	Basic Information	Server Name: shows the server blade name set in ”Asset information”. BMC IP Address: shows the BMC IP address of the server blade. For BMC IP address settings, see ‘LC Command’ in Chapter 6. BMC MAC Address: shows the BMC MAC address. BMC Firmware Version: shows the BMC firmware version. EFI Firmware Version: shows the EFI firmware version.
3	Server FRU Information	Shows the product information of each server blade in the server partition. Product Name: shows the product name of the server blade. Product Part/Module Number: shows the product part number of the server blade. Product Version: shows the hardware version of the server blade. Product Serial Number: shows the serial number of the server blade. UUID: shows the UUID of the server blade.
4	Chassis Information	Slot Number (Primary Server Blade): shows the number of the slot where the primary server blade is inserted. Chassis ID: shows the chassis ID set in the management module.

❑ Power and LEDs

This screen shows the power and LED status of the server partition. You can control the power status and reset of the server partition on this screen.

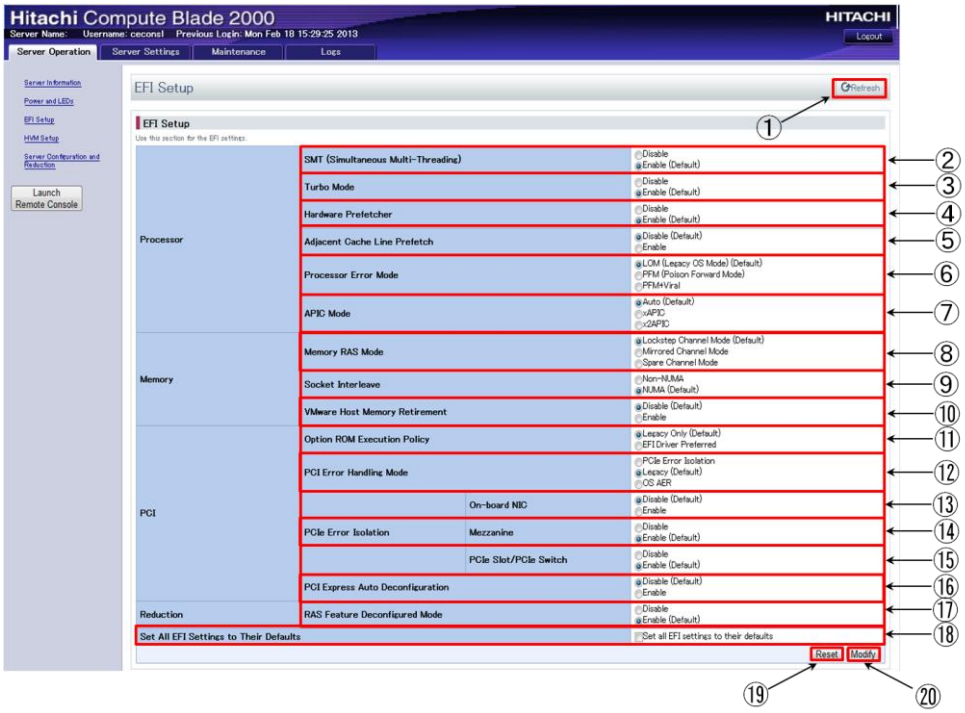


#	Item	Description
1	Refresh	Reloads the information.
2	Power Status	Shows the current power status of the server partition. OFF: The power of the server partition is off. ON: The power of the server partition is on. OFF (Power-on is disabled): The power cannot be turned on due to the power failure.
3	Power-on	Turns on the power of the server partition.
4	Force Power-off	Turns off the power of the server partition without OS shutdown. Shutdown on the OS screen or use the SC function to turn off the power.
5	Hard Reset	Hardware resets the server partition. Enabled when the server partition power is on.
6	NMI	Generates an NMI signal. The dump process will start if the dump function of the OS is configured. Enabled when the server partition power is on.
7	Hardware Memory Dump	Performs hardware memory dump of the server partition.
8	LID On	Turns on LID (Location ID Lamp).
9	LID Off	Turns off LID (Location ID Lamp).
10	LED Status	Shows the status of the LEDs on the front panel of the server partition. Location ID Lamp (LID) POWER Lamp (PWR) ERROR Lamp (ALM) CONDITION Lamp (CND) Primary Lamp (PRIM) For color and description of each LED, see

#	Item	Description
		“High-performance Server partition (X57A1/X57A2)” in Chapter 2.

❑ EFI setup

You can configure the main settings of EFI on the following screen.



#	Item	Description
1	Refresh	Reloads the information.
2	SMT (Simultaneous Multi-Threading)	Disables or enables the SMT function of Intel CPU. Disable / Enable (Default)
3	Turbo Mode	Disables or enables the Turbo mode of Intel CPU. Disable / Enable (Default)
4	Hardware Prefetcher	Disables or enables the Prefetch function of the memory controller in Intel CPU. Disable / Enable (Default)
5	Adjacent Cache Line Prefetch	Disables or enables the Adjacent Cache Line Prefetch function of the memory controller in Intel CPU. Disable (Default) / Enable
6	Processor Error Mode (*1)	Sets Error mode of Intel CPU: LOM (Default): Legacy OS Mode PFM: Poison Forward Mode PFM+Viral: Poison Forward Mode + Viral Mode
7	APIC Mode (*2)	Sets the operation mode of advanced programmable interrupt controller (APIC). Auto (default): Choose this setting to use an OS which supports x2APIC (RHEL6.x and Win2008R2). xAPIC: Choose this setting to use an OS which does not support x2APIC (Any other OS than RHEL6.x and Win2008R2). x2APIC: Do not choose this because this is currently not supported.
8	Memory RAS Mode (*3)	Sets the operation mode of the memory system. Lockstep Channel Mode (Default) Mirrored Channel Mode Spare Channel Mode
9	Socket Interleave	Sets the shared memory configuration of the memory system. Non-NUMA NUMA (Default) (NUMA: Non-Uniform Memory Access)
10	VMware Host Memory Retirement (*4)	Enables or Disables the error memory report function for VMware. Disable (Default) / Enable
11	Option ROM Execution Policy	Sets execution mode of the expansion ROM of I/O mezzanine cards and the PCI-Express adapters. Legacy Only (Default): Prioritize the code for the legacy BIOS. EFI Driver Preferred: Prioritize the code for EFI.
12	PCI Error Handling Mode (*5) (*6)	Sets handling mode for PCI Express failure: PCIe Error Isolation: EFI isolates PCI Express failure

#	Item	Description
		Legacy (Default): EFI does not isolate PCI Express failure. OS AER: OS performs Advanced Error Reporting (AER). Available only for OS that supports AER.
13	On-board NIC (*7)	Disables or enables PCI Express Error Isolation for the on-board NIC. Disable (Default) / Enable This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
14	Mezzanine (*7)	Disables or enables PCI Express Error Isolation for mezzanine cards. Disable / Enable (Default) This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
15	PCIe Slot/PCIe Switch (*7)	Disables or enables PCI Express Error Isolation for PCIe slots and PCIe switches. Disable / Enable (Default) This setting is effective only if PCI Error Handling Mode is set to PCIe Error Isolation.
16	PCI Express Auto Deconfiguration	Disables or enables PCI Express Auto Deconfiguration. Disable (Default) / Enable
17	RAS Feature Deconfigured Mode	Disables or enables the processor and memory deconfiguration (or reduction) that is executed when a component fails. Disable / Enable (Default)
18	Set All EFI Settings to Their Defaults	Restores the EFI Default settings. All the EFI settings, including the settings #2 to #16 are set to the Default.
19	Reset	Cancels the edited settings.
20	Modify	Validates the edited settings and moves to the confirmation screen.

(*1) For EFI firmware version 07-43/08-43 or later on X57A2, you can specify LOM or PFM for the value of Processor Error Mode. PFM can be specified only with Window Server 2012 or later. But for redundancy configuration with the system, do not change from the default value LOM. For model other than X57A2, EFI firmware version later than 07-43/08-43, and OS other than described above , do not change the default value: LOM for Processor Error Mode.

(*2) This function is available only with BMC firmware version 04-48 or later, 06-01 or later, but not available with server blade model X57A1.

(*3) When using VMware with EFI firmware version earlier than 03-12, do not change the value of Memory RAS Mode: The Default value “Lockstep Channel Mode” should be fixed.

(*4) To use this function, BMC firmware version 04-73 or later, 06-01 or later, or EFI firmware version 07-51/08-51 or later is required. With server blade X57A1 model, however, this function is not available.

(*5) When using Windows Server 2003 R2 with X57A1/X57A2 model to which an I/O slot expansion unit is connected, select Legacy as a value for PCi Error Handling Mode.

(*6) If the BMC firmware version is 04-32 or earlier, the default value of this item is PCIe Error Isolation. If the BMC firmware version is 04-33 or later, 06-01 or later, the default value is Legacy.

(*7) To use this settings on the server blade X57A1/X57A2 model, BMC firmware version 04-32 or later, 06-01 or later, must be installed on the server blade.



- The edited EFI settings will be effective on the next power-on or reset.
- When you use the remote FD or remote CD/DVD as a boot path, start Remote Console Application and start the remote FD or remote CD/DVD before you power on the server blade.
- For details about Remote Console Application, see the *Remote Console Application User's Guide Hitachi Compute Blade 2000* in the CD that came with this equipment.

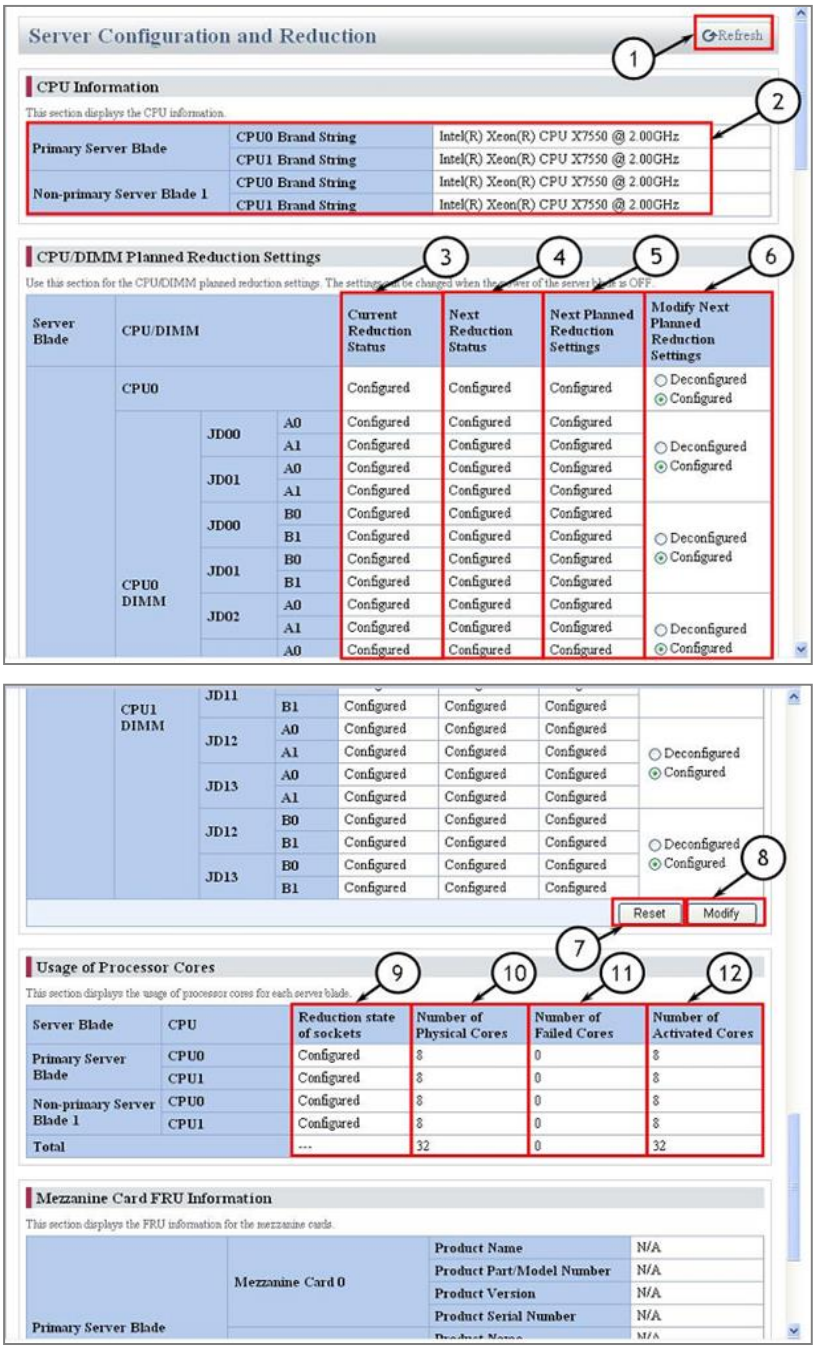
❑ LP setup

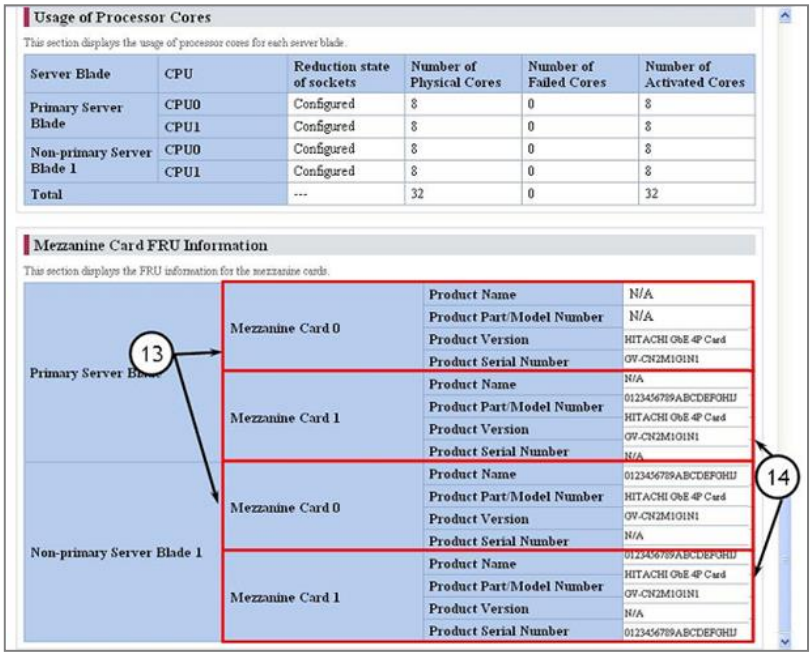
You can enable and disable the LP boot and set the LP firmware to be used for the LP boot on this screen. See "LPAR manager boot settings" in "Initial Settings with Server Blade Web Console".

❑ Server configuration and reduction

This screen displays information of the CPUs and mezzanine cards installed in the server partition, and also displays the reduction information on the CPUs, DIMMs, and processor cores.

Reduction information includes whether components are deconfigured due to a failure or not. You can also set up the planned reduction for the CPUs, DIMMs, and processor cores on this screen.





#	Item	Description
1	Refresh	Reloads the information.
2	CPU Information: CPU0 Brand String CPU1 Brand String	Shows the types of CPUs: information on the last EFI boot.
3	Current Reduction Status	Shows the current reduction status of CPU/DIMM. Configured : Not deconfigured. Deconfigured : Deconfigured as planned. Absent : Not installed. Failed : Deconfigured due to failure. Not Available : Deconfigured due to failure of other CPU or DIMM.
4	Next Reduction Status	Shows the CPU/DIMM reduction status to be applied at the next power on or reset.
5	Next Planned Reduction Settings	Shows the planned CPU/DIMM reduction settings to be applied at the next power on or reset. Deconfigured: CPU/DIMM will be deconfigured. Configured: CPU/DIMM will not be deconfigured.
6	Modify Next Planned Reduction Settings	Changes the planned CPU/DIMM reduction settings to be applied at the next power on or reset. Deconfigured: CPU/DIMM will be deconfigured. Configured: CPU/DIMM will not be deconfigured.
7	Reset	Cancels the edited settings.
8	Modify	Validates the edited settings and moves to the confirmation screen.

#	Item	Description
9	Reduction state of sockets	Shows the current reduction status of the CPUs. Configured : Not deconfigured. Deconfigured : Deconfigured as planned. Absent : Not installed. Failed : Deconfigured due to failure.
10	Number of Physical Cores	Shows the number of the processor cores that are contained in the CPU.
11	Number of Failed Cores	Shows the number of the processor cores that are deconfigured due to failure.
12	Number of Activated Cores	Shows the number of the processor cores that are active.
13	Mezzanine Card FRU Information: Mezzanine Card 0	Shows the FRU information of the mezzanine card 0 per server blade in the server partition.
14	Mezzanine Card FRU Information: Mezzanine Card 1	Shows the FRU information of the mezzanine card 1 per server blade in the server partition.



- You cannot set up the planned reduction or deconfigure CPU or DIMM below the minimum configuration. A message, indicating that planned reduction is not allowed, is displayed.
- Planned reduction can be set only when the power to the server blade is off.
- The screenshots are of 2-blade SMP server partition. The reduction units, each of which is a group of CPUs or DIMMs that need to be deconfigured or configured simultaneously, of 4-blade SMP server partition are different from those of 2-blade SMP server partition.

Server Settings tab

Using the Server Settings tab, you can configure the functions to manage the server blade.

See Server Settings tab in Standard Server Blade Setup (X55A1/X55A2/X55R3/X55S3/X55R4 models).

Maintenance tab

Using the Maintenance tab, you can update the firmware, backup and restore the data managed on the firmware, and restart BMC.

See Maintenance tab in Standard Server Blade Setup (X55A1/X55A2/X55R3/X55S3/X55R4 models).

❑ EFI firmware management

Only maintenance personnel can use this menu.

❑ FPGA ROM management

Only maintenance personnel can use this menu.

Log tab

Using the Log tab, you can download the logs collected by BMC, the blade management micro controller.

See Logs tab in Standard Server Blade Setup (X55A1/X55A2/X55R3/X55S3/X55R4 models) for information about how to operate the screen.



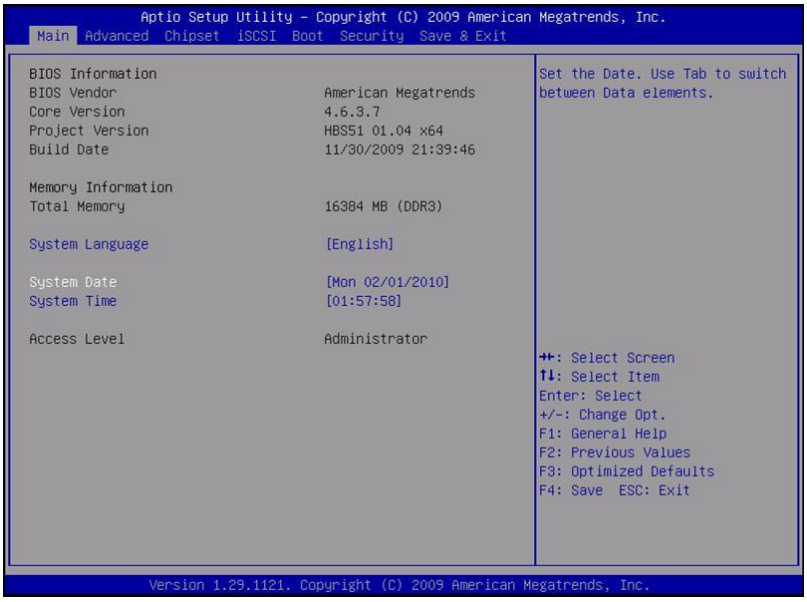
When using the operation log with server blades X57A1 model, you need to install BMC firmware 04-51 or later.

High-performance server blade setup menu (X57A1/X57A2 models)

EFI setup screen

By entering the EFI Setup screen while the server blade is booting, you can halt the boot process, and check or change the settings.

With the EFI startup screen open, press the **F2** key to display the EFI Setup screen



The EFI Setup screen has six setup menus: Main, Advanced, Chipset, iSCSI, Boot, Security, and Save & Exit.

Main menu

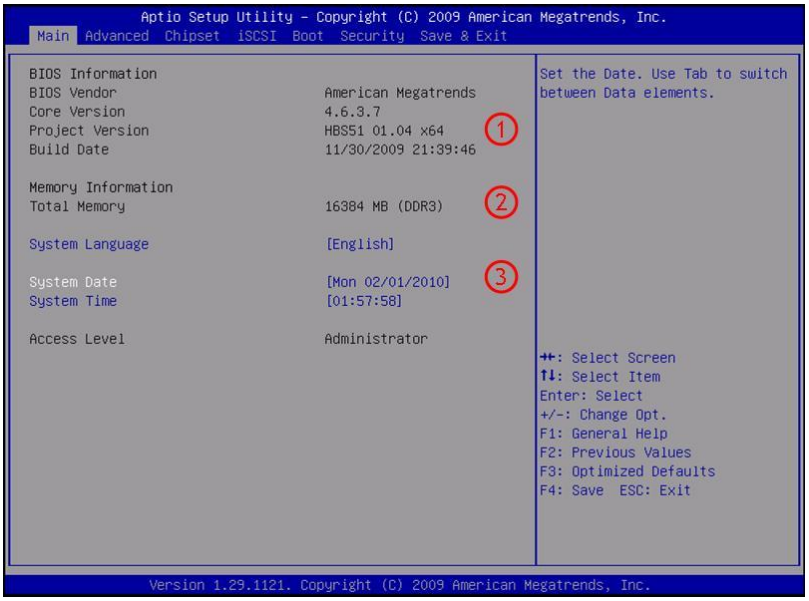


Figure 5-34 Main menu

On the Main menu, you can check the following items:

- EFI version: (1)
- Installed memory: (2)
- Server blade system time: (3)

Note: The keys used for operations in the EFI Setup menus are shown on the right side of the screen. Make sure not to use function keys F1 to F4 because you may unintentionally alter the settings with those keys.

❑ Checking the EFI version

The EFI version is the "XX.YY" part of "HBS51 XX.YY x64" in the "Project Version" field, where:

XX : Major Version

YY : Minor Version

In the example below, the EFI version is 01-04.



❑ Checking the installed memory

After increasing or replacing memory, you can check the amount of installed memory from the following item. Note that the displayed size is the total memory.*

In this example, 16384 MB of memory is installed.



*Note that when memory mirroring mode is enabled, the displayed size is one half of the total installed memory.

❑ Setting the server blade system time

You can check and set the date and time set in the server blade system.

Move the cursor to the item you want to change.



Use the **Tab** key to toggle between **System Date** and **System Time**. To change the setting, use the plus (+) and minus (-) keys.

Advanced menu

On the **Advance**d menu, you can enable or disable the PXE booting option.

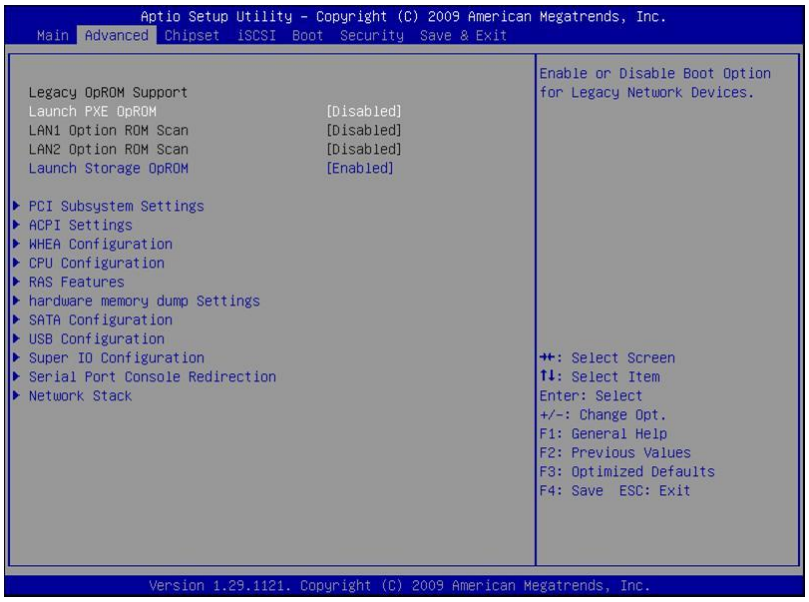


Figure 5-35: Advanced menu

To enable PXE booting, move the cursor to **Launch PXE OpROM**, and press **Enter**. The following screen displays.

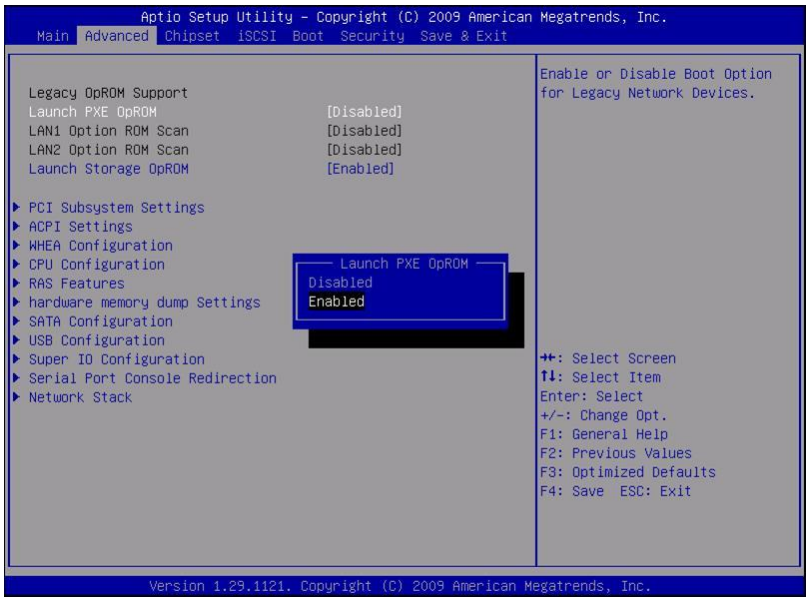


Figure 5-36: Setting PXE enabled

To specify **Enabled**, move the cursor to **Enabled**, and press **Enter**.

Next, enable PXE booting for LAN1 in the same manner.

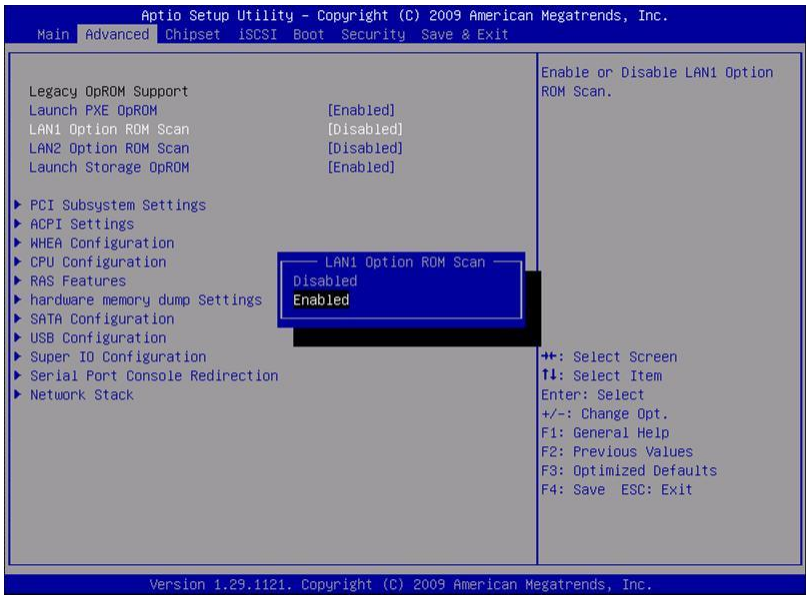


Figure 5-37: Setting LAN1 PXE enabled

To enable PXE booting for LAN2, perform the setting in the same manner. You can enable PXE for LAN1 and LAN2 respectively or simultaneously.

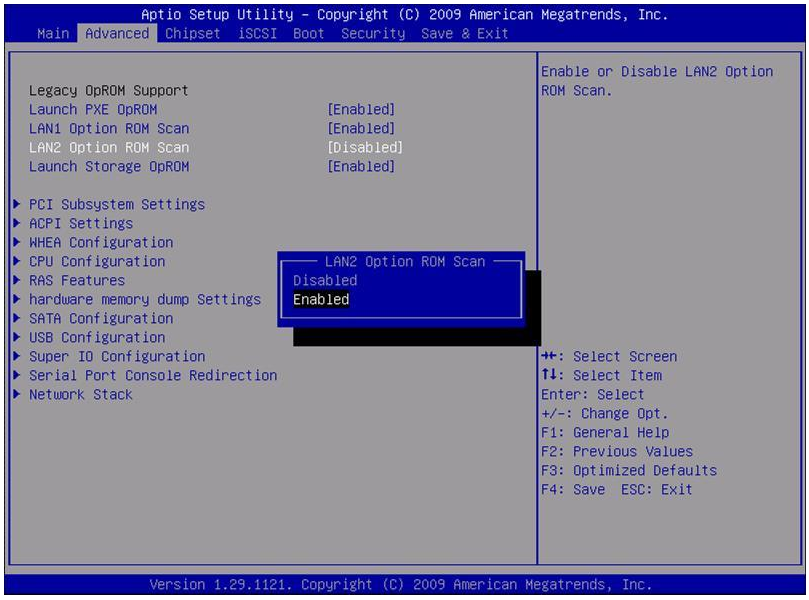


Figure 5-38: Setting LAN2 PXE enabled

After changing settings, make sure to select "Save Changes and Reset" or "Save Changes" on the Save & Exit menu.

This is the last item that can be set on the Advanced menu.

Be sure not to change other settings because EFI might fail to restart.

Chipset menu

On the **Chipset** menu, you can check memory-related and Wake On Lan settings.

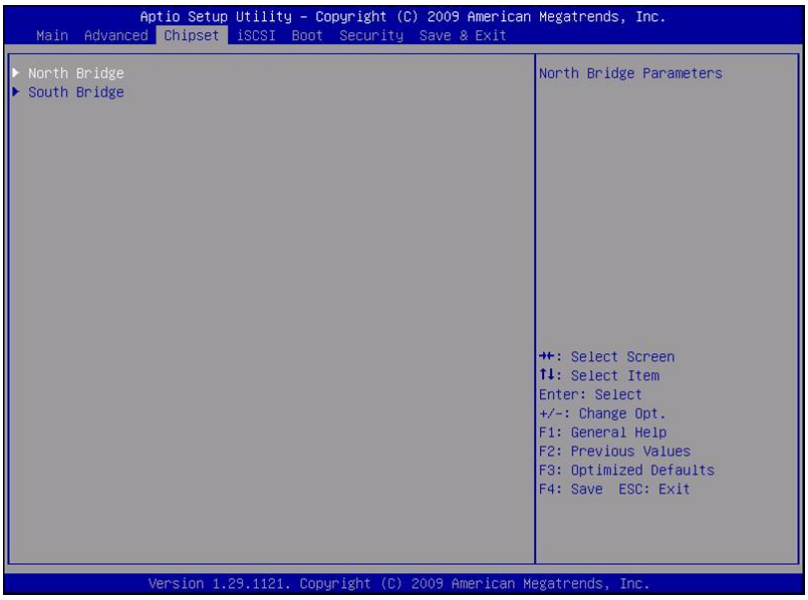


Figure 5-39: Chipset menu

(1) Checking the Memory Init Mode and NUMA Settings

To check the Memory Init Mode and NUMA settings, select **North Bridge** on the Chipset menu to show the following sub-menu.

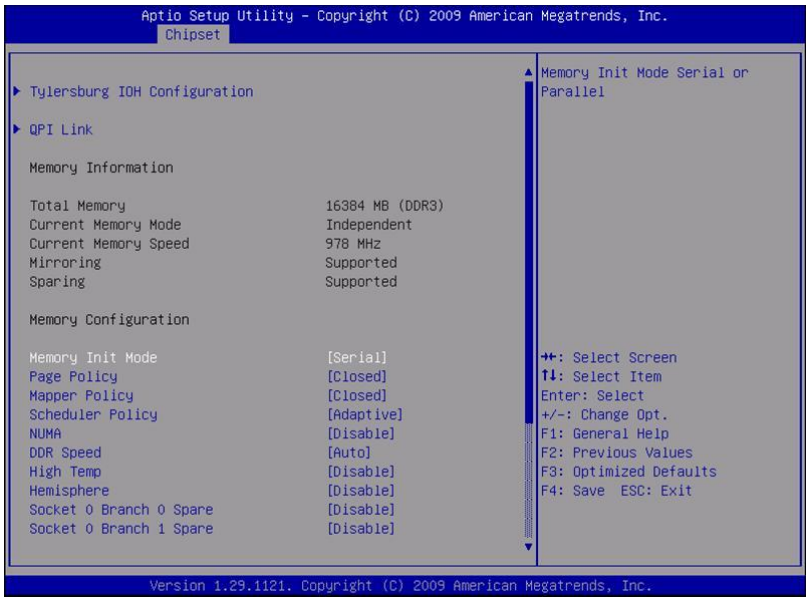


Figure 5-40: North Bridge sub-menu

Make sure that the settings for **Memory Init Mode** and **NUMA** are the same as the settings on server blade Web console.

See the BMC manual for details about setting the memory mode on the server blade Web console.

On the North Bridge sub-menu, you can check the **Memory Init Mode** and **NUMA** settings, but you must not attempt to change the settings.

Change the **Memory Init Mode** and **NUMA** settings, if necessary, only from the server blade Web console.

The settings on the North Bridge sub-menu can be viewed only. They must not be changed because if a setting is changed inadvertently, the EFI may not start.

(2) Checking and setting Wake On Lan

To check the **Wake On Lan** setting, select **South Bridge** on the **Chipset** menu to show the following sub-menu.

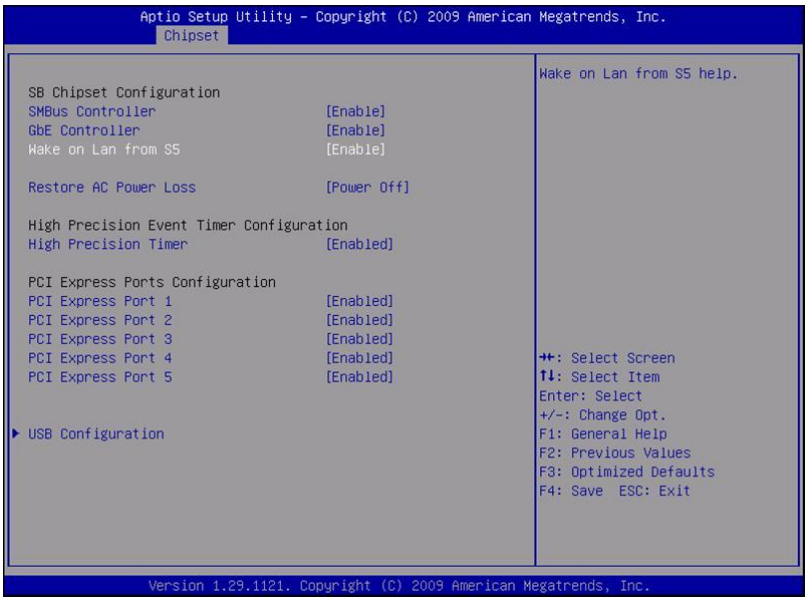


Figure 5-41: South Bridge sub-menu

Wake On Lan is always set to **Enable**.

If the setting appears as **Disable**, change it to **Enable**. On the South Bridge sub-menu, **Wake On LAN** is the only setting you can change. You must not change the other settings.

iSCSI menu

On the **iSCSI** menu, you can check iSCSI settings.

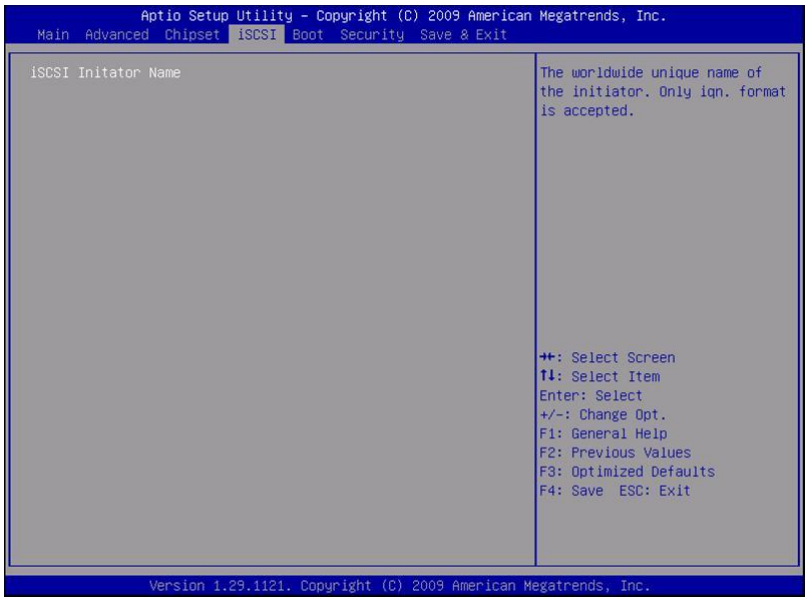


Figure 5-42: iSCSI selection menu

Boot menu

On the **Boot** menu, you can set the boot paths.



Figure 5-43: Boot menu

The boot devices are booted in the order (#n) set in the **Boot Option Priorities** (where n: 1, 2, 3,...).

Up to four boot paths can be set. Items to be set in this screen depend on devices connected.

(1) About Boot Paths (Legacy Boot and EFI Boot)

Boot paths are categorized into two boot modes in the Compute Blade 2000. The implemented boot processing depends on which mode you select.

The two Compute Blade 2000 boot modes are:

- Legacy booting (conventional mode and boot method)
- EFI booting (newly supported mode and boot method)

The boot mode is determined automatically according to the boot device selected as **Boot Option #1**.

When **Built-in Shell** or **UEFI:xxxxx** is selected as **Boot Option #1**, EFI booting applies and the legacy boot path will be ignored.

Note that when a boot device other than **Built-in Shell** or **UEFI:xxxxx** is selected as **Boot Option #1**, the EFI boot path will be ignored.

❑ Selecting PXE booting

PXE booting can be specified in the boot path if **Enabled** is set for **Launch PXE OpROM** on the **Advanced** menu.

To specify PXE booting, set **Boot Option #1** as shown in the following screen:

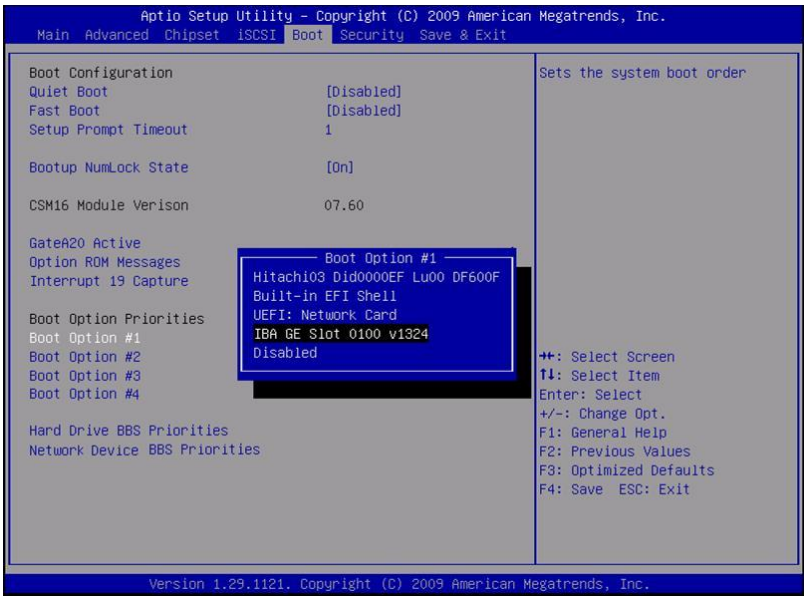


Figure 5-44: Setting the PXE boot path

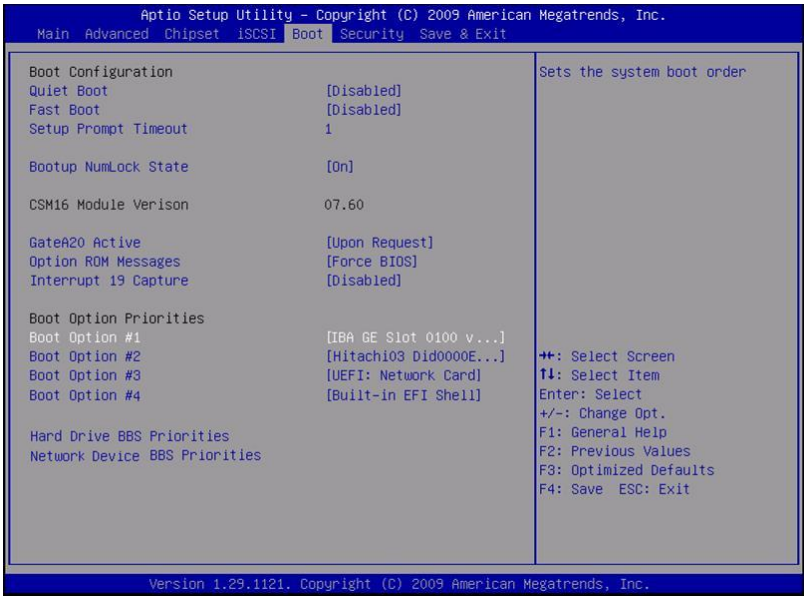


Figure 5-45: Screen with PXE boot path specified

After changing the setting, remember to select **Save Changes and Reset**, or **Save Changes** on the Save & Exit menu.

❑ Reset boot option

When you reboot a server blade with Reset Boot Option Enabled, Boot Option Priorities is initialized. Execute the following to initialize Boot Option Priorities.

- Remove the boot device and Built-in EFI shell to delete the boot option
- Initialize the boot priorities to the default.

Reset Boot Option is shown and available for EFI firmware version 07-43/08-43 or later for X57A2. Make sure to execute Save Changes and Reset referring to Save & Exit menu before initializing Boot Option Priorities.



You cannot separately delete boot options and initialize boot priorities. Initialize Boot Option Priorities, and then reset boot options as necessary.

Security menu

The **Security** menu is for setting the administrator or user password.

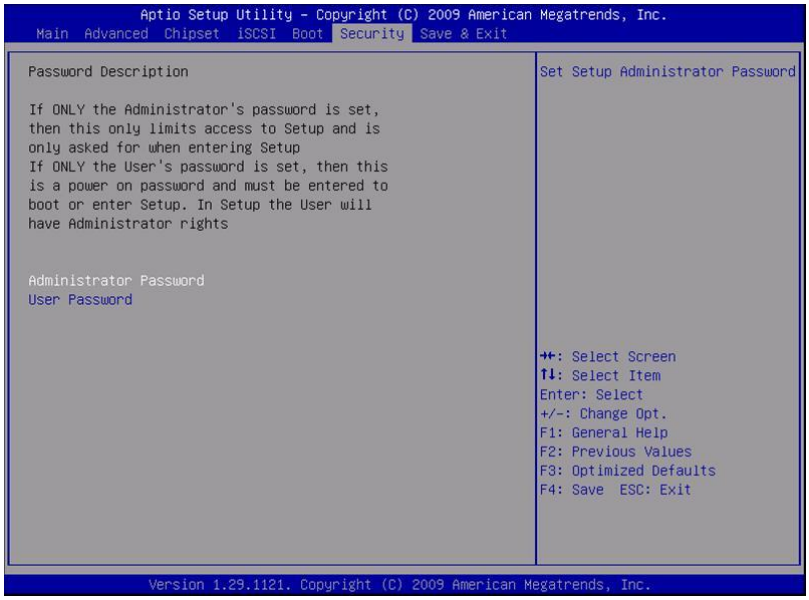


Figure 5-46: Security menu

You will need to input a password, which you have set, at the timing shown in the table below.

#	Administrator password	User password	Request for password authentication
1	✓	✓	While a server blade is being booted
2	✓	-	When you enter the EFI Setup screen
3	-	✓	While a server blade is being booted

[✓]: The password is set; [-]: The password is not set.

Any password can be set for a user.

When you set a password, it is always necessary to enter the password for authentication while booting the server module.

When you set the N+M cold standby, HA, or automatic OS boot, do not set a password. Otherwise, the password authentication interrupts switching systems or booting modules.

Save & Exit menu

Use the **Save & Exit** menu to save changes or to restore changed settings to the Defaults.

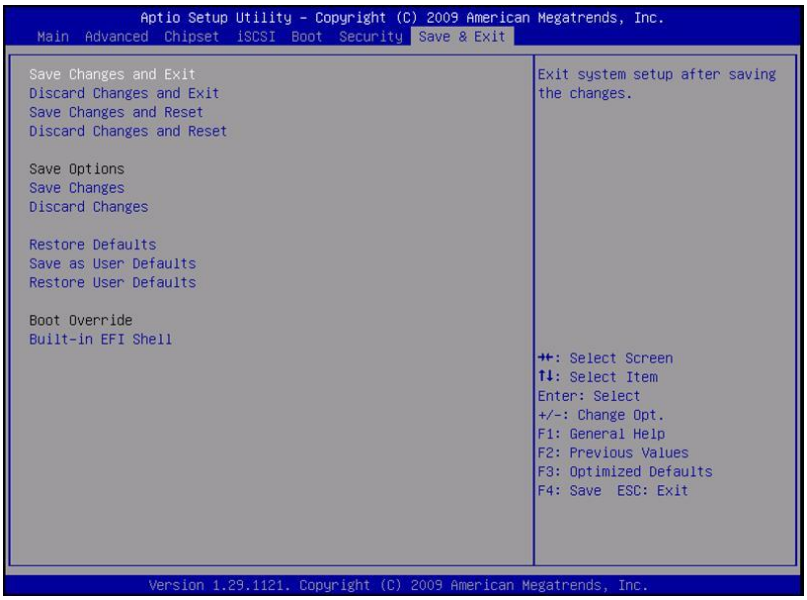


Figure 5-47: Save & Exit menu

The following table describes the items in the Save & Exit menu.

#	Item	Processing
1	Save Changes and Exit	Saves changes and exits the Setup utility. Boots the system from the device set in the boot path.
2	Discard Changes and Exit	Discards changes and exits the Setup utility. Boots the system from the device set in the boot path.
3	Save Changes and Reset	Saves changes and restarts the system.
4	Discard Changes and Reset	Discards changes and exits the Setup utility. Restarts the system.
5	Save Changes	Saves changes.
6	Discard Changes	Discards changes.
7	Restore Defaults	Restores settings to the system Defaults.
8	Save as User Defaults	Saves settings as user Defaults.
9	Restore User Defaults	Restores settings to the user Defaults.

❑ Boot override

Boot Override on the **Save & Exit** menu allows you to boot the system from a specific device, disregarding the boot path set as **Boot Option #1**.

Unless otherwise specified, **Boot Override** would not normally be used.

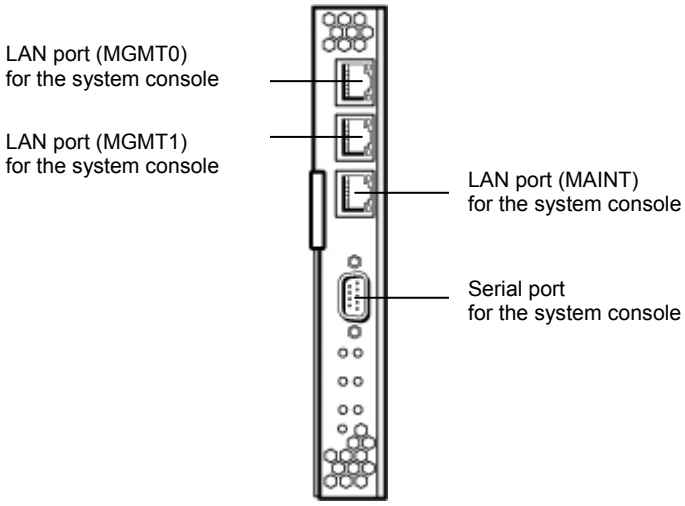
6

Management module settings

The management module controls the system equipment and monitors its environment. This chapter describes how to set the management module.

External interface for the management module....430
Cable connection for the system console....432
Initial settings of management module....434
Backing up and restoring the settings....441
Account....452
Privilege and role....454
System console command reference....455
System web console....658
SVP (service processor log) message....774
HCSM (Hitachi Compute Systems Manager) alert message....789

External interface for the management module



Port number	Description
LAN port (MGMT0)	Port for connecting to the management network: Connect this port at the initial setting.
LAN port (MGMT1)	Port for connecting to the management network: This is not available at the initial installation. See “Setting the Connection Method” in Chapter 13 for details.
LAN port (MAINT)	Dedicated port for maintenance. Only maintenance personnel can use this port. Any user cannot use this.
Serial Port	Serial port for the system console: used for maintenance when a local area network (LAN) port is not available.

Tip

Prepare the following items for connection with the MAINT port:

- A terminal for the system console
- Unshielded Twist Pair cable (UTP) cable: UTP-5 or better
- Client software: HyperText Transfer Protocol (HTTP), Telnet, or Secure SHell (SSH)

When you connect the management module via HTTP, Telnet, or SSH, see the following table about the default setting of the management module at the shipment:

Item	Setting at the shipment
IP address	192.168.0.1
Subnet mask	255.255.255.0
HTTP	Enabled
SSH	Enabled
Telnet	Enabled

- Prepare the following items for connection via serial port.
  - A terminal for the system console
  - A connecting cable for the serial port (RS-232C cross cable D-SUB9 pin female-female connector)
  - Terminal software such as Hyper Terminal: available for VT100 emulation

When you connect to the serial port of a management module, see the following table about communication parameter settings to the terminal software.

Communication parameter	Setting
Communication rate	9600bps
Data	8 bit
Parity	None
Stopbit	1 bit
Flow control	None

- The system Web console cannot be used via serial port.

Cable connection for the system console

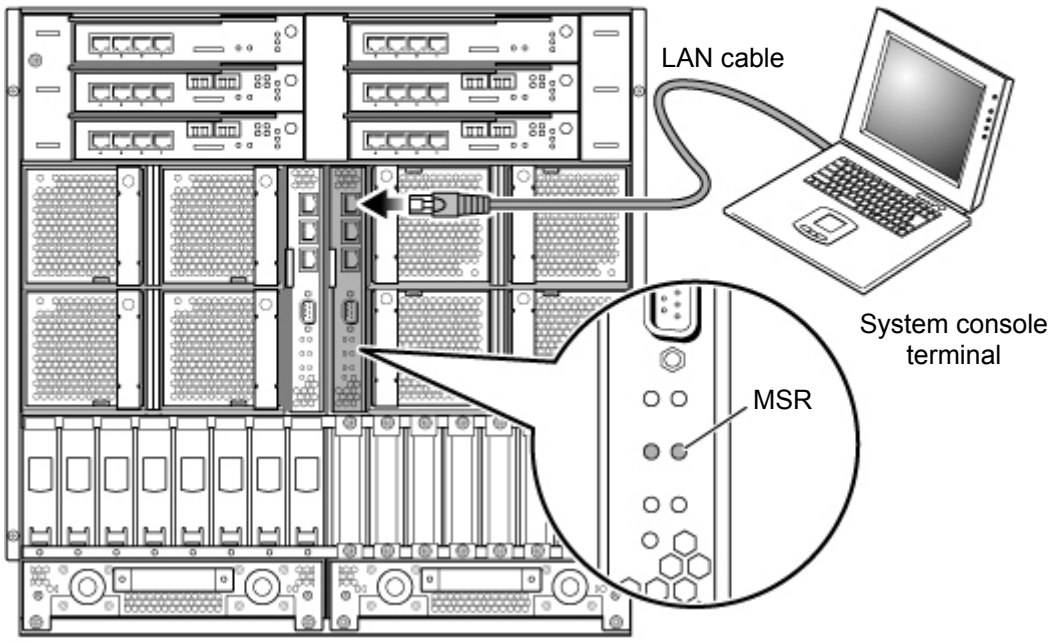
NOTICE

If a device with the same IP address as that for the Baseboard Management Controller (BMC) on the management module or server blade exists on the network, a failure will occur on the system equipment when you connect the management module to a network.

Complete a network configuration before connecting a cable to the management module.

Connect with LAN cable

Both straight cable or cross cable are available for the LAN port for the system console. Communication rate is automatically selected from 10, 100, or 1000 Mbps.

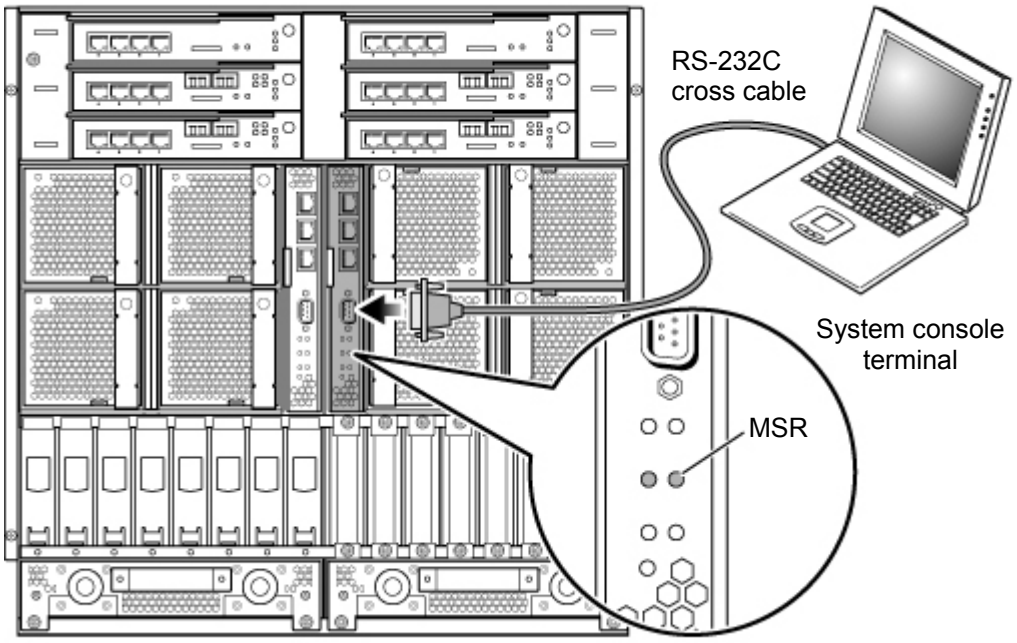


Connect the MGMT0 port of the management module in the rear of the system equipment to your system console terminal using a LAN cable. When two management modules are installed, connect to the management module with the Master light emitting diode (MSR LED) that lights solid green. Prepare the LAN cable to connect to the terminal by yourself.

Connect with serial cable

Use RS-232C cross cable (D-SUB9 pin female-female) for the serial port of the system console. Communication rate setting at the shipment is 9600 bps.

Connect the serial port of the management module in the rear of the system equipment



to your system console terminal using a RS-232C cross cable. When two management modules are installed, connect to the management module with the MSR LED that lights solid green. Prepare the RS-232C cross cable to connect to the terminal.

Initial settings of management module

The management module is hardware that manages the Compute Blade equipment. It must be initialized to suit your environment.

This section describes how to initialize the management module.

The following data needs to be initialized:

Registration of user account information

Setting of device identification information

Setting of network information such as IP addresses

To set the information above, use the console functions through the user interface port of the management module. The management module has the following console function.

Initial settings of the management module via system web console

(1) Prerequisites for using the system Web console

A system console terminal should satisfy the following conditions to use the system Web console.

.

Item	Condition
OS	Microsoft® Windows® Server 2008, Standard Edition Microsoft® Windows® Server 2008, Enterprise Edition Microsoft® Windows® Server 2003 R2, Standard Edition Microsoft® Windows® Server 2003 R2, Enterprise Edition Microsoft® Windows® Server 2003, Standard Edition Microsoft® Windows® Server 2003, Enterprise Edition Microsoft® Windows® XP Professional Microsoft® Windows® 2000 Professional Microsoft® Windows® Vista Business
Browser	Internet Explorer 6.0 or later versions (Tab functions of the browser, however, are not available.)
Resolution	800 x 600 or higher with 65536 or more colors (1280 x 1024 or higher is recommended.)

(2) Browser setting

Check the browser setting of the terminal for the system console before using the system Web console. With improper settings, the system Web console will not operate properly.

- Disable the Proxy server setting for use.
- Enable JavaScript download and execution.
- Add the management module IP address to the trusted site.
- Disable the popup block function.
- Enable the image display.
- Enable the cookie.

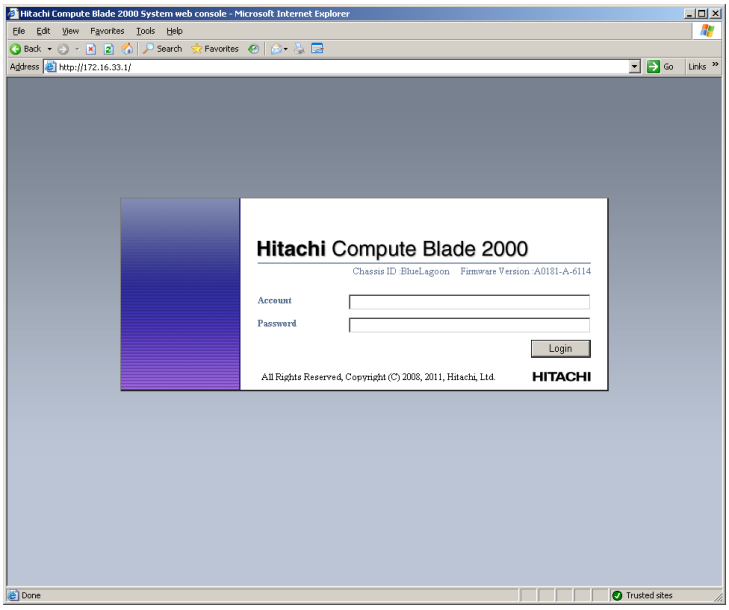
See the OS manual for each procedure.

(3) First login

1 Boot the browser of the system console terminal.

2 Enter `http://192.168.0.1/` in the URL field on the browser. When the firmware version of your management module is A0310 or later, enter `https://192.168.0.1/` here.

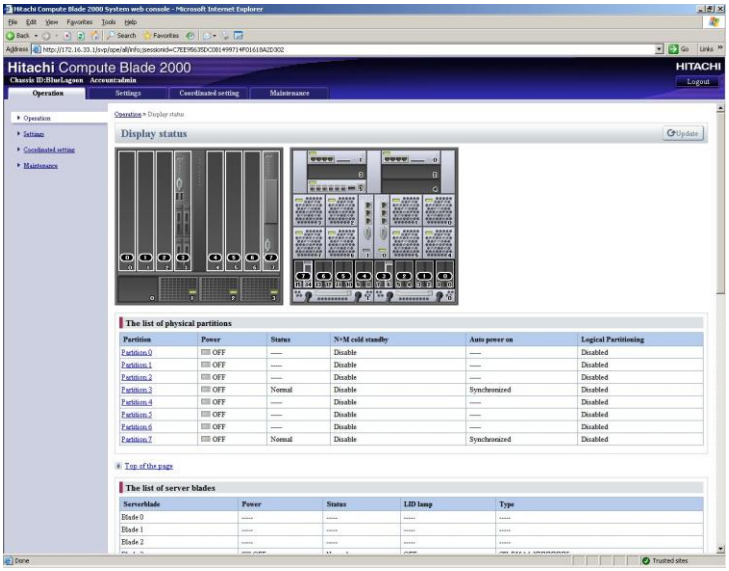
3 When connection is successful, the login screen of the Web console will appear.



4 Fixed user account and password is set to the Administrator account for the system console at the shipment. Enter the following user account and password to login.

Item	Setting at the shipment
User account	administrator
Password	password

5 When login is successful, the operation screen of the Web console will appear.



(4) Password change in Administrator account

See “User Account Setting”.

Tip

It is strongly recommended that the password to the Administrator account is changed.

(5) Device identifier setting

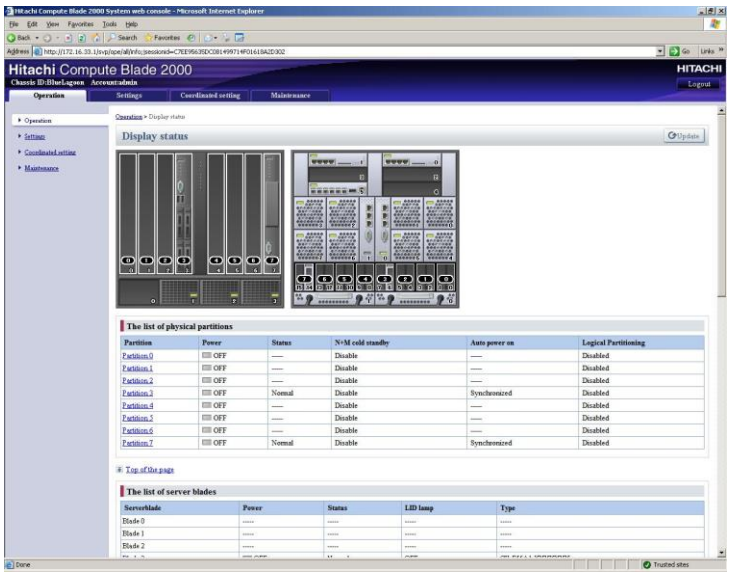
See “Server Chassis Module Management”.

(6) Network information setting, such as IP address

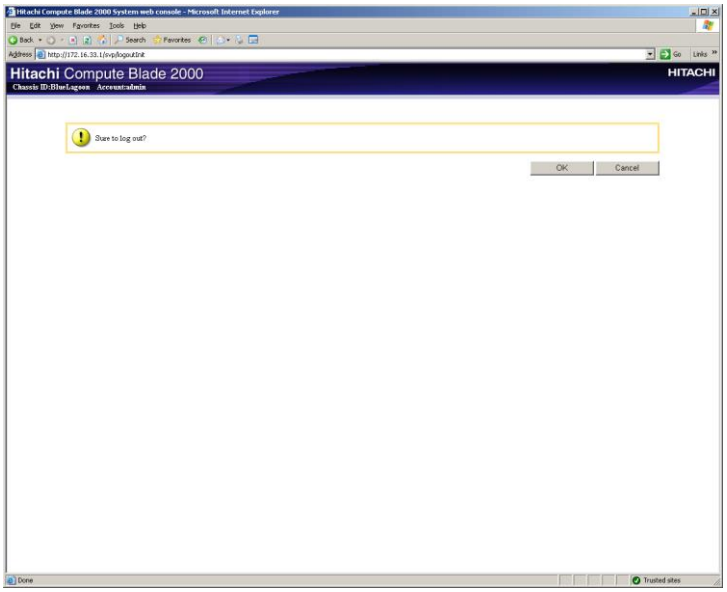
See Configuration of Network” in System Web Console.

(7) Logout

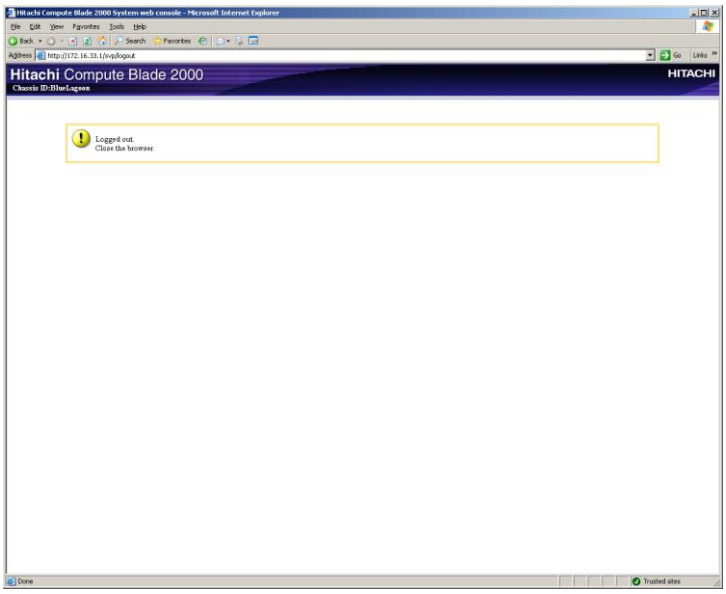
1 Click **Logout** on the upper right on the system Web console screen.



2 When the logout confirmation screen appears, click **OK.**



3 Logout is complete. Close the browser.



Note

Make sure to log out of the Web console before closing the browser. If you close the browser before logging out, close all browsers and then log into the Web console the next time.

Initial settings of the management module via system console

(1) First login

1 Boot client software, such as Telnet, SSH, or Serial terminal software, of the system console.

2 Specify 192.168.0.1 to connect the client software in Telnet or SSH, and start the connection.
Specify the port connected to the management module for the serial connection.

3 Fixed user account and password is set to Administrator account for the system console at the shipment. Enter the following user account and password to login.

Item	Setting at the shipment
User account	administrator
Password	password

4 When login is successful, the **system console main** menu will appear.

```
Hitachi Compute Blade 2000 Management Module
ALL RIGHTS RESERVED,COPYRIGHT (C), 2008, 2010, HITACHI,LTD.
Chassis ID        : 5713RF0 00108
Firmware Revision : B0100-Z-2919

<< System Console Main Menu >>
    P. Start OS console session.
   SW. Start switch module console session.
    S. System command mode.
    X. Exit.
```

5 Enter S on the **system console main** menu to enter the command mode.

```
<< System Console Main Menu >>

    P. Start OS console session.
   SW. Start switch module console session.
    S. System command mode
    X. Exit.
(P,SW,S,X) : S (Enter)
[Clear the screen.]
Use EX Command to return to Main Menu.
Use HE Command to get a list of available commands.
```

(2) Password change in Administrator account

See “User Account Setting”.



It is recommended that the password to Administrator account is changed.

(3) Device identifier setting

See CI command .

(4) Network information setting, such as IP address

See LC command.

(5) Logout

Execute the EX command in the command mode, and then enter **X** on the **system console main** menu to complete the logout.

```
5713RF0 00108(0)SVP> EX (Enter)
[Clear the screen.]
<< System Console Main Menu >>

    P. Start OS console session.
   SW. Start switch module console session.
    S. System command mode
    X. Exit.
(P,SW,S,X) : S (Enter)
```

Backing up and restoring the settings

The following setting can be saved and restored from the management module.

Item	Operation available
Management module setting	Save and Restore
Fibre-channel setting	Save
Logical partitioning (LPAR) manager setting	Save and Restore

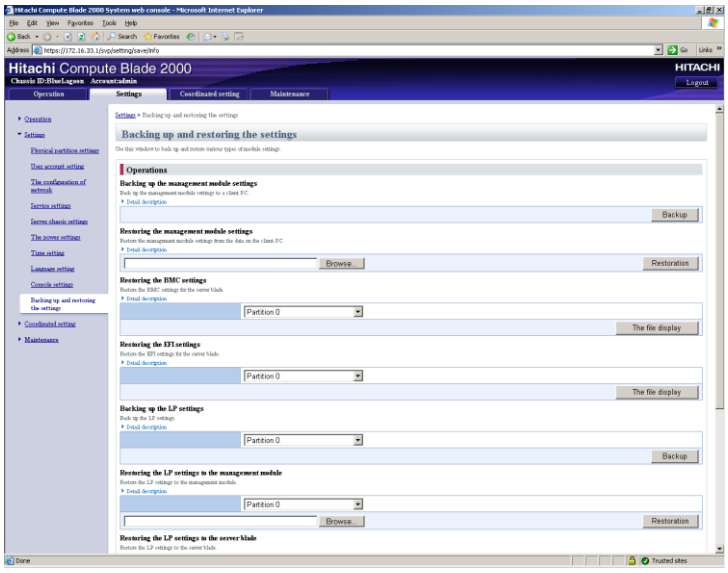
The procedure with the system Web console is described below. For the system console, see UBR command.

Tip

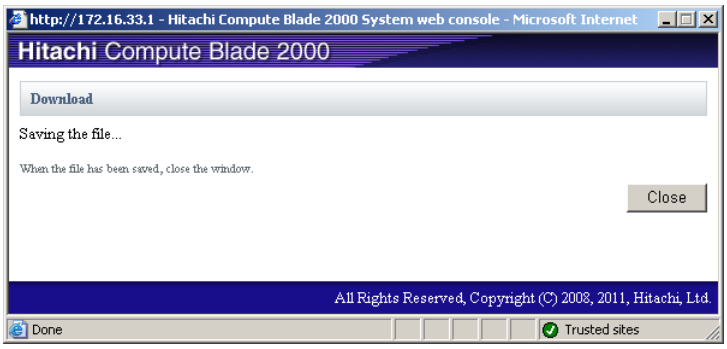
- Setting backup files that are created using the system web console or system console can be restored using the system console as well as the system web console.
- LPAR manager backup files saved in the management module can be restored using the LPAR manager Maintenance Tool.

Backing up the management module settings

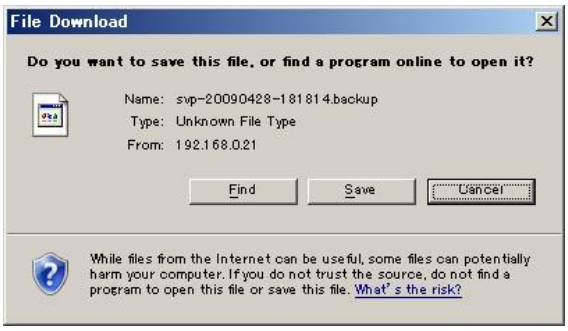
1. Log in to the system web console as Administrator.
2. Select **Settings** and then **Backing up and Restoring the Settings** from the tree menu.



3 Click **Backup** in the item **Backing up the management module settings**. The following window appears. Download will start in about five minutes. Make sure to click **Close** only after the download has been completed.



4 When the file is ready to download, the following dialog box appears. Click **Save**.



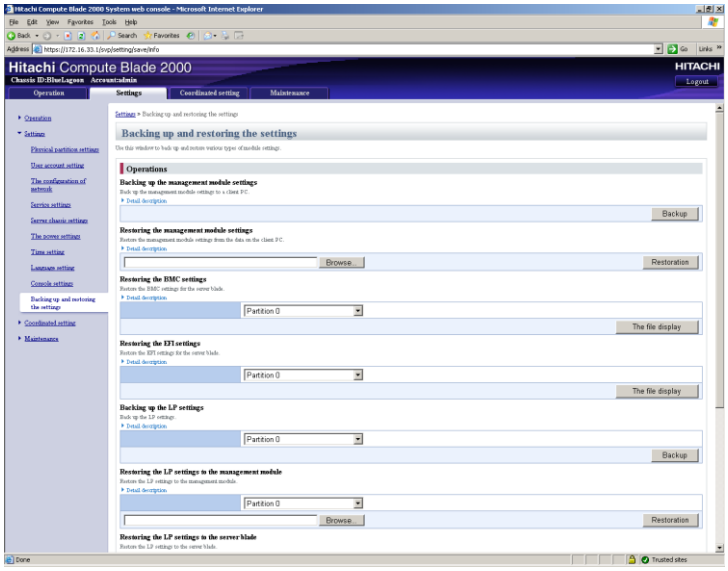
5 Select a destination to save the backup file.
Backup file name is “svp-YYYYMMDD-hhmmss.backup” by default, which can be changed. Enter a file name and then select **Save**. Download will start.

6 After the download has been completed, close the window.

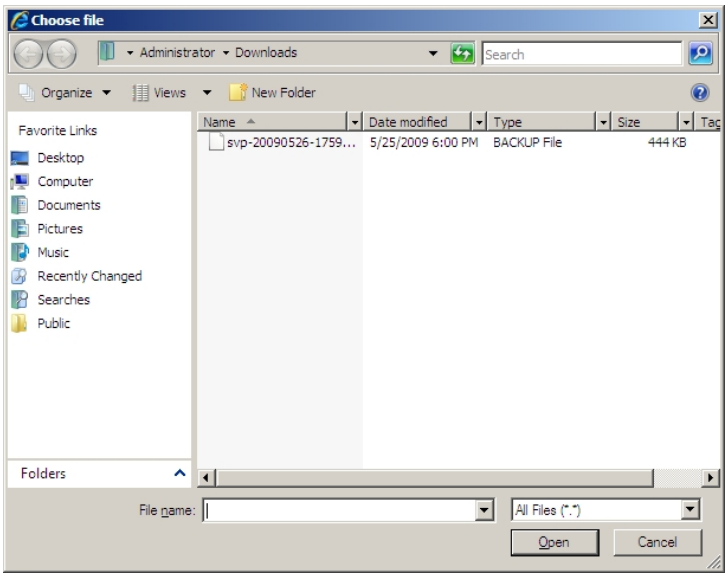
Restoring the management module settings

1 Log in to the web console as Administrator.

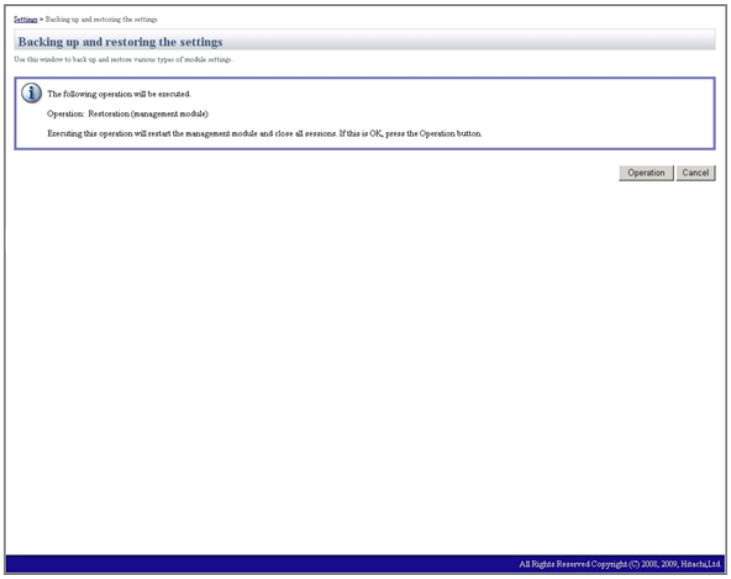
2 Select **Settings** and then **Backing up and Restoring the Settings** from the tree menu.



3 Click **Browse** in **Restoring the LPAR manager settings to the management module**, and select a backup file for restoration.



4 Confirm that the backup file name is correct, and click **Restoration**. The following screen appears:

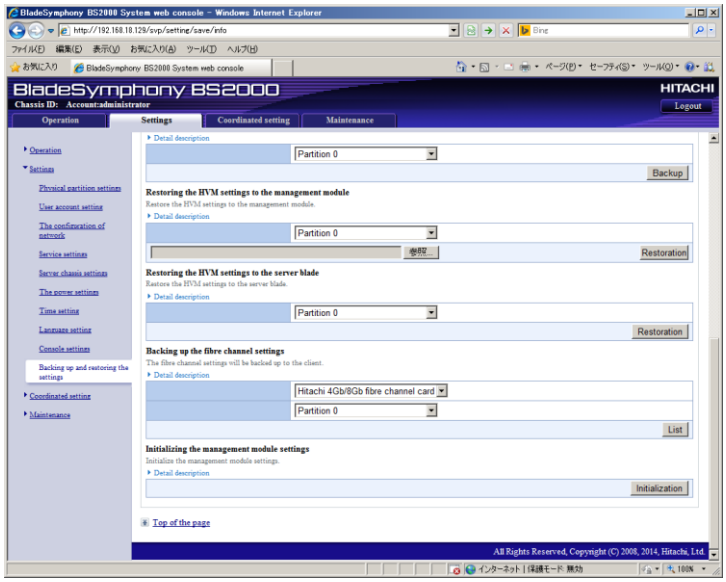


5 Click **Operation** on the above confirmation screen. The management module configuration will be restored. The screen returns to the **Backup or Restoration of the configuration** screen.

Backing up the Fibre-channel card settings

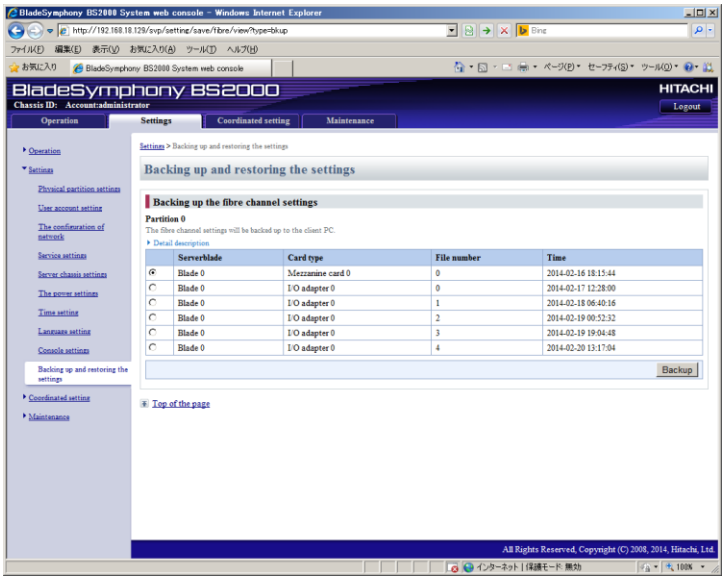
1 Log into the Web console as Administrator.

2 Select **Settings** and then **Backing up and restoring the settings** from the tree menu.

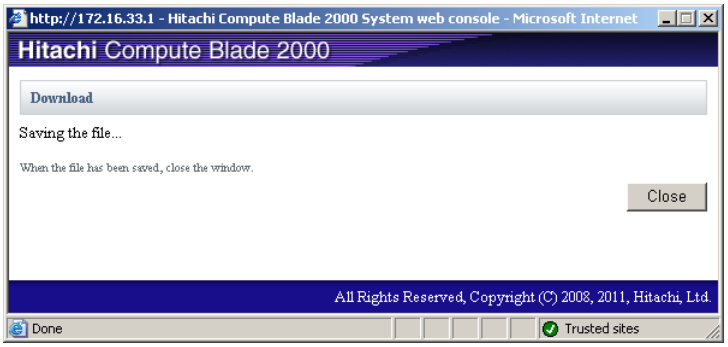


3 In **Backing up the fibre channel settings** on the screen above, select a card type and a partition, and click **List**.

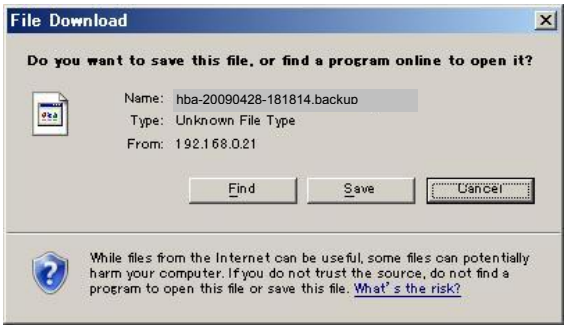
4 The following list including backup files that can be saved will appear.



5 Select a file to backup, and click **Backup**. The following window appears. Download will start in about a minute. Do not close the window before the download has completed, although you can close it by clicking **Close**.



6 When the file is ready to download, the following dialog box appears. Click **Save**.



7 Select a destination to save the backup file.
Backup file name is “hba-YYYYMMDD-hhmmss.backup” (for Hitachi 16 Gb fibre channel mezzanine card, hba16-YYYYMMDD-hhmmss.backup) by default, which can be changed. Enter a file name and then select **Save**. Download will start.

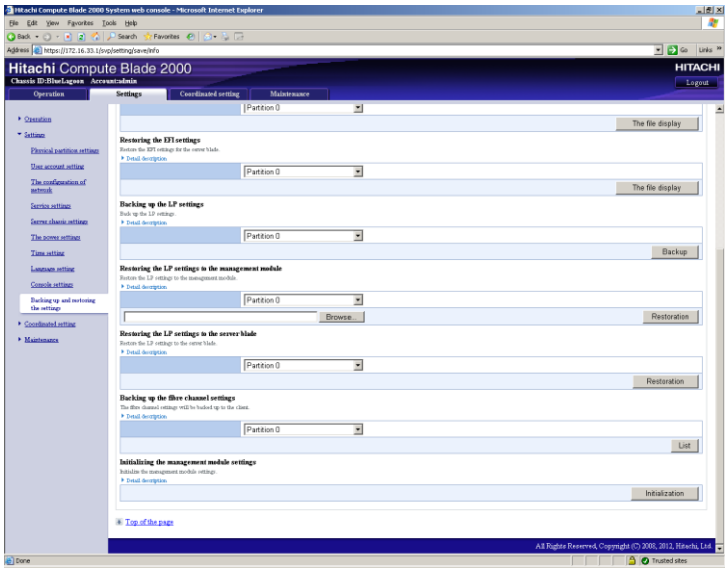
8 After the download has been completed, close the window.

Tip The backup file of the Fibre-channel card configuration saved with the management module can be restored with tools for restoration or tools on the OS.

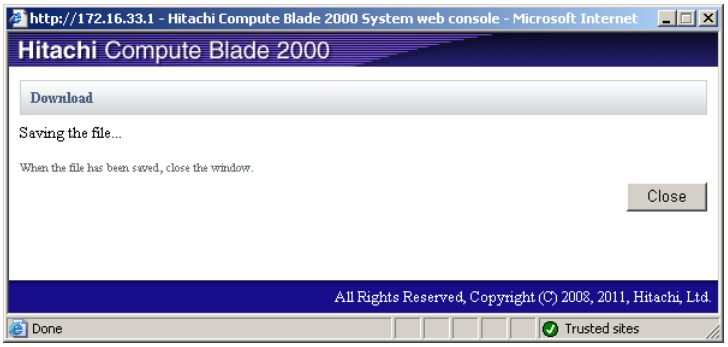
Backing up the LPAR manager settings

1 Log in to the web console as Administrator.

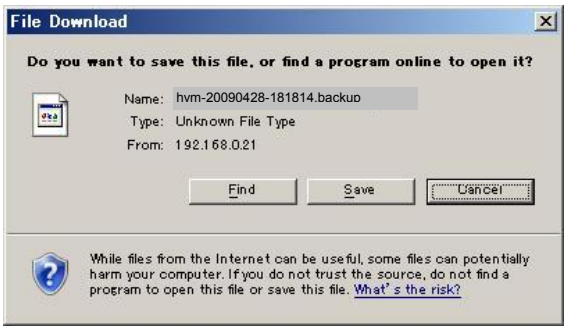
2 Select **Settings** and then **Backing up and Restoring the Settings** from the tree menu.



3 In **Backing up the LPAR manager settings**, select a partition for backup from the pull-down menu, and click **Backup**. The following window appears. Download will start in about five minutes. Click **Close** *only* after the download has been completed.



4 When the file is ready to download, the following dialog box appears. Click **Save**.



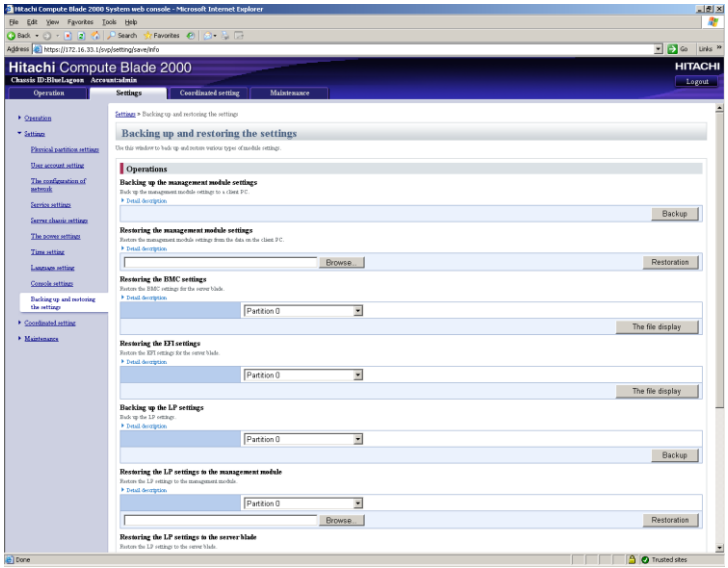
5 Select a destination to save the backup file.
The backup file name is “hvm-YYYYMMDD-hhmmss.backup” by default, which can be changed. Enter a file name and then select **Save**. Download will start.

6 After the download has been completed, close the window.

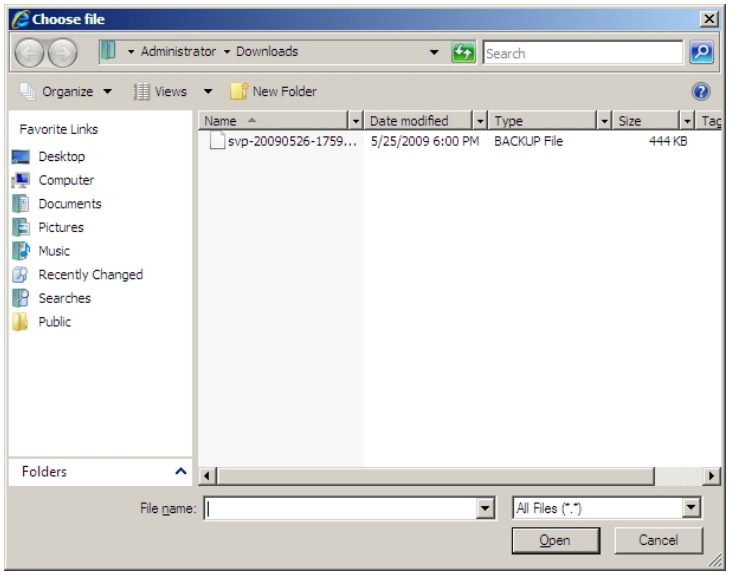
Restoring the LPAR manager settings to the management module

1 Log in to the web console as Administrator.

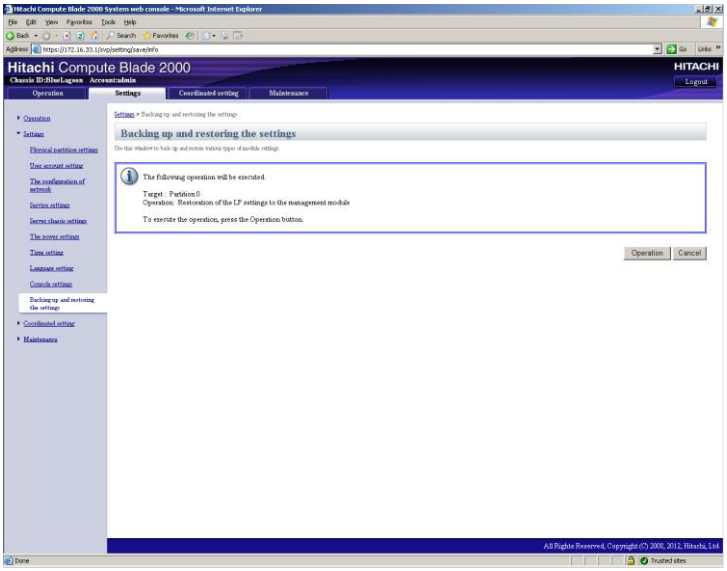
2 Select **Settings** and then **Backing up and Restoring the Settings** from the tree menu.



3 Click **Browse** in the item **Restoring the LPAR manager settings to the management module** and select a backup file for restoration.



4 Confirm that the backup file name is correct. Select the resource partition from the pull-down menu, and click **Restoration**. The following screen appears:

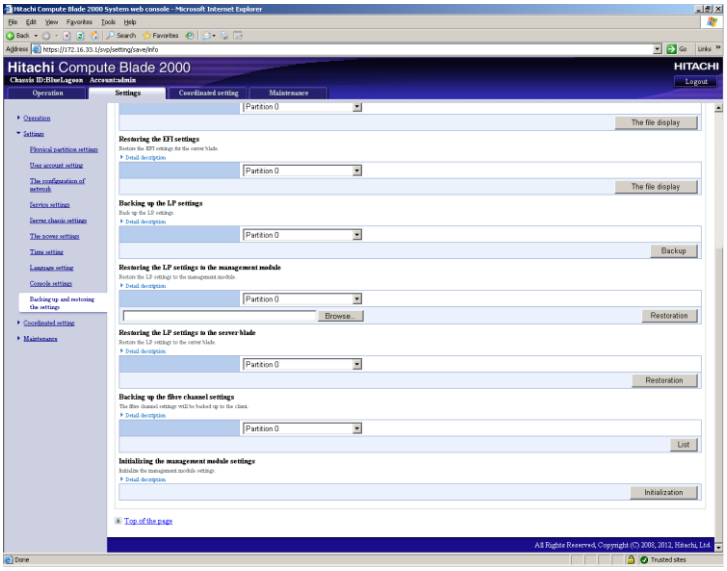


5 Click **Operation** on the above confirmation screen. The management module configuration will be restored. The screen returns to the **Backup or Restoration of the configuration** screen.

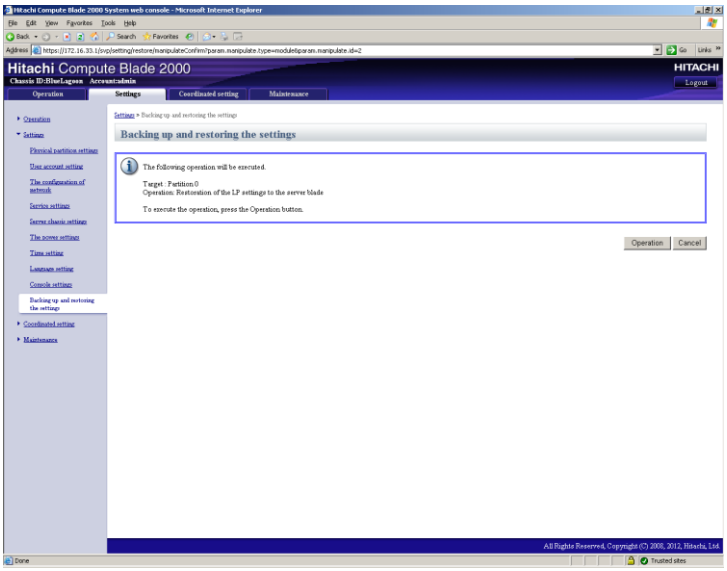
Restoring the LPAR manager settings to the server blade

1 Log in to the web console as Administrator.

2 Select **Settings** and then **Backing up and Restoring the Settings** from the tree menu.



3 In the Restoring the LPAR manager Settings to the server blade, select a partition for backup from the pull-down menu, and click **Restoration**. The following window appears:



4 Click **Operation** on the above confirmation screen. The LPAR manager configuration will be restored into the server blade. The screen returns to the **Backup or Restoration of the configuration** screen.

Tip The restoration of LPAR manager configuration to the server blade can be executed with the LPAR manager Maintenance Tool.

Account

Account overview

❑ Purpose of account

To use the console functions of the management module, you need to set accounts for the following purposes:

(1) To log in the console

When logging in the system console or system web console, you can set or operate functions.

To prevent incorrect login, you have to type the corresponding password to each account to log in. Since multiple accounts can be set, some people can log in with their own account.

(2) To send and receive files with File Transfer Protocol (FTP) protocol

You can send and receive files to/from the user directory using FTP protocol with the management module. To use this function, you need to type your account and password.

❑ Account specifications

The following table shows the account specifications registered in the management module. You need to set the following items for the account setting.

#	Item	Description
1	Account name	- A user account name It can contain up to 32 characters with the following conditions: First character: Alphabetic character Second and subsequent characters: Alphanumeric characters, hyphens (-), underscores (_), and periods (.).
2	Status	Indicates whether a user account is enabled or disabled. Set as: Enabled or Disabled. With Enabled, the account is available.
3	Role	Role names assigned to an account. See Privilege and role for the details of Role.
4	Type of text-based console	Type of the text-based console to be used with an account. Only the system console at present.
5	Type of prompt	Type of a prompt displayed Select one from “SVP>” fixed and “chassis ID (a slot number of the management module) SVP>”.
6	Timeout minutes	Time to wait until automatic logout occurs when you logs in the console but do nothing. The wait time can be set in minutes from 0 to 1440 for the system console; from 1 to 1440 for the system Web console. If 0 is set, however, the automatic logout function is disabled.
7	Password	A password required for login It can contain up to 32 printable characters (*1). Keep your password somewhere because a password string is not displayed on the screen.
8	SSH public	Public keys recorded in an account

#	Item	Description
	key	Record this key to log in with authentication using a public key. Up to five public keys can be assigned to one account. The key algorithm supports RSA (the first public key cryptosystem) and digital signature algorithm (DSA). It is recommended that the key length should be 1024 bits or over. Public keys must be recorded after an account has been set.

*1: American Standard Code for Information Interchange (ASCII) characters from character codes 0x20 to 0x7e.

❑ Account setting

You can use the system console or system Web console to set accounts. For procedures, see SO command for the system console; “User Account Settings” for the system web console.

Privilege and role

Privilege, role, and account

Using the management module console function, you can define a role with specified privileges by adding or removing each privilege for your user management. The following table describes privileges that can be set to a role.

Privilege List

#	Privilege	Description
1	Chassis	Can set and operate a chassis.
2	Network	Can set network.
3	Switch	Can set and operate a switch module. Each slot has individual privilege.
4	Partition	Can set and operate a partition. Each partition has individual privileges.
5	Account	Can add and delete Account or Role.

The following role account is set during shipment.

Defined Roles at the shipment

#	Role name	Privilege				
		Account	Chassis	Network	Switch module	Partition
1	Administrator	Permitted	Permitted	Permitted	Permitted: all slots	Permitted: all partitions

Defined Account at the shipment

#	Account name	Default password	Assigned role	Description
1	administrator	password	Administrator	System manager with all privileges

System console command reference

Command list

1 Basic operation

Command	Description	See page:
EX	Finishes the system console.	457
HE	Help	458
SCO	Console setting	459
WHO	Session information	460
CHCO	Connects the console to a partition or a switch module.	461

2 Chassis management

Command	Description	See page:
CI	Chassis ID setting	462
SD	Time setting	463
SDN	Shutdown the equipment	466
PS	Displays status of all modules.	467
PSV	Power saving setting	472
DF	Displays modules installed in the equipment.	474
DH	Displays the relation between partitions and IO board modules	479
WWN	Sets WorldWideName.	480
PSM	Displays and sets the power module status	490
MMC	Operates the management module.	494
FAN	Displays the FAN module status.	497
DL	Log	498
DEL	Deletes files in the user directory of the management module.	515
FV	Displays the firmware version.	516
FW	Displays the firmware version of the management module and the state of equipment parameter application.	519
LM	Sets a language to use onscreen.	522
ELI	Displays a license: Not available in this equipment.	523
SBC	Operates server blades	523
MAC	Sets a MAC address.	523

3 Partition management

Command	Description	See page:
PR	Partition setting	528
PC	Partition operation	537
UTL	Sets the power-on deterrence to a partition.	542

4 Network management

Command	Description	See page:
LC	Management network setting	543
LFT	Redundant setting for LAN	561
LS	Displays MAC address.	563
XD	Network diagnosis	565
MLC	Reference for maintenance network setting	566
ILC	Internal LAN setting	567

5 External server connection management

Command	Description	See page:
BSM	SC/BSM cooperation setting	569
SNM	SNMP setting	574
MI	E-mail setting	581
HA	HA monitor setting: Not available in this equipment.	595
LDAP	LDAP setting	595
HCSM	HCSM (Hitachi Compute Systems Manager)	600
ST	Syslog transfer setting	607

6 Security management

Command	Description	See page:
CER	Operates SSH public keys and certificates.	609
SEC	Security setting	619
SO	Role and account setting	623
SC	Sets security strength levels and enables/disables a TSL version.	634

7 Switch module management

Command	Description	See page:
SWC	Switch operation	639

8 Backup and restore the configuration

Command	Description	See page:
DC	Restores to the default setting at the shipment	643
UBR	Backups and restores each module configuration.	645

Basic operation

To enter a command to the management module, press **Enter**.

When an option in parentheses is displayed, characters in parentheses can be entered.

Q means that the screen goes to the prompt or returns to the previous menu.

Unchange means that you do not change it.

Input characters in brackets means that you can input the value by just pressing **Enter**.

Prompt is displayed in the following composition.

```
Chassis ID (the slot number of the management module that
currently logs in)SVP>
```

Example: the slot number is 0 of the management module that logs in with Chassis ID 5713RF0 NNNNN:

```
5713RF0 NNNNN(0)SVP>
```

❑ EX command

```
5713RF0 NNNNN(0)SVP> EX (Enter)
[the screen is cleared.]
<<System Console Main Menu>>

  P. Start OS console session.
 SW. Start switch module console session.
  S. System command mode.
  X. Exit.
(P, SW, S, X):
```

To disconnect, select **X. Exit** in this screen.

❑ HE command

You can show a feasible command list in this session. Enter `HE` to the prompt and press **Enter**. Displayed commands depend on the privilege assigned to a role. The following figure is an example, which may different from the actual screen.

```
5713RF0 NNNNN(0)SVP> HE (Enter)

<<HE - Help.>>

BSM  - SC/SBM setting.
CER  - Public key.
CHCO - Change console.
CI   - Chassis ID.
DC   - Restore factory setting.
DEL  - Delete copy of log.
DF   - Show field replaceable unit information.
DH   - Show connection of I/O board module and partition.
DL   - Log.
EX   - Exit.
FAN  - FAN module.
FV   - Show firmware version.
HA   - HA monitor setting.
HE   - Help.
ILC  - Internal LAN setting.
LC   - LAN configuration.
LFT  - Link Fault Tolerance setting.
LM   - Language Mode.
LS   - LAN controller discriminating information.
MI   - E-mail notification.
MLC  - Maintenance LAN setting.
MMC  - Management module control.
PC   - Partition control.
PR   - Physical partition setting.
PS   - Show power and other sensors.
PSM  - Power supply module.
PSV  - Power saving setting.
SCO  - Setting console.
SD   - Edit local time, time zone and NTP.
SDN  - System shutdown.
SEC  - Service setting.
SNM  - SMNP setting.
SO   - Security setting.
SWC  - Switch module control.
UBR  - Backup and restore setting.
UTL  - Utility.
WHO  - Show who is logged on.
  - World wide name.
XD   - Execute diagnostics.

5713RF0 NNNNN(0)SVP>
```

❑ SCO command

You can show and set the inactivity timer and serial connection. Enter `SCO` to the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SCO (Enter)

<<SCO -Setting console.>>

-- Current session setting --
Inactivity timer (min): 10

-- Serial console setting --
Baud rate (bps)        : 9600
Serial console         : Management module

-- Console setting menu --
   I. Set inactivity timer.
   B. Set baud rate.
   P. Set serial port connection.
   Q. Quit.
(I, B, P, [Q]):
```

Select a menu you require from the following list, and execute it.

Menu		Description
I.	Set in activity timer	Sets the inactivity timeout period.
B.	Set baud rate.	Sets the baud rate of a serial port.
P.	Set serial port connection.	Sets the destination for a serial port.
Q.	Quit	Quits the SCO command.

The current setting, the session information that you currently log in, is shown in the following list.

Item	Description of item	Value	Description of value
Inactivity timer	Monitoring timer for inactivity	0 to 1440	Integers from 0 to 1440 can be specified. Unit: minute Setting “0” cancels the timer, and timeout for inactivity is not executed.

The serial console setting, the console information on serial connection, is shown in the following list.

Item	Description of item	Value	Description of value
Baud rate	The baud rate of the serial console for the management module	9600	Can Select a baud rate among the three: 9600 bps, 38400 bps, and 115200 bps.
		38400	
		115200	
Serial console	The destination for a serial port	Management module	Can switch destinations to connect the serial port to: the management

Item	Description of item	Value	Description of value
		Switch module0 to Switch module 9	module or switch module. For switch module, a slot number is specified.
		Unknown	

❑ WHO command

The following figure shows information on a user who currently logs in. Enter `WHO` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> WHO (Enter)

<<WHO - Show who is logged on.>>

No. Name            Role  Login              Access    IP address
-- ---------------- ----- ---------------- -------- ----------
0   administrator   0    2009-03-02 10:37:30 SSH   192.168.0.200
1   MailServerAdmin 1    2009-03-02 10:20:12 SSH   192.168.0.210

-- Session menu --
D. Disconnect user.
Q. Quit.
(D,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
D.	Disconnect User.	Disconnects a user who currently logs in.
Q.	Quit	Quits the WHO command.

The information on the user currently logged in is shown in the following list.

Item	Description of item	Value	Description of value
No.	Serial number of sessions during the user login	0 to 21	
Name	Account name	Character string in ASCII	Comprised of up to 32 characters.
Role	Role ID	Integer	Role ID: from 0 to 23
		MNT	Maintenance personnel
Login	Login time	YYYY-MM-DD hh:mm:ss	YYYY: A. D.; MM: month; DD: day; hh: hour; mm: minute; ss: second
Access	Type of connection	Serial	Serial connection
		Telnet	Telnet connection
		SSH	SSH connection

Item	Description of item	Value	Description of value
		HTTP	HTTP connection: System Web console
		HTTPS	HTTPS connection: System Web Console
IP address	A user IP address	Type of IP address	A user IP address has been connected via LAN
		----------	Connected from a serial port.

❑ CHCO command

You can execute console connection to a partition or switch module. Enter `CHCO` to the prompt, and press **Enter** key.

```
5713RF0 NNNNN(0)SVP> CHCO (Enter)

<<CHCO - Change console.>>

-- Console menu --
  P. Start OS console session.
 SW. Start switch module console session.
  Q. Quit.
(P, SW, [Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
P.	Start OS console session.	Starts the OS console.
SW.	Start switch module console session.	Starts the switch module console.
Q.	Quit	Quits the CHCO command.



When you operate from the console terminal connected to the serial port of the management module, a break signal sent from the terminal software cannot reach the server blade or switch module.

Send a break signal from the console terminal connected to the LAN port of the management module. To connect to the OS console, it is recommended that you use the procedure OS Console > Server Blade Operation in Chapter 13.

Chassis management

❑ CI command

You can display and set a chassis ID with this command. Enter `CI` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> CI (Enter)

<<CI - Chassis ID.>>

Chassis ID : 5713RF0 NNNNN
-- Chassis ID menu --
   C. Edit chassis ID.
   Q. Quit.
(C,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
C.	Edit chassis ID.	Sets a chassis ID.
Q.	Quit	Quits the CI command.

The following table describes the displayed item.

Item	Description of item	Value	Description of value
Chassis ID	Chassis ID	Up to 20 ASCII characters	Identifier for a chassis. The default value is the chassis serial number.

❑ SD command

You can display and set time. Enter `SD` to the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SD (Enter)

<< SD - Edit local time, time zone and NTP. >>

-- Local time --
Date : 2009-03-02
Time : 09:37:50

-- Time zone and Daylight Saving Time --
Time zone      : +09:00
DST            : Disable
DST start time : -------
DST end time   : -------

-- Time synchronization --
NTP   : Enable

-- NTP server --
<NTP0>
Hostname : ------
Status   : Not connect
<NTP1>
Hostname : ------
Status   : Not connect
<NTP2>
Hostname : ------
Status   : Not connect
<NTP3>
Hostname : ------
Status   : Not connect

-- NTP disconnection alert policy --
Policy : Immediately

-- Time setting menu --
    L. Edit local time.
    Z. Edit time zone and Daylight Saving Time.
    S. Edit synchronization setting.
    N. Edit NTP server setting.
    R. Restart NTP service.
    D. Edit NTP disconnection alert policy setting.
    Q. Quit.
(L,Z,S,N,R,D,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
L.	Edit local time.	Sets time of day.
Z.	Edit time zone and Daylight Saving Time.	Sets a time zone and Daylight Saving Time.
S.	Edit synchronization setting.	Sets time synchronization setting.
N.	Edit NTP server setting	Sets Network Time Protocol (NTP) server.
R.	Restart NTP service.	Restarts NTP service running at management module.
Q.	Quit	Quits the Setting Date (SD) command.

Local time information on the management module is described in the table below.

Item	Description of item	Value	Description of value
Date	Local date	YYYY-MM-DD	YYYY: AD year; MM: month; DD:day
Time	Local time	hh:mm:ss	hh: hour; mm:minute; ss: second

Time zone and DST (Daylight Saving Time) information on the management module is described in the table below.

Item	Description of item	Value	Description of value
Time zone	-	from –12:00 to +14:00	Time difference from Coordinated Universal Time (UTC)
DST	Daylight Saving Time	Enable	The daylight saving time setting is enabled.
		Disable	The daylight saving time setting is disabled.
DST start time	When DST starts.	MMM ZZZZZ hh:mm	The time to start DST MMM: the first 3 characters of a month (ex. Apr, Oct) ZZZZZ: start date (hh: hour; mm: minute)
DST end time	When DST finishes.	MMM ZZZZZ hh:mm	The time to finish DST MMM: the first 3 characters of a month (ex. Apr; April; Oct: October) ZZZZZ: end date (hh: hour; mm: minute)

Details of DST are described in the following list.

Item	Description of value
Y	What number day in the month.
lastXXX	The last day of a week in the month: XXX is 3 characters to show a day of a week. (ex. Sun, Mon, Tue, etc.)
XXX>=Y	The first XXX after the Y in the month: XXX is 3 characters to show a day of a week. (ex. Sun, Mon, Tue, etc.)
XXX<=Y	The last XXX before the Y in the month: XXX is 3 characters to show a day of a week. (ex. Sun, Mon, Tue, etc.)

Time synchronization information by NTP is described in the table below.

Item	Description of item	Value	Description of value
NTP	Time synchronization by NTP	Enable	The setting of time synchronization by NTP enabled.
		Disable	The setting of time synchronization by NTP disabled.

NTP server information is described in the table below.

Item	Description of item	Value	Description of value
No.	NTP server number	NTP0 to NTP3	Up to 4 NTP servers can be registered.
Hostname	NTP server address	Domain name	FQDN for NTP servers: displays up to 127 characters as ASCII code.
		IP address	IP address for NTP servers
		-------	No NTP server is set.
Status	Connection status to NTP server	Not connect	Connection is unavailable.
		Connect	Connection is available but the NTP server is not synchronized: a server with higher priority exists.
		Sync	Connection is available and the NTP server is synchronized.
		Unknown	Connection status is unknown.
		-------	No NTP server is set.



With the following conditions, time synchronization is not available:

- NTP server address is specified as the domain name.
- The management module with time synchronization by NTP enabled cannot be connected to the DNS server.
- If you enter 128 or more characters as an NTP server address, Internal error message appears and setting fails.

NTP disconnection alert policy is described in the table below.

Item	Description of item	Value	Description of value
Policy	Policy on alerting disconnection from a NTP server	Immediately	Immediately determines and alerts disconnection.
		x minutes being disconnected	Determines and alerts disconnection in x minutes after disconnected. Values (x): 1 to 1440 minutes
		Disable	Not alerts if disconnected.

❑ SDN command

You can shut down the system. Enter `SDN` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SDN (Enter)

<< SDN - System shutdown. >>

-- Shutdown menu --
  S. Shutdown system.
  Q. Quit.
(S,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
S.	Shutdown system.	Shuts down the system.
Q.	Quit	Quits the SDN command.

❑ PS command

Status of all modules is displayed. Enter `PS` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> PS (Enter)

<< PS - Show power and other sensors. >>

-- Sensor menu --
   C. Show information of server chassis.
   M. Show sensors of management module.
   P. Show sensors of partition.
   SW. Show sensors of switch module.
   PS. Show sensors of power supply module.
   F. Show sensors of fan module.
Q. Quit.
```

Select a menu you require from the following list, and execute it.

Menu		Description
C.	Show information of server chassis.	Displays the server chassis.
M.	Show sensors of management module.	Displays sensors of the management module.
P.	Show sensors of partition.	Displays sensors of the partition.
SW.	Show sensors of switch module.	Displays sensors of the switch module.
PS.	Show sensors of power supply module.	Displays sensors of the power supply module.
F.	Show sensors of fan module.	Displays sensors of the fan module.
Q.	Quit	Quits the PS command.

If you enter `C` in the **PS command** menu and press **Enter**, the server chassis information is displayed. The screen display may be different depending on your configuration.

```
-- Current data of Server chassis --
Name : GVX-RE2A1X11
Nameplate Power : 1023(W)
Present AC Power : 1327(W)
Present DC Power : 1109(W)
Average DC Power : 1110(W)
Maximum DC Power : 1119(W)
Minimum DC Power : 1103(W)
Airflow Volume : 10.91(m^3/min)
Current Power Cap : -----------
Minimum Power Cap : 973(W)
```

If you enter M in the **PS command** menu and press **Enter**, the management module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Management module0 --
Temperature : 38.00(degrees C)
3.3V : 3.30(V)
2.5V : 2.52(V)
1.8V : 1.84(V)
1.2V : 1.19(V)
12.0V : 12.21(V)

-- Current data of Management module0 --
Name : GVX-BE2MNG1X1
Slot : 0
Nameplate Power : 25(W)
Average Power : 25(W)
Maximum Power : 25(W)
Minimum Power : 25(W)
```

If you enter P in the **PS command** menu and press **Enter**, the partition information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Partition4 --
-- Server blade4 --
MB0 CPU0 TEMP : -24.00(degrees C)
MB0 CPU1 TEMP : -25.00(degrees C)
MB0 INTAKE TEMP : 28.00(degrees C)
MB0 CPU0 VCCP : 1.07(V)
MB0 CPU1 VCCP : 1.06(V)
MB0 CPU0 VTT : 1.11(V)
MB0 CPU1 VTT : 1.14(V)
MB0 CPU0 1.5V : 1.50(V)
MB0 CPU1 1.5V : 1.49(V)
MB0 12V : 11.97(V)
MB0 3.3V : 3.27(V)
MB0 1.5V : 1.50(V)
MB0 1.1V : 1.08(V)
MB0 3.3VSB : 3.30(V)
MB0 1.8VSB : 1.78(V)
MB0 BAT 3V : 3.20(V)
MB0 HDDBP 12V : 11.94(V)
MB0 HDDBP 5V : 4.98(V)
MB0 MEZZ0 3.3V : 3.25(V)
MB0 MEZZ0 2.5V : 2.50(V)
MB0 MEZZ0 1.8V : 1.78(V)
MB0 MEZZ0 1.0V : 0.98(V)
MB0 MEZZ1 3.3V : 3.25(V)
MB0 MEZZ1 2.5V : 2.48(V)
MB0 MEZZ1 1.8V : 1.79(V)
MB0 MEZZ1 1.0V : 0.99(V)

-- Current data of Partition4 --
Name(Server blade4) : GVxE55A1-xxxxxxx
Nameplate Power : NO DATA
Present Power : 245(W)
Average Power : NO DATA
Maximum Power : NO DATA
Minimum Power : NO DATA
Current Power Cap : -----------
Minimum Power Cap : NO DATA
Current CPU Speed : NO DATA
Maximum CPU Speed : NO DATA
```

If you enter SW in the **PS command** menu and press **Enter**, the switch module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Switch module1 --

-- Current data of Switch module1 --
Name : GVX-BE2LSW1X1
Slot : 1
Nameplate Power : 60(W)
Average Power : 60(W)
Maximum Power : 60(W)
Minimum Power : 60(W)
```

If you enter PS in the **PS command** menu and press **Enter**, the power supply module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Power supply module1 --
Ambient : 30.53(degrees C)
Hot spot : 46.84(degrees C)
Exhaust : 44.07(degrees C)
Main 12V : 12.26(V)
Standby 12V : 12.53(V)
Input : 196.00(V)
Main 12V : 49.00(A)
Standby 12V : 0.87(A)
Input : 3.60(A)
FAN : 4260(rpm)

-- Current data of Power supply module1 --
Name : 357-KPA0000000-001
Slot : 1
Total Power : 4008(W)
AC Input Power : 707(W)
DC Output Power : 601(W)
```

If you enter F in the **PS command** menu and press **Enter**, the fan module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Fan module3 --
Temperature : 31.50(degrees C)
Voltage : 12.01(V)
Current : 4.10(A)
FAN0 : 6375(rpm)
FAN1 : 6716(rpm)
FAN2 : 6844(rpm)

-- Current data of Fan module3 --
Slot : 3
Nameplate Power : 46(W)
Average Power : 46(W)
Maximum Power : 46(W)
Minimum Power : 46(W)
```

❑ PSV command

You can set and display the power saving information. Enter `PSV` to the prompt, and press **Enter**.

```
<< PSV - Power saving setting. >>

-- Power saving setting menu -
    S. Show power saving setting.
    C. Edit server chassis power cap setting.
    P. Edit partition power cap setting.
    O. Edit order to power off.
    Q. Quit.
(S,C,P,O,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
S.	Show power saving setting.	Displays information on power saving.
C.	Edit server chassis power cap setting	Sets the power capping in a server chassis.
P.	Edit partition power cap setting	Sets the power capping in a partition.
O.	Edit order to power-off.	Sets the partition order to power-off when the power supply capacity is exceeded.
Q.	Quit	Quits the PSV command.

Server chassis power cap information is described in the table below.

Item	Description of item	Value	Description of value
Power cap	Control of maximum power consumption	Enable	Power capping function is enabled.
		Disable	Power capping function is disabled.
Upper limit	Maximum power consumption by a server chassis	-------	The value is not set.
		Integer	Maximum value of power consumption. Unit: watt

Partition power cap information is described in the table below.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Power cap	Power capping function of the server blade that belongs to a partition	-------	No server blade slot that belongs to a partition. (Only current) No server blade that belongs to a partition is installed.
		Enable	Power capping is enabled.
		Disable	Power capping disabled.
Mode	Control mode of power capping	-------	No server blade slot that belongs to a partition. (Only current) No server blade that belongs to a partition is installed. When power capping is disabled.
		Static	Static control
		Dynamic	Dynamic control
Upper limit	Maximum value of power consumption by the server blade that belong to a partition	-------	No server blade slot that belongs to a partition No setting value is set.
		Integer	Maximum power consumption value (Unit: watt)
Exception handling	Exceptional processing	-------	No server blade slot that belongs to a partition.
		Warning only	Only warning when the maximum power consumption value defined by a user is exceeded.
		Warn & Set Frequency	Warning and lowering the central processing unit (CPU) frequency forcibly when the maximum power consumption value defined by a user is exceeded.

Priority order to power-off when the maximum power consumption is exceeded is described in the table below.

Item	Description of item	Value	Description of value
Order	Priority order	Integer	Partition priority order to turn off power when the maximum power consumption is exceeded. Power-off begins with partition #1 in numerical order. This setting is available regardless of whether or not a partition exists or blade is installed.
P	Partition number	0 to 7	-

❑ DF command

Information on modules in the system is displayed. Enter **DF** to the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> DF (Enter)

<< DF - Show field replaceable unit information. >>

-- Detail field replaceable unit information menu --
C. Server chassis.
M. Management module.
S. Server blade.
I. I/O board module.
SW. Switch module.
PS. Power supply module.
T. Show mass of modules.
A. All module.
Q. Quit.
(C,M,S,I,SW,PS,T,A,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
C.	Server chassis.	Displays information on a server chassis.
M.	Management module	Displays information on a management module.
S.	Server blade.	Displays information on a server blade.
I.	I/O board module.	Displays information on an I/O module.
SW.	Switch module.	Displays information on a switch module.
PS.	Power supply module.	Displays information on a power supply module.
T.	Show mass of modules.	Displays information on mass.
A.	All module.	Displays information on all modules.
Q.	Quit	Quits the DF command.

If you enter C in the **DF command** menu and press **Enter**, information on the server chassis is displayed. The screen display may be different depending on your configuration.

```
--- Server chassis ---
Part/Model Number : GVX-RE2A1X11
Serial Number     : 5713RF0 00108
Model ID          : BladeSymphony 2000 (00)
Backplane ID      : Basic model (00)
Chassis ID        : Chassis-7
```

If you enter M in the **DF command** menu and press **Enter**, information on the management module is displayed. The screen display may be different depending on your configuration.

```
--- Management module ---
Slot          : 0

-- Board information --
Manufacturer  : HITACHI
Product Name  : HBS03-ZA
Serial Number : 851590

-- Product information --
Manufacturer      : HITACHI
Product Name      : Management Module
Part/Model Number : GVX-BE2MNG1X1
Serial Number     : 851590

-- MultiRecord information --
Manufacturer ID   : 000074
Module Type1      : 04
Module Type2      : 00
```

If you enter S in the **DF command** menu and press **Enter**, information on the server blade is displayed. The screen display may be different depending on your configuration.

```
--- Server blade ---
Slot          : 0

-- Board information --
Manufacturer  : TEST VENDER
Product Name  : X8DTE-HTC01
Serial Number : XXXXXXXX

-- Product information --
Manufacturer          : HITACHI
Product Name          : BladeSymphony E55
Part/Model Number     : GVAE55A1-XXXXXXX
Product Version       : 0020G55100
Serial Number         : 4609QF0 10439

-- MultiRecord information --
Manufacturer ID       : 000074
Module Type1          : 00
Module Type2          : 01
E Type                : 01
Capacity on Demand    : 01
UUID                  : XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

-- Processor information --
Physical Processors   : 2
Physical Cores        : 16
Activated Cores       : 8

-- Memory information --
Physical DIMMs        : 32
Activated DIMMs       : 32

-- LP license information --
LP License         : Not Installed

Hit enter key.
```

LP License is described in the table below:

Item	Description of item	Value	Description of value
LP License	-	Installed	LPAR manager: Installed. LPAR manager model: Unknown.
		Not Installed	LPAR manager: Not installed.
		Essential	LPAR manager: Installed. Essential model: Available.
		Enterprise	LPAR manager: Installed. Enterprise model: Available.
		ERROR	An error occurred when LPAR manager license information was being retrieved.

If you enter [l] in the **DF command** menu and press **Enter**, information on the I/O adapter and the I/O slot expansion unit that connected to the I/O adapter is displayed. The screen display may be different depending on your configuration.

```
--- I/O adapter ---
Slot              : 0

-- Board information --
Manufacturer  : HITACHI
Product Name  : HBS04-AA00
Serial Number : XXXXXXXX

-- Product information --
Manufacturer          : HITACHI
Product Name          : I/O Board Module
Part/Model Number     : GV-BE2CDM1N1
Serial Number         : XXXXXXXX

-- MultiRecord information --
Manufacturer ID       : 000074
Module Type1          : 04
Module Type2          : 00

--- I/O slot expansion unit chassis ---
Part/Model Number : GV0EDW11-224N11N
Serial Number     : XXXXXXXX

-- Server chassis connect port information --
I/O module number                  : 0
Server chassis connect port number : 0
PCI Express expander setting       : 1:8

Hit enter key.
```

If you enter SW in the **DF command** menu and press **Enter**, information on the switch module is displayed. The screen display may be different depending on your configuration.

```
--- Switch module --
Slot      : 0
Type      : 1G LANSW

-- Product information --
Part/Model Number : GVX-BE2LSW1X1
Serial Number     : 000085
```

If you enter **PS** in the **DF command** menu and press **Enter**, information on the power supply module is displayed. The screen display may be different depending on your configuration.

```
-- Power supply module --
Slot : 1

-- Product information --
Manufacturer          : FUJI ELECTRIC
Product Name          : SWR400001-2U
Part/Model Number     : 357-KPA0000000-001
Product Version       :
Serial Number         : 081100132
```

If you enter T in the **DF command** menu and press **Enter**, information on mass is displayed. The screen display may be different depending on your configuration.

```
-- Server chassis --
Total : 103.87(kg)
```

If you enter A in the **DF command** menu and press **Enter**, information on each module and mass is displayed. The screen display may be different depending on your configuration.

```
--- Server chassis ---
Part/Model Number :
Serial Number     :
Model ID          : BladeSymphony 2000 (00)
Backplane ID      : Basic model (00)
Chassis ID        :

(omitted in the middle.)

-- Server chassis --
Total : 94.23(kg)
```

❑ DH command

Connection between the partition and I/O adapter is displayed. Enter `DH` to the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> DH (Enter)

<< DH - Show connection of I/O adapter module and partition. >>

-- I/O adapter connection --
P I Presence
- -- -------------
0  0 Installed
0  1 Installed
1  2 -----------
1  3 -----------
2  4 Installed
2  5 Not Installed
3  6 -----------
3  7 -----------
4  8 Not Installed
4  9 Not Installed
5 10 -----------
5 11 -----------
6 12 -----------
6 13 -----------
7 14 -----------
7 15 -----------

-- I/O board module menu --
   Q. Quit.
([Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
Q.	Quit	Quits the DH command.

Correspondence between I/O adapters and partitions is described in the table below.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
I	Slot number of the I/O adapter	0 to 15	-
Presence	I/O adapter installation	Installed	Installed.
		Not Installed	Not installed.
		-------	Unknown No server blade is installed.

❑ WWN command

You can set and display World Wide Name (WWN). Enter WWN at the prompt, and press **Enter**.

```
<<  - World wide name. >>

-- World wide name menu --
    C. Show current WWN.
    O. Show/Edit original WWN.
    A. Show/Edit additional WWN.
    Q. Quit.
(C,O,A,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
C.	Show current WWN.	Displays information on WWN currently used.
O.	Show/Edit original WWN .	Displays and sets information on the Default Physical WWN.
A.	Show/Edit additional WWN.	Displays and sets information on the Optional Physical WWN.
Q.	Quit	Quits the WWN command.

If you enter C in the WWN command menu, press **Enter**, and select a partition number, Current WWNs are displayed.

```
Select partition (0-7,[Q=Quit]) : 7

-- Current WWN --
P S Card Port World wide port name     World wide node name     Type
- - ---- ---- ------------------------ ------------------------ ---------
-
7 7 MC1     2  24:00:00:00:87:00:01:EC  24:00:00:00:87:00:01:ED
Additional
7 7 MC1     3  24:00:00:00:87:00:01:EE  24:00:00:00:87:00:01:EF
Additional
7 7 IO14    0 *50:00:00:00:87:00:01:F0 *50:00:00:00:87:00:01:F1
Additional
7 7 IO14    1 *50:00:00:00:87:00:01:F2 *50:00:00:00:87:00:01:F3
Additional
7 7 IO14    2 *50:00:00:00:87:00:01:F4 *50:00:00:00:87:00:01:F5
Additional
7 7 IO14    3 *50:00:00:00:87:00:01:F6 *50:00:00:00:87:00:01:F7
Additional
7 7 IO15  --   ----------------------   ----------------------   --------

-- IOEU (I/O slot expansion unit connect adapter 14) --
Part/Model Number : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Serial Number     : xxxxxxxxxxxxxxxxxxx

I  Port World wide port name     World wide node name     Type
-- ---- ------------------------ ------------------------ ----------
 0    0  24:00:00:00:87:00:01:80  24:00:00:00:87:00:01:81 Additional
 0    1  24:00:00:00:87:00:01:82  24:00:00:00:87:00:01:83 Additional
 0    2  24:00:00:00:87:00:01:84  24:00:00:00:87:00:01:85 Additional
 0    3  24:00:00:00:87:00:01:86  24:00:00:00:87:00:01:87 Additional
 1    0  24:00:00:00:87:00:02:80  24:00:00:00:87:00:02:81 Additional
 1    1  24:00:00:00:87:00:02:82  24:00:00:00:87:00:02:83 Additional
 1    2  24:00:00:00:87:00:02:84  24:00:00:00:87:00:02:85 Additional
 1    3  24:00:00:00:87:00:02:86  24:00:00:00:87:00:02:87 Additional
 4    0  24:00:00:00:87:00:03:80  24:00:00:00:87:00:03:81 Additional
 4    1  24:00:00:00:87:00:03:82  24:00:00:00:87:00:03:83 Additional
 4    2  24:00:00:00:87:00:03:84  24:00:00:00:87:00:03:85 Additional
 4    3  24:00:00:00:87:00:03:86  24:00:00:00:87:00:03:87 Additional
 5    0  24:00:00:00:87:00:04:80  24:00:00:00:87:00:04:81 Additional
 5    1  24:00:00:00:87:00:04:82  24:00:00:00:87:00:04:83 Additional
 5    2  24:00:00:00:87:00:04:84  24:00:00:00:87:00:04:85 Additional
 5    3  24:00:00:00:87:00:04:86  24:00:00:00:87:00:04:87 Additional

Hit enter key
```

Information on the WWN currently used is described in the table below: Current WWN.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	FC card type and slot number	ECX	Expansion card
		IOXX	I/O adapter
Port	Port number	0 to 3	-
World wide port name	WWPN	-------	No card is installed.
		XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN equivalent to the initial value
			Default Physical WWN
		*XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN changed from the initial value
		+XX:XX:XX:XX:XX:XX:XX:XX	User Default Physical WWN
World wide node name	WWNN	-------	No card is installed.
		XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN equivalent to the initial value
			Default Physical WWN
		*XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN changed from the initial value
		+XX:XX:XX:XX:XX:XX:XX:XX	User Default Physical WWN
Type	Type of WWN	Additional	Additional
		Original	Original
		-------	Not installed.
		(CONFLICT)	Detected an Optional Physical WWN with the same value as the existing one.

When connected to an I/O slot expansion unit, the unit’s part/model number and serial number, and information on the I/O adapter of the I/O slot expansion unit included in the partition.

If you enter o in the **WWN command** menu and press **Enter**, Default Physical WWNs are displayed.

```
-- Original  menu --
    S. Show.
    Q. Quit.
(S,[Q]) : S

Select partition (0-7,[Q=Quit]) : 7

-- Original  --
P S Card Port World wide port name     World wide node name
- - ---- ---- ------------------------ ------------------------
7 7 MC1     2  24:00:00:00:87:00:01:EC  24:00:00:00:87:00:01:ED
7 7 MC1     3  24:00:00:00:87:00:01:EE  24:00:00:00:87:00:01:EF
7 7 IO14    0  50:00:00:00:87:00:01:F0  50:00:00:00:87:00:01:F1
7 7 IO14    1  50:00:00:00:87:00:01:F2  50:00:00:00:87:00:01:F3
7 7 IO14    2  50:00:00:00:87:00:01:F4  50:00:00:00:87:00:01:F5
7 7 IO14    3  50:00:00:00:87:00:01:F6  50:00:00:00:87:00:01:F7
7 7 IO15  --   ----------------------   ----------------------

-- IOEU (I/O slot expansion unit connect adapter 14) --
Part/Model Number : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Serial Number     : xxxxxxxxxxxxxxxxxxx

I  Port World wide port name     World wide node name
-- ---- ------------------------ ------------------------
 0    0  24:00:00:00:87:00:01:80  24:00:00:00:87:00:01:81
 0    1  24:00:00:00:87:00:01:82  24:00:00:00:87:00:01:83
 0    2  24:00:00:00:87:00:01:84  24:00:00:00:87:00:01:85
 0    3  24:00:00:00:87:00:01:86  24:00:00:00:87:00:01:87
 1    0  24:00:00:00:87:00:02:80  24:00:00:00:87:00:02:81
 1    1  24:00:00:00:87:00:02:82  24:00:00:00:87:00:02:83
 1    2  24:00:00:00:87:00:02:84  24:00:00:00:87:00:02:85
 1    3  24:00:00:00:87:00:02:86  24:00:00:00:87:00:02:87
 4    0  24:00:00:00:87:00:03:80  24:00:00:00:87:00:03:81
 4    1  24:00:00:00:87:00:03:82  24:00:00:00:87:00:03:83
 4    2  24:00:00:00:87:00:03:84  24:00:00:00:87:00:03:85
 4    3  24:00:00:00:87:00:03:86  24:00:00:00:87:00:03:87
 5    0  24:00:00:00:87:00:04:80  24:00:00:00:87:00:04:81
 5    1  24:00:00:00:87:00:04:82  24:00:00:00:87:00:04:83
 5    2  24:00:00:00:87:00:04:84  24:00:00:00:87:00:04:85
 5    3  24:00:00:00:87:00:04:86  24:00:00:00:87:00:04:87

Hit enter key.
```

Select a menu item you require from the following list, and execute it.

Menu		Description
S.	Show	Displays information on Default Physical WWN.
Q.	Quit	Returns to the previous menu.

Information on the on Default Physical WWN is described in the table below.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	FC card type and slot number	ECX	Expansion card
		IOXX	I/O adapter
Port	Port number	0 to 3	-
World wide port name	WWPN	-------	No card installed.
		XX:XX:XX:XX:XX:XX:XX:XX	Default Physical WWN
		+XX:XX:XX:XX:XX:XX:XX:XX	User Default Physical WWN
World wide node name	WWNN	-------	No card installed.
		XX:XX:XX:XX:XX:XX:XX:XX	Default Physical WWN
		+XX:XX:XX:XX:XX:XX:XX:XX	User on Default Physical WWN

When connected to an I/O slot expansion unit, the unit's part/model number and serial number, and information on the I/O adapter of the I/O slot expansion unit included in the partition.

Note

- When a Fibre-channel adapter has two ports, information on four ports is displayed. In this case, the Fibre-channel adapter WWNs are displayed in port0 and port1, and "0" is displayed in port2 and port3 as WWN values.
- For 10 Gb converged network adapter (CNA) adapter or 10 Gb CNA board, the following values are shown.
  - WWN for port 0 is the WWN value for port 0 of the controller 0.
  - WWN for port 1 is the WWN value for port 1 of the controller 0.
  - WWN for port 2 is the WWN value for port 0 of the controller 1.
  - WWN for port 3 is the WWN value for port 1 of the controller 1.

  WWN is shown only when CNA Personality setting is Fibre Channel over Ethernet (FCoE).

  When a single CNA controller is installed, WWN values for port 2 and port 3 are shown as all 0, zero.
- For Emulex 8 Gb 2-port fibre channel mezzanine card, current WWN may be shown in the Default Physical WWN field.
  - Applicable extensible firmware interface (EFI) firmware versions with each server blade model are as follows:
    - All EFI firmware versions with standard server blade X55A1 and X55A2 models
    - All EFI firmware versions with high-performance server blade X57A1 model
    - EFI version 07-29/08-29 or earlier with high-performance server blade X57A2 model
  - To find the Default Physical WWN for Emulex 8 GB 2-port fibre channel mezzanine card, perform the following steps:
    1. Shut down the OS and power off the server blade.
    2. Power on the server blade and boot the OS.
    3. Check the Default Physical WWN without rebooting the OS.



For Fibre-channel mezzanine card, Default Physical WWN may be shown as a value consisting of all zeros.

- How to check Default Physical WWN
  - For Emulex Fibre-channel mezzanine card
    See the *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI edition)* to check it on the BIOS Utility screen.
  - For Hitachi Fibre-channel mezzanine card
    See *HITACHI Gigabit Fibre-channel Adapter User's Guide (BIOS/EFI Edition)* to check it on the SELECT HBA screen.
- Applicable EFI firmware version with each server blade model is as follows:

  - EFI firmware version 09-33/10-33 or earlier with standard server blade X55S3/X55R3 models.

If you enter A in the **WWN command** menu and press **Enter**, Optional Physical WWNs are displayed.

```
-- Additional  menu --
    S. Show.
    I. Initialize.
    E. Edit.
    H. Show change history.
    Q. Quit.
(S,I,E,H,[Q]) : S

Select partition (0-7,[Q=Quit]) : 7

-- Original  --
P S Card Port World wide port name     World wide node name
- - ---- ---- ----------------------- -----------------------
7 7 MC1     2  24:00:00:00:87:00:01:EC  24:00:00:00:87:00:01:ED
7 7 MC1     3  24:00:00:00:87:00:01:EE  24:00:00:00:87:00:01:EF
7 7 IO14    0 *50:00:00:00:87:00:01:F0 *50:00:00:00:87:00:01:F1
7 7 IO14    1 *50:00:00:00:87:00:01:F2 *50:00:00:00:87:00:01:F3
7 7 IO14    2 *50:00:00:00:87:00:01:F4 *50:00:00:00:87:00:01:F5
7 7 IO14    3 *50:00:00:00:87:00:01:F6 *50:00:00:00:87:00:01:F7
7 7 IO15  --   ----------------------   ----------------------

-- IOEU (I/O slot expansion unit connect adapter 14) --
Part/Model Number : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Serial Number     : xxxxxxxxxxxxxxxxxxx

I  Port World wide port name     World wide node name
-- ---- ----------------------- -----------------------
 0    0  24:00:00:00:87:00:01:80  24:00:00:00:87:00:01:81
 0    1  24:00:00:00:87:00:01:82  24:00:00:00:87:00:01:83
 0    2  24:00:00:00:87:00:01:84  24:00:00:00:87:00:01:85
 0    3  24:00:00:00:87:00:01:86  24:00:00:00:87:00:01:87
 1    0  24:00:00:00:87:00:02:80  24:00:00:00:87:00:02:81
 1    1  24:00:00:00:87:00:02:82  24:00:00:00:87:00:02:83
 1    2  24:00:00:00:87:00:02:84  24:00:00:00:87:00:02:85
 1    3  24:00:00:00:87:00:02:86  24:00:00:00:87:00:02:87
 4    0  24:00:00:00:87:00:03:80  24:00:00:00:87:00:03:81
 4    1  24:00:00:00:87:00:03:82  24:00:00:00:87:00:03:83
 4    2  24:00:00:00:87:00:03:84  24:00:00:00:87:00:03:85
 4    3  24:00:00:00:87:00:03:86  24:00:00:00:87:00:03:87
 5    0  24:00:00:00:87:00:04:80  24:00:00:00:87:00:04:81
 5    1  24:00:00:00:87:00:04:82  24:00:00:00:87:00:04:83
 5    2  24:00:00:00:87:00:04:84  24:00:00:00:87:00:04:85
 5    3  24:00:00:00:87:00:04:86  24:00:00:00:87:00:04:87

Hit enter key.
```

Select a menu item you require from the following list, and execute it.

Menu		Description
S.	Show.	Displays information on Optional Physical WWN.
I.	Initialize.	Initializes Optional Physical WWNs.
E.	Edit.	Sets the information on Optional Physical WWNs.
H.	Show change history.	Displays the change history of Optional Physical WWNs.
Q.	Quit	Returns to the previous menu.

Information on the Optional Physical is described in the table below.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	FC card type and slot number	ECX	Expansion card
		IOXX	I/O adapter
Port	Port number	0 to 3	-
World wide port name	WWPN	XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN equivalent to the initial value
		*XX:XX:XX:XX:XX:XX:XX:XX	WWN changed from the initial value.
World wide node name	WWNN	XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN equivalent to the initial value
		*XX:XX:XX:XX:XX:XX:XX:XX	WWN changed from the initial value.
		(CONFLICT)	Detected an Optional Physical WWN with the same value as the existing one.

When connected to an I/O slot expansion unit, the unit's part/model number and serial number, and information on the I/O adapter of the I/O slot expansion unit is included in the partition.

If you enter H in the **Optional Physical WWN** menu and press **Enter**, the change history of Optional Physical WWN is displayed.

```
-- Additional  menu --
I. Initialize.
E. Edit.
H. Show change history.
Q. Quit.
(I,E,H,[Q]) : H (Enter)

Date              P S Card Port   Before                  After                   From
----------------- - - ---- ---- ---- ----------------------- ----------------------- --------
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 IO01  0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 IO01  0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX Console
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM0
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM1
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM2
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM3
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM0
YY-MM-DD hh:mm:ss 0 0 EC1   0   N XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM1
YY-MM-DD hh:mm:ss 0 0 EC1   0   WWPN XX:XX:XX:XX:XX:XX:XX:XX XX:XX:XX:XX:XX:XX:XX:XX BSM2
Hit enter key.
```

The change history of the Optional Physical WWN is itemized in the table below.

Item	Description of item	Value	Description of value
Date	Changed date	YY-MM-DD hh:mm:ss	When the Optional Physical WWN is changed. YY: the last 2 figures of a year; MM: month; DD: day; hh: hour; mm:minute; ss: second
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	FC card type and slot number	ECX	Expansion card
		IOXX	I/O adapter
		IOXX-IOX	I/O adapter on the I/O slot expansion unit. Displays “I/O adapter slot number connected to the I/o slot expansion unit – slot number on the I/O slot expansion unit”.
Port	Port number	0 to 3	-
WWN	World Wide Name	WWNN	World Wide Node Name
		WWPN	World Wide Port Name
Before	WWN before changed	XX:XX:XX:XX:XX:XX:XX:XX	-
After	WWN after changed	XX:XX:XX:XX:XX:XX:XX:XX	-
From	Resource that requests change	BSMX	Change requested from the BSM
		Console	Change requested from the console
		Unknown	Change requested from other then the BSM and console.

❑ PSM command

You can set a power supply module and display the status. Enter `PSM` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> PSM (Enter)

<< PSM - Power supply module. >>

-- Power supply module status --
PS Power                Condition AC input
-- -------------------- --------- --------
0 On                    Normal    Normal
1 On                    Normal    Normal
2 On                    Normal    Normal
3 On                    Normal    Normal

-- Power supply redundancy setting --
Policy : N+1

-- Power supply optimization setting --
Optimization : Enable

-- Power supply AC recovery setting --
PS AC recovery
-- -----------
 0 Enable
 1 Enable
 2 Enable
 3 Enable

-- Power supply module menu --
   R. Edit power supply redundancy setting.
   O. Edit power supply optimization setting.
   P. Show power supply module statistics.
   A. Edit power supply AC recovery setting.
   Q. Quit.
(R,O,P,A,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
R.	Edit power supply redundancy setting.	Sets redundancy in power supply modules.
O.	Edit power supply optimization setting.	Sets power-off into unnecessary power supply modules.
P.	Show power supply module statistics.	Displays information on the power supply module statistics.
A.	Edit power supply AC recovery setting.	Sets the behavior after AC power is restored.
Q.	Quit	Quits the PSM command.

Items of power supply module status are described in the table below.

Item	Description of item	Value	Description of value
PS	Power supply slot number	0 to 3	-
Power	Power status	-------	No power supply module is installed.
		On	The power is on.
		Processing power off	In the process of powering-off.
		Off	The power is off.
		Processing power on	In the process of powering-on
Condition	Status: failure status	-------	No power supply module is installed.
		Normal	No problem
		FAIL	The power supply fails and does not work according to specifications.
AC input	AC input status	-------	No power supply module is installed.
		Normal	AC input exists.
		None	No AC input.

An item of the power supply redundancy setting is described in the table below.

Item	Description of item	Value	Description of value
Policy	Redundancy setting in the power supply module	N+N	N+N redundancy setting (AC input redundancy)
		N+1	N+1 redundancy setting (power supply redundancy)
		Not redundant	Non-redundancy setting
		Unknown	Redundancy setting is unknown.

An item of the power supply optimization setting is described in the table below.

Item	Description of item	Value	Description of value
Optimization	Powering-off unnecessary power supply modules	Enable	Power-off function is enabled.
		Disable	Power-off function is disabled.
		Unknown	The setting value is unknown.
		ERROR	Failed to obtain the value. Unexpected setting value.

Items of power supply AC recovery setting are described in the table below.

Item	Description of item	Value	Description of value
PS	Power supply slot number	0 to 3	-
AC recovery	Power supply AC recovery setting	Enable	The system will be automatically booted when power is restored to the power supply module.
		Disable	The system will not be automatically booted when power is restored to the power supply module.

If you enter R in the **PSM command** menu and press **Enter**, you can change the redundancy setting on the power supply module. The current value and specifiable values are displayed and prompt is ready. Press **Enter** or input a setting value and press **Enter**, and the changed value is displayed. A message to confirm the setting appears and prompt is ready. Input Y and press **Enter**, the redundant setting for the power supply module will be effective.
To cancel the setting change, input N after the confirmation message and press **Enter** key or just press **Enter**.

```
Policy : N+N
(0=N+N,1=N+1,2=Not redundant,[Unchange]) : 1 (Enter)

-- Power supply redundancy setting --
Policy : N+1

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter O in the **PSM command** menu and press **Enter**, you can change the optimization setting. The current setting value and specifiable values are displayed and prompt is ready. Press **Enter** or input a setting value and press **Enter**, and the changed value is displayed. A message to confirm the setting appears and prompt is ready. Input Y and press **Enter**, the optimization setting for the power supply module will be effective.

To cancel the setting change of the optimization function, input N after the confirmation message and press **Enter**, or just press **Enter**.

```
Optimization : Disable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)

-- Power supply optimization setting --
Optimization : Enable

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter P in the **PSM command** menu and press **Enter**, Power cycle count is displayed.

```
-- Power cycle count --
PS Count
-- -------
0         0
1         0
2         0
3       114

Hit enter key.
```

Power cycle count is itemized in the table below.

Item	Description of item	Value	Description of value
PS	Power supply slot number	0 to 3	-
Count	Frequency of power supply module on and off	Integer	How many times each power supply module changes from active to standby.
		-------	No power supply module is installed No privilege to display the power supply module details

If you enter A in the **PSM command** menu and press **Enter**, you can change the power supply AC recovery setting. You are requested to select a power supply module, and the prompt is ready. When you input the number of a power supply, the current setting values and specifiable values are displayed: the prompt is ready. Just press **Enter** or input a setting value and press **Enter**, and the new setting value is displayed. A message appears to confirm the settings, and the prompt is ready. Input Y and press **Enter**, and the new setting value will be effective. To cancel the setting, input N to the confirmation message and press **Enter** or just press **Enter**.

```
Select power supply module (0-3,A=All,[Q=Quit]) : 0 (Enter)

AC recovery  : Enable
(0=Disable,1=Enable,[Unchange]) : 0 (Enter)

-- Power supply AC recovery setting --
PS AC recovery
-- -------
 0 Disable
 1 Enable
 2 Enable
 3 Enable


Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.

Hit enter key. (Enter)
```

❑ MMC command

You can set a management module and display the status. Enter `MMC` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> MMC (Enter)

<< MMC - Management module control. >>

-- Management module status --
M Behavior Power Condition LID lamp
- -------- ----- ------------ --------
0 Active   On    Normal       Off
1 Standby  On    Normal       Off

-- Management module control menu --
   P. Power control.
   L. LID lamp control.
   Q. Quit.
(P,L,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
P.	Power control.	Executes the power operation of the management module.
L.	LID lamp control.	Executes the identification LED of the management module.
Q.	Quit	Quits the MMC command.

Items of management module status are described in the table below.

Item	Description of item	Value	Description of value
M	Management module slot number	0 or 1	-
Behavior	Management module performance	-------	No management module is installed. “Active” undecided Boot is disabled.
		Active	
		Standby	
Power	Power supply status	-------	No management module is installed.
		On	The management module is powered on.
		Off	The management module is powered off.
Condition	Status: Whether or not available for the user operation; FAIL status	-------	No management module is installed.
		Normal	Active; standby
		Booting	Booting now
		Shutting down	Shutting down now
		Boot disable	Boot is disabled.
		FAIL	The module fails.
LID Lamp	Status of the identification LED	-------	No management module is installed. Boot is disabled. Boot of the other module is disabled.
		On	LED lights solid.
		Off	LED is off.

Enter `P` in the **MMC command** menu and press **Enter**. The Power control menu is displayed.

```
(P,L,[Q]) : P (Enter)
-- Management module status --
M Behavior Power Condition     LID lamp
- -------- ----- ------------- --------
0 ------    ---   -----------   ------
1 Active   On    Normal       Off

-- Power control menu --
    S. Shutdown.
    R. Restart.
   SW. Switch active/standby.
    Q. Quit.
(S,R,SW,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
S.	Shutdown.	Shuts down the management module.
R.	Restart.	Restarts the management module.
SW.	Switch active/standby.	Switches between the active and standby management modules.
Q.	Quit.	Returns to the previous menu.

Note

Do not perform Shutdown and Restart on the management module while the server blade is operating. Error events, which have occurred while the management module is restarting or shutting down, may not be detected.

When restarting and shutting down a management module while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

If you enter `L` in the **MMC command** menu and press **Enter**; the identification LED menu is displayed.

```
(P,L,[Q]) : L (Enter)
-- Management module status --
M Behavior Power Condition LID lamp
- -------- ----- ------------ --------
0  ------   ---   -----------   ------
1 Active    On   Normal        Off

-- LID lamp control menu --
   T. Turn on
   F. Turn off
   Q. Quit.
(T,F,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
T.	Turn on	Turns on the identifying LED of the management module.
F.	Turn off	Turns off the identifying LED of the management module.
Q.	Quit.	Returns to the previous menu.

❑ FAN command

You can display the fan module status. Enter `FAN` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> FAN (Enter)

<< FAN - FAN module. >>

-- FAN module status --
F Power                Condition Unit1(rpm) Unit2(rpm) Unit3(rpm)
- -------------------- --------- ---------- ---------- ----------
0 On                   Normal    3000       3000       3000
1 On                   Normal    3000       3000       3000
2 On                   Normal    3000       3000       3000
3 On                   Normal    3000       3000       3000
4 On                   Normal    3000       3000       3000
5 On                   Normal    3000       3000       3000
6 On                   Normal    3000       3000       3000
7 On                   Normal    3000       3000       3000

-- FAN module menu --
   Q. Quit.
([Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
Q.	Quit	Quits the FAN command.

Items of fan module status are described in the table below.

Item	Description of item	Value	Description of value
F	Fan module slot number	0 to 7	-
Power	Power supply status	-------	No fan module is installed.
		On	Power is supplied to the fan module.
		Processing power-off	Power is being turned off.
		Off	No power is supplied to the fan module.
		Processing power-on	Power is being supplied to the fan module.
Condition	Status: FAIL status	-------	No fan module is installed.
		Normal	No problem
		FAIL	The module fails and does not operate as the specifications.
Unit1 (rpm)	Fan 1	-------	Fan 1 is not installed.
		Integer	Revolution per minute of Fan 1 (Unit: rpm)
Unit2 (rpm)	Fan 2	-------	Fan 2 is not installed.
		Integer	Revolution per minute of Fan 2 (Unit: rpm)

Item	Description of item	Value	Description of value
Unit3 (rpm)	Fan 3	-------	Fan 3 is not installed.
		Integer	Revolution per minute of Fan 3 (Unit: rpm)

❑ DL command

You can display logs. Enter `DL` to the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> DL (Enter)

<< DL - Log. >>

-- Log menu --
   S. Show SVP log.
   H. Show HCSM log.
   E. Show system event log.
   D. Dump log to file.
   P. Show power monitoring log.
   M. Show environment monitoring log.
   A. Show management module console access log.
   F. Create error log file.
   I. Show MARLOG.
   C. Show RC list.
   Q. Quit.
(S,H,E,D,R,P,M,A,F,I,C,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
S.	Show SVP log.	Views service processor (SVP) logs.
H.	Show HCSM log.	Views Hitachi Compute Server Manager (HCSM) logs.
E.	Show system event log.	Views system event logs.
D.	Dump log to file.	Creates a log file for a probe to the current system equipment, and saves the file to the user directory in the management module. The file can be downloaded via FTP.
P.	Show power monitoring log.	Views power monitoring logs.
M.	Show environment monitoring log.	Views environment monitoring logs.
A.	Show management module console access log.	Views console access logs.
F.	Create error log file.	Views and creates error logs.
I.	Show MARLOG.	Views maintenance action report (MAR) logs.
C.	Show RC list.	Views the Reference Code (RC) list.
Q.	Quit	Quits the dump log (DL) command.

If you enter S in the **DL command** menu and press **Enter**, SVP logs are displayed.

```
-- SVP log --
Timestamp           ID   Level   Message
------------------- ---- ------- ------------------------------------------
--
2009-03-03 17:05:18 1794 FAIL    Module <Power Supply Module> lacks
redundancy. (SEL=0000024E63AD4961000409320BA5FFFF,SID=,PAR=XX,MTY=05,SLT=00)
2009-03-03 17:05:22 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:08:09 17A9 WARNING Sending out an e-mail report message
failed.(SEL=000002F963AD49610004F2F907A10341,SID=,PAR=XX,MTY=04,SLT=01)
2009-03-03 17:22:22 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:28:06 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:28:21 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:28:33 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:29:18 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:29:18 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:30:05 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:30:12 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:31:08 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:31:08 17E0 Info    The management module sent out a connection
request alert.
2009-03-03 17:31:26 17E0 Info    The management module sent out a connection
request alert.

Hit enter key.
```

Items of the SVP log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (Local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
ID	Log ID (Alert ID)	NNNN	-
Level		Info	Information
		WARNING	-
		FAIL	-
Message	Event message	Character string	Displayed in ASCII.

If you enter H in the **DL command** menu and press **Enter**, HCSM logs are displayed.

```
-- HCSM log -

Timestamp           ID   Level   Message
------------------- ---- ------- ------------------------------------------
2012-04-25 12:13:59 FD91 Info    Server is powered off.(Location:Partition
1)
2012-04-25 12:13:55 FD31 Info    Module is removed.(Location:Server Blade 4)
2012-04-25 12:13:58 FD31 Info    Module is removed.(Location:Server Blade 1)
2012-04-25 12:30:33 FD00 WARNING Temperature of chassis became warning
level.(Temp(Upper),Location:Switch Module 3 - IOSW3 TEMP)
Hit enter key.
```

Items of the HCSM log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (Local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
ID	Log ID (Alert ID)	NNNN	-
Level	-	Info	Information
		WARNING	-
		FAIL	-
Message	Event message	Character string	Displayed in ASCII.

If you enter E in the **DL command** menu and press **Enter**, system event logs are displayed.

```
Select module (P=Partition,M=Management module,A=All,[Q=Quit]) : A (Enter)

-- System event log --
Timestamp           Module Level   System event log              Message
------------------- ------ ------- ------------------------------
2009-03-09 18:50:47 M1     Info    0000 02 6100 04 1D15 6FA1FFFF Management
Module#1: General Reset
2009-03-09 18:50:47 M1     Info    0001 02 6100 04 F2F9 07A80B00 Management
Module#z: In operation as master
2009-03-09 18:50:47 PS0    FAIL    0002 02 6100 04 0932 0BA5FFFF Power
Supply module#z: Operated without Redundancy (<N)
2009-03-09 18:53:05 M1     Caution 0003 02 6100 04 F2F9 07A10341 Email
notification: failure

Hit enter key.
```

Items of the system event log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Module	Where the event occurs	PX	PartitionX
		MX	SVPX
		SWX	Switch module
		IOXX	I/O board module
		PSX	Power supply module
		FANX	Fan module
		ETC	Others including “Unknown”
Level		Info	Information
		Caution	
		WARNING	
		FAIL	
System event log	Event data	IIII RR gggg ee ssSS ee11223344	IIII: Record ID RR: Record type gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3
Message	Event message		Displayed in ASCII.

If you enter `D` in the **DL command** menu and press **Enter**, you are required to select a module for data collection: the prompt is ready. Select a module for data collection, and a message to confirm the data collection: the prompt is ready. If you select the physical partition, input the physical partition number. Input `Y` and press **Enter**, and the log file data for a probe start to be created. To cancel creating the data file for a probe, input `N` after the confirmation message and press **Enter** or just press **Enter**.

```
Select module (P=Partition,M=Management module,A=All,[Q=Quit]) : A (Enter)

WARNING : If confirm, it will take few minutes to dump log to file.

Confirm? (Y,[N]) : Y (Enter)
- Dumping log to file was completed.
- File name is "mm-20090303-184046.dmp".
Hit enter key. (Enter)
```

It takes a few minutes to create a log data file for a probe. When it is completed, the file name is displayed: the prompt is ready. Press **Enter**, and the screen returns to **the DL command** menu.

If you enter P in the **DL command** menu and press **Enter**, power monitoring logs are displayed. Server chassis and partition have different items on the display.

```
Select target (C=Server chassis,P=Partition,A=All,[Q=Quit]) : C (Enter)
Select trend data(0=last 24 hours,1=yesterday,[Q=Quit]) : 0 (Enter)

-- Server chassis power monitoring log --
                        Power consumption[W]
Timestamp           Ave     Max     Min     Upper limit
------------------- ------- ------- ------- -----------
YYYY-MM-DD hh:mm:ss    7600    7800    7500        8000

(omitted in the middle.)

YYYY-MM-DD hh:mm:ss    7600    7800    7500        8000

Hit enter key.
```

Items of the server chassis power monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Ave [DC]	Average power consumption value [DC output]	Integer	Average power consumption value by the server chassis. (DC output; Unit: watt)
Max [DC]	Maximum power consumption value [DC output]	Integer	Maximum power consumption value by the server chassis. (DC output; Unit: watt)
Min [DC]	Minimum power consumption value [DC output]	Integer	Minimum power consumption value by the server chassis. (DC output; Unit: watt)
Upper limit	Upper limit value of power consumption	0	No setting
		Integer	Upper limit value of power consumption (Unit: watt)

Partition

```
Select target (C=Server chassis,P=Partition,A=All,[Q=Quit]) : P (Enter)
Select partition (0-7,A=All,[Q=Quit]) : 2 (Enter)
Select trend data(0=last 24 hours,1=yesterday,[Q=Quit]) : 1 (Enter)

-- Partition2 power monitoring log --
                      Power consumption[W]
Timestamp           Ave   Max    Min  Upper limit Speed[MHz]
------------------- ----- ----- ----- ----------- ----------
YYYY-MM-DD hh:mm:ss   760   800   750   800             2960

(Omitted in the middle.)

YYYY-MM-DD hh:mm:ss   760   800   750   800             2960

Hit enter key.
```

Items of the partitionX power monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Ave	Average power consumption value [DC output]	Integer	Average power consumption value by the partition. (Unit: watt)
Max [DC]	Maximum power consumption value [DC output]	Integer	Maximum power consumption value by the partition. Unit: watt)
Min [DC]	Minimum power consumption value [DC output]	Integer	Minimum power consumption value by the partition. (Unit: watt)
Upper limit	Upper limit value of power consumption	0	No setting Power cap is disabled.
		Integer	Upper limit value of power consumption (Unit: watt)
Speed	CPU performance	Integer	The latest operation frequency of CPU in the 3-minute sampling. This value changes only with static power cap setting enabled. (Unit: MHz)

If you enter M in the **DL command** menu and press **Enter**, the environment log menu is displayed. Then enter S and press **Enter**, and the environment monitoring log menu. Select a module and the environment logs are displayed.

```
-- Environment monitoring log menu --
   S. Show log in recent days.
   Q. Quit.
(S,[Q]) : S (Enter)

-- Recent log menu --
P. Partition.
M. Management module.
SW. Switch module.
PS. Power supply module.
Q. Quit.
(P,M,SW,PS,[Q]) : P (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)

-- Partition0 environment monitoring log --

Date     |                 intake temperature[C]                |
         |------------------------------------------------------|
         | avg | min | max | 00 01 02 03 04 05 06 07 08 09 10 11|
         |     |     |     | 12 13 14 15 16 17 18 19 20 21 22 23|
---------+-----+-----+-----+------------------------------------|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX -- -- -- -- --|
         |     |     |     | -- -- -- -- -- -- -- -- -- -- -- --|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
         |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
```

```
Date      |                    exhaust temprature[C]              |
          |-------------------------------------------------------|
          | avg | min | max | 00 01 02 03 04 05 06 07 08 09 10 11|
          |     |     |     | 12 13 14 15 16 17 18 19 20 21 22 23|
----------+-----+-----+-----+------------------------------------|
          |-------------------------------------------------------|
          | avg | min | max | 00 01 02 03 04 05 06 07 08 09 10 11|
          |     |     |     | 12 13 14 15 16 17 18 19 20 21 22 23|
----------+-----+-----+-----+------------------------------------|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX -- -- -- -- --|
          |     |     |     | -- -- -- -- -- -- -- -- -- -- -- --|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|
YY-MM-DD  | aa  | bb  | cc  | XX XX XX XX XX XX XX XX XX XX XX XX|
          |     |     |     | XX XX XX XX XX XX XX XX XX XX XX XX|

Hit enter key.
```

Items of the **target module name** environment monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Date		YYYY-MM-DD	YYYY: AD year; MM: month; DD: day
		-------	Date is invalid.
avg	Average value of the sensor int a specific day	Integer	Average value of the temperature sensor. (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day
min	Maximum value of the temperature in a specific day	Integer	The minimum value of the temperature sensor (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day.
max	Minimum value of the temperature in a specific day	Integer	The maximum value of the temperature sensor (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day.
00-23	Temperature sensor value by the hour	Integer	Average value of the temperature sensor by the hour (Unit: °C)
		--	Temperature sensor values are invalid.

If you enter A in the **DL command** menu and press **Enter**, the access log menu is displayed.

```
-- Management module console access log menu --
   C. Create log file.
   A. Show all log.
   P. Show log for a period of time.
   Q. Quit.
(C,A,P,[Q]) :
```

Menu		Description
C.	Create log file.	Outputs access logs as a comma-separated values (CSV) file to the user directory in the management module. You can download the file via FTP.
A.	Show all log.	Displays access logs.
P.	Show log for a period of time.	Displays access logs for a specific period.
Q.	Quit	Returns to the previous menu.

If you enter C in the **access log** menu and press **Enter**, the access log file is created.

```
Confirm? (Y,[N]) : Y (Enter)
- Creating management module console access log file was completed.
- File name is "acs-20090303-150957.csv".
Hit enter key. (Enter)
```

If you enter A in the **access log** menu and press **Enter**, the access log list is displayed.

```
(C,A,P,[Q]) : A (Enter)

Full period : 2009-02-21 13:37:15 - 2009-03-09 04:47:27

-- Management module console access log --
No. Name                             Host            Login
--- -------------------------------- --------------- -------------------
 0 00003_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 1 00002_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 2 00001_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 3 00000_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 4 00019_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 5 00018_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 6 00017_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 7 00016_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 8 00015_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 9 00014_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
10 00013_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
11 00012_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
12 00011_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
13 00010_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
14 00009_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
15 00008_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38

(0-15,Q=Quit,[N=Next]) :
```

Items of the management module console access log are described in the table below.

Item	Description of item	Value	Description of value
No.	Log number	0 to 15	-
Name	Account name	Character string in ASCII	Account name: consists of up to 32 characters.
		MAINTENANCE	Maintenance personnel
		SPECIALIST	Factory specialist
Host	Connection source IP address	IP address	Source IP address for the user connected via LAN
		--	Connected from a serial port.
Login	Login time	YYYY-MM-DD hh:mm:ss	Login date: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second

Select a log number from the access log list, and the access log details are displayed.

```
(0-15,Q=Quit,[N=Next]) : 1 (Enter)
-- Management module access log detail --
Name     : 00002_ABCDEFGHIJKLMNOPQRSTUVWXY
Role     : 2
Host     : 192.168. 0. 1
Access   : HTTP
Login    : 2009-02-21 13:47:59
Logout   : 2009-02-21 13:47:59
Behavior : Active
Slot     : 0

Hit enter key.
```

Items of the management module access log details are described in the table below.

Item	Description of item	Value	Description of value
Name	Account name	Character string in ASCII	Account name: consists of up to 32 characters.
		MAINTENANCE	Maintenance personnel
		SPECIALIST	Factory specialist
Role		Integer	Role ID: from 0 to 23
		Maintenance	Maintenance personnel
		Specialist	Factory specialist
Host	Connection source IP address	IP address	Source IP address for the user connected via LAN
		--	Connected from a serial port.
Access	Connection type	Serial	
		Telnet	
		SSH	
		HTTP	
		HTTPS	
Login	Login time	YYYY-MM-DD hh:mm:ss	Login date and time: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Logout	Logout time	YYYY-MM-DD hh:mm:ss	Logout date and time: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Behavior	Management module type	active	
		standby	
Slot	Management module slot number	0 or 1	Slot number of the management module that you log in.

If you enter P in the **access log** menu and press **Enter**, you can specify a period of the access logs to display.

```
(C,A,P,[Q]) : P (Enter)

Full period : 2009-02-21 13:37:15 - 2009-03-09 04:47:27

Start Date([Quit]) : 2009-02-21 (Enter)
Start Time([Quit]) : 00:00:00 (Enter)
Set current date and time as end of period? (Y,[N]) : N (Enter)
End Date([Quit]) : 2009-02-28 (Enter)
End Time([Quit]) : 00:00:00 (Enter)

Selected period : 2009-02-21 00:00:00 - 2009-02-28 00:00:00

-- Management module console access log --
No. Name                            Host            Login
--- ------------------------------- --------------- -------------------
 0 00003_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 1 00002_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 2 00001_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 3 00000_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:47:59
 4 00019_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 5 00018_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 6 00017_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 7 00016_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 8 00015_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
 9 00014_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
10 00013_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
11 00012_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
12 00011_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
13 00010_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
14 00009_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38
15 00008_ABCDEFGHIJKLMNOPQRSTUVWXY  192.168. 0. 1   2009-02-21 13:45:38

(0-15,Q=Quit,[N=Next]) :
```

If you enter F in the **access log** menu and press **Enter**, the error log list is displayed.

```
-- Error log and E-mail notification history --
No. Timestamp           System event log
--- ------------------- --------------------
 0 2009-03-07 15:12:15  2000 04 010E 07A30000
 1 2009-03-07 15:23:42  2000 04 010E 07A30000
 2 2009-03-07 15:25:44  2000 04 0862 6FA10000
 3 2009-03-07 15:28:45  0100 04 F4E0 07A84000
 4 2009-03-07 15:28:26  0100 04 0710 07A30000
 5 2009-03-07 15:40:06  0100 04 0700 6FA20000
 6 2009-03-07 15:54:37  0100 04 0700 6FA20000
 7 2009-03-07 16:01:38  0100 04 F4E0 07A84000
 8 2009-03-07 16:01:19  0100 04 0710 07A30000
 9 2009-03-07 16:28:21  2000 04 010E 07A30000
10 2009-03-07 16:31:37  2000 04 010E 07A30000
11 2009-03-07 16:34:08  2000 04 010E 07A30000
12 2009-03-07 16:36:38  2000 04 010E 07A30000
13 2009-03-09 10:24:04  6100 04 0932 0BA5FFFF
14 2009-03-09 12:08:49  6100 04 0932 0BA5FFFF
15 2009-03-09 13:23:23  6100 04 0932 0BA5FFFF
16 2009-03-09 13:34:27  6100 04 0932 0BA5FFFF
17 2009-03-09 13:39:48  6100 04 0932 0BA5FFFF
18 2009-03-09 13:49:58  6100 04 0932 0BA5FFFF
19 2009-03-09 14:05:28  6100 04 0932 0BA5FFFF

Select No. (0-19,[Q=Quit]) :
```

Items of the error logs and e-mail notification history are described in the table below.

Item	Description of item	Value	Description of value
No.	E-mail notification history number	0 to 31	-
Timestamp	When the event that triggers the notification happens	YYYY-MM-DD hh:mm:ss	Date and time when the event that triggered e-mail notification happened: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
System Event Log		IIII RR gggg ee ssSS ee11223344	IIII: Record ID RR: Record type gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3

Specify an e-mail notification history number, and the log data file to probe the system in failure is created and saved in the user directory in the management module. You can download it via FTP.

If you enter [l] in the **DL command** menu and press **Enter**, the MAR log list is displayed.

```
-- MARLOG INDEX --
No. Timestamp           Assist Reason
--- ------------------- ------ ------------------------------------------
----
  0 2009-03-09 10:13:39   OK   BMC detected failure
  1 2009-03-09 10:13:48   OK   Dumplog collected
  2 2009-03-09 10:13:29   OK   Processor abnormal
  3 2009-03-09 10:07:40   OK   LP detected failure
  4 2009-03-09 10:07:34   OK   BMC detected failure
  5 2009-03-09 10:07:40   OK   Dumplog collected
  6 2009-03-09 09:38:54   OK   PCI Slot/IOA failure
  7 2009-03-09 09:38:56   OK   Dumplog collected
  8 2009-03-09 09:38:50   OK   BMC detected failure
  9 2009-03-09 09:33:23   OK   Dumplog collected
 10 2009-03-09 09:28:52   NG   BMC detected failure
 11 2009-03-09 09:29:00   OK   Dumplog collected
 12 2009-03-09 06:25:29   OK   Power module failure
 13 2009-03-09 06:25:05   OK   Environment abnormal

Select MARLOG (0-13,[Q=Quit]) :
```

Item	Description of item	Value	Description of value
No.	Log number	from 0 to 31	Used to select a log.
Timestamp	Recorded time and date	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Assist	Assist notification result	OK	Notification is successful.
		NG	Notification fails.
Reason	Message to show a cause	Character string	Available in English and Japanese according to the language mode.

Select a MAR log from the MAR log list, and the MAR log details are displayed.

```
+------------------------------+
| MARLOG (2009-03-09 10:13:39) |
+------------------------------+
-- CALL FACTOR INFORMATION --
 Reason : 15
 Impact : UU

-- RC INFORMATION --
 EVENT          : 0000 02 D3EBB449 0100 04 1530 07A30001
 RC             : 10 0100 10 15300000 07A30001
 RC NAME        : IOH RUNTIME ERROR
 COMMENT        : Uncorrectable IOH QPI failure
EventData2
bit [7]   : Logical Node ID
bit [3:0] : QPI Port#
1.Replace CPU Chip
 (Suspected chip is specified by QPI Port#.)
2.Replace MB


Hit enter key. (Enter)
-- FRU INFORMATION --
-- --------------- ------------------- ----------------- --------------
 0 | UNIT         : SRV0                | FRU MNEMONIC   : CPU0
   | PARTS NAME   : UNIT Not Inst       | REV            :  -
   | ACTION       : RPL                 | WEIGHT         : 60
   | DRAWING_NO   :  -                  | SERIAL NO      :  -
-- --------------- ------------------- ----------------- --------------
 1 | UNIT         : SRV0                | FRU MNEMONIC   : MB
   | PARTS NAME   : UNIT Not Inst       | REV            :  -
   | ACTION       : RPL                 | WEIGHT         : 40
   | DRAWING_NO   :  -                  | SERIAL NO      :  -
-- --------------- ------------------- ----------------- --------------
-- End of data --
Hit enter key.
```

Items of the detailed MAR log are described in the table below:

Item	Description of item	Value	Description of value
Timestamp	Recorded time and date (Local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Reason	Message to show a reason	XX	XX: Reason code
Impact	Connection trigger	UU	Emergency: fix it quickly.
		UE	Non-emergency: fix it the next day.
		US	Non-emergency: fix it within a week.
		UC	Non-emergency: the redundant component.
		PR	Protective maintenance request

Item	Description of item	Value	Description of value
EVENT	Event code	Hexadecimal string	-
RC	RC	Hexadecimal string	-
RC NAME	RC name	Character string	Displayed in ASCII.
COMMENT		Character string	RC comment in ASCII.

Field replaceable unit (FRU) information to MAR logs is described in the list below:

Item	Description of item	Value	Description of value
UNIT	Unit name	The value of the target unit	
PARTS NAME	Component name	Character string in ASCII	-
ACTION	Action code	RPL	Replace
		CHK	Check
		ADJ	Adjust
		CRT	Correct
		CLN	Clean
		CKE	Check externally.
		RTM	Execute TMP.
		RPE	Replace externally.
		RMD	Execute MD.
		CSP	Call maintenance personnel.
		ADD	Add
		REM	Remove
DRAWING NO	Part number	Character string in ASCII	-
FRU MNEMONIC	FRU mnemonic	The value of the target mnemonic	
REV	Revision	Character string in ASCII	-
WEIGHT		Integer	Unit: Kg
SERIAL NO	Serial number	Character string in ASCII	-

If you enter C in the **DL command** menu and press **Enter**, the Reference Code (RC) list is displayed. Then select an RC, and the detailed information is displayed.

```
-- RC list --
No.  Timestamp            RE UID  EC Failure  Additional
---- -------------------- -- ---- -- -------- ----------
   0 2009-03-09 12:50:17  10 0100 68 F4E00000 07A29300
   1 2009-03-09 12:50:17  10 0100 38 F4E00000 07A3EC00
   2 2009-03-09 12:50:15  10 0100 38 F4E00000 07A3CC00
   3 2009-03-09 12:50:15  10 0100 38 F4E00000 07A3EB00
   4 2009-03-09 12:50:15  10 0100 38 F4E00000 07A3CB00
   5 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2EA00
   6 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2CA00
   7 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2E900
   8 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2C900
   9 2009-03-09 12:50:15  10 0100 38 F4E00000 07A3E800
  10 2009-03-09 12:50:15  10 0100 38 F4E00000 07A3C800
  11 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2D200
  12 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2E231
  13 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2E221
  14 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2E211
  15 2009-03-09 12:50:15  10 0100 70 F4E00000 07A2E201
-- more (Q:Quit) --
Select No. (0-15) : 2 (Enter)
-- RC INFORMATION --
 RC             : 10 0100 38 F4E00000 07A3CC00
 RC NAME        : OEMBIOS(LP)
 COMMENT        : PCI bus error occurred at an Expansion FC card shared by
LPARs.
 EventData3  :  Expansion Card Slot Number
Refer to the "Maintenance Activities"-"Classification F" in the FC Board
Maintenance Manual.


Hit enter key.
```

Items of the RC list are described in the table below:

Item	Description of item	Value	Description of value
No.	Log number	0 to 15	-
Timestamp	Recorded time and date (Local)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
RE	RC type enhanced bit	XX	2 digits in hex
UID	Unit ID	XXXX	4 digits in hex
EC	Event code	XX	2 digits in hex
Failure	Failure code	XXXXXXXX	8 digits in hex
Additional	Additional code	XXXXXXXX	8 digits in hex

Items of the RC information are described in the table below:

Item	Description of item	Value	Description of value
RC	Reference code	Hexadecimal string	Consists of RE, UID, EC, Failure, and Additional in the RC list.
RC NAME	RC name	Character string	Displayed in ASCII.
COMMENT	-	Character string	RC comment in ASCII.

❑ DEL command

You can delete files in the user directory of the management module. Enter `DL` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> DEL (Enter)

<< DEL - Delete copy of log. >>

-- Log menu --
   D. Delete file.
   Q. Quit.
(D,[Q]) :
```

Select a menu item you require from the following list, and execute it.

Menu		Description
D.	Delete file.	
Q.	Quit	Quits the DEL command.

❑ FV command

You can display the firmware version in the internal module. Enter `FV` at the prompt, and press **Enter**.

```
<< FV - Show firmware version. >>

-- Management module firmware --
M Behavior Revision
- -------- --------------------------------
0 Active   A0151-B-4770
1 Standby  A0151-B-4770

-- Dictionary --
Revision : 00053

-- Equipment parameter --
Revision : A002

-- Server blade firmware --
--- BMC firmware ---
S Active                          Alternate
- -------------------------------- --------------------------------
0 04-00                           87-60
1 ERROR                           ERROR
2  ------------------------------  ------------------------------
3 08-47                           ------------------------------
4  ------------------------------  ------------------------------
5  ------------------------------  ------------------------------
6  ------------------------------  ------------------------------
7 03-53                           03-49

--- EFI firmware ---
S Active                          Alternate(Spool)
- -------------------------------- --------------------------------
0 01-03                           99-70
1 ERROR                           ERROR
2  ------------------------------  ------------------------------
3 01-36                           ------------------------------
4  ------------------------------  ------------------------------
5  ------------------------------  ------------------------------
6  ------------------------------  ------------------------------
7 70-48                           70-48

-- LP firmware --
S Active                          Alternate
- -------------------------------- --------------------------------
0 Not installed                   Not installed
1 Not installed                   Not installed
2  ------------------------------  ------------------------------
3 Not installed                   Not installed
4  ------------------------------  ------------------------------
5  ------------------------------  ------------------------------
6  ------------------------------  ------------------------------
7

-- Switch module firmware --
SW Revision
-- --------
 0  ------
 1  ------
 2  ------
 3  ------
 4  ------
 5  ------

-- Interop file -
Current Revision: CR00-01

-- Firmware version menu --
    Q. Quit.
([Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
Q.	Quit	Quits the FV command.

Items of the management module firmware are described in the table below:

Item	Description of item	Value	Description of value
M	Management module slot number	0 or 1	-
Behavior	SVP: Active or standby	Active	-
		Standby	-
		--------	Not installed; or sets neither Active nor Standby.
Revision	SVPFW integrated version	XXXXXXXXXXXXXXXX	General version of SVPFW: 32 characters

Dictionary information is described in the table below:

Item	Description of item	Value	Description of value
Dictionary	Dictionary file version	XXXXX	Dictionary version: 5 characters

Equipment parameter is described in the table below: Equipment parameter information.

Item	Description of item	Value	Description of value
Equipment parameter	Equipment parameter version	XXXX	Equipment parameter version: 4 characters

Items of the BMC firmware are described in the table below: BMC (Baseboard Management Controller) firmware information.

Item	Description of item	Value	Description of value
S	Server blade slot number	0 to 7	-
Active	Active BMC FW version	XXXXXXXXXXXXXXXX	BMC firmware version currently used: 32 characters
Alternate	Alternate BMC FW version	XXXXXXXXXXXXXXXX	BMC firmware version Not used currently: 32 characters

Item	Description of item	Value	Description of value
Current Revision	Information on the file of interoperability	CRMM-mm "-" is shown when no Interop file is applied.	CRMM-mm: Modification of the Interop file contents. MM: Major modification] mm: Minor modification M; m: 0 to 9

Items of EFI (Extensible Firmware Interface) firmware are described in the table below:.

Item	Description of item	Value	Description of value
S	Server blade slot number	0 to 7	-
Active	Active EFI firmware version	XXXXXXXXXXXXXXXX	EFI firmware version currently used: 32 characters
Alternate	Alternate EFI firmware version	XXXXXXXXXXXXXXXX	EFI firmware version Not used currently: 32 characters

Items of the LP firmware are described in the table below:

Item	Description of item	Value	Description of value
S	Server blade slot number	0 to 7	-
Active	Active bank firmware version	XXXXXXXXXXXXXXXX	LPAR manager bank firmware version currently used: 32 characters
Alternate	Alternate bank firmware version	XXXXXXXXXXXXXXXX	LPAR manager bank firmware version Not used currently: 32 characters

Items of switch module firmware are described in the table below:

Item	Description of item	Value	Description of value
SW	Switch module slot number	XXXX	-
Revision	Firmware version of the switch module	XXXX	Firmware version of the switch module: 4 characters Displays only supported switch modules.

❑ FW command

You can update the firmware held by the management module. Enter `FW` at the prompt, and press **Enter**.

```
<< FW - Update management module firmware. >>

-- Management module firmware --
M Behavior Revision
- -------- --------------------------------
0 ------ --------------------------------
1 Active A0110-D-4252

-- Dictionary --
Revision : 00032

-- Equipment parameter --
Revision : -----

-- Equipment parameter update status --
P Update
- --------
0 Done
1 Done
2 Done
3 Done
4 Done
5 Done
6 Done
7 Done

-- Management module firmware menu --
    U. Update firmware.
    Q. Quit.
(U,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
U.	Update firmware	Updates the dictionary file.
Q.	Quit	Quits the FV command.

Items of the management module firmware are described in the table below:

Item	Description of item	Value	Description of value
M	Management module slot number	0, 1	-
Behavior	SVP mode	Active	Active mode
		Standby	Standby mode

Item	Description of item	Value	Description of value
		-------	Not installed or undecided mode
Revision	SVPFW integrated version	XXXXXXXXXXXXXXX	General version of SVPFW: 32 characters

Dictionary information is described in the table below:

Item	Description of item	Value	Description of value
Dictionary	Dictionary file version	XXXXX	Dictionary version: 5 characters

Equipment parameter is described in the table below:

Item	Description of item	Value	Description of value
Equipment parameter	Equipment parameter version	XXXXX	Equipment parameter version: 5 characters

Items of the equipment parameter update status are described in the table below:
Information on how the equipment parameter is applied to each partition.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Update	Equipment parameter status on each partition	Done	Already updated: Update is not required.
		Not done	Note yet updated: Update is required.
		Unknown	Status unknown
		ERROR	Status cannot be obtained.
		-------	Undefined partition

Type `U` in the **FW command** menu, and press **Enter** to update the dictionary. Files that can be updated and the confirmation message are displayed. To start updating, type `Y` and press **Enter**.

```
-- Update file information --
File name              File size(byte)
---------------------- ---------------
dict.XX-XX.update              XXXXXX

Confirm? (Y,[N]) : Y

-- Update managment module firmware progress --
Process : Writing dict...
0% ----- 20% ----- 40% ----- 60% ----- 80% ----- 100%
|.........................................      | [ 90%]
```

- Update firmware was completed.



- Be sure not to downgrade the current dictionary to any earlier version.
- Locate the currently installed dictionary version in “Firmware Management View”, or “FV command”.
- Check your dictionary version with the dictionary file name as follows:

  Naming rules: dict.xxxxx.update

  xxxxx — Dictionary version

  Transfer the dictionary file to the user directory in the management module via FTP or SSH File Transfer Protocol (SFTP) before updating the dictionary. To log into FTP or SFTP, use the same account name and password as login to the system console.

❑ LM command

You can display and set a language. Input LM at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> LM (Enter)

<< LM - Language Mode. >>

-- Language mode --
Language      : English

-- Language mode setting menu --
   L. Set language mode.
   Q. Quit.
(L,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
L.	Set language mode.	
Q.	Quit	Quits the LM command.

Items of the language mode are described in the table below:

Item	Description of item	Value	Description of value
Language	Language used onscreen	English	
		Japanese	

If you enter L in the **LM command** menu and press **Enter**, you can set a language. The current setting value and specifiable values are displayed and the prompt is ready. Just press **Enter** or input a setting value and press **Enter**, and the new setting value is displayed. A message appears to confirm the setting, and the prompt is ready. Press Y and press **Enter**, and the language value will become effective. To cancel the setting value, input N after the confirmation message and press **Enter**, or just press **Enter**.

```
Language      : English
(0=English,1=Japanese,[Unchange]) : 0 (Enter)
<< LM - Language Mode. >>

-- Language mode --
Language      : English

-- Language mode setting menu --
   L. Set language mode.
   Q. Quit.
(L,[Q]) :
```

❑ ELI command

This command is not available in this system equipment.

❑ SBC command

You can display the server blade status and operate it. Enter `SBC`, and press **Enter**.

```
<< SBC - Server blade control >>

-- Server blade status --
S LID lamp
- --------
0 On
1 Off
2  ------
3 Off
4 Off
5 On
6 Off
7 Off

-- Server blade control menu --
    L. LID lamp control.
    Q. Quit.
(L,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
L.	LID lamp control	Turns on or off LID per server blade.
Q.	Quit	Quits the SBC command.

❑ MAC Command

You can display and set a media access control (MAC) address. Type `MAC` at the

```
 SVP>MAC

<< MAC - MAC address. >>

-- MAC address menu --
    C. Show current MAC address.
    O. Show original MAC address.
    A. Show/Edit additional MAC address.
    Q. Quit.
(C,O,A,[Q]) :
```

prompt, and press **Enter**.

Select a menu you require from the following list, and execute it.

Menu		Description
C.	Show current MAC address.	Displays the current MAC address information.
O.	Show original MAC address.	Displays the Default Physical MAC address information.
A.	Show/Edit additional MAC address.	Displays and edits the Optional Physical MAC address information.
Q.	Quit.	Quits the MAC command.

If you enter C in the **MAC command** menu, press **Enter**, and select a partition number, the current MAC address is shown.

```
(C,O,A,[Q]) : C
Select partition (0-7,[Q=Quit]) : 0

-- Current MAC address --
P S Card Controller Port MAC address        Type
- - ---- ---------- ---- ------------------ ----------
0 0 ONBD          0    0  00:30:48:D7:DF:60 Original
0 0 ONBD          0    1  00:30:48:D7:DF:61 Original

Hit enter key.
```

If you enter O in the **MAC command** menu, press **Enter**, and select a partition number, the Default Physical MAC address is shown.

```
(C,O,A,[Q]) : O
Select partition (0-7,[Q=Quit]) : 0

-- Original MAC address --
P S Card Controller Port MAC address
- - ---- ---------- ---- ------------------
0 0 ONBD          0    0  00:30:48:D7:DF:60
0 0 ONBD          0    1  00:30:48:D7:DF:61

Hit enter key.
```

If you enter A in the **MAC command** menu, and press **Enter**, the Optional Physical MAC address menu is shown.

```
(C,O,A,[Q]) : A

-- Additional MAC address menu --
    S. Show.
    I. Initialize.
    E. Edit.
    H. Show change history.
    Q. Quit.
(S,I,E,H,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
S.	Show.	Displays the Optional Physical MAC address information.
I.	Initialize.	Initializes the Optional Physical MAC address.
E.	Edit	Edits the Optional Physical MAC address information.
H.	Show change history.	Displays the Optional Physical MAC address change history.
Q.	Quit.	Returns to the previous menu.

If you enter S in the **Optional Physical MAC** menu, press **Enter**, and select a partition number, the Optional Physical MAC address is shown.

```
(S,I,E,H,[Q]) : S
Select partition (0-7,[Q=Quit]) : 0

-- Additional MAC address --
P S Card Controller Port MAC address
- - ---- ---------- ---- -----------------
0 0 ONBD           0    0  00:00:87:C4:45:20
0 0 ONBD           0    1  00:00:87:C4:45:21
0 0 MC0            0    0 *00:00:87:C4:AA:AA
0 0 MC0            0    1  00:00:87:C4:45:23 (CONFLICT)
0 0 MC0            0    2 *00:00:87:C4:CC:CC (CONFLICT)
0 0 MC0            0    3  00:00:87:C4:45:25

0 0 IO1            0    6  00:00:87:C4:45:50
0 0 IO1            0    7  00:00:87:C4:45:51

!!! CONFLICT is detected. (between partition 1)
!!! CONFLICT is detected. (between partition 2)

Hit enter key.
```

Items of the **Optional Physical MAC** address are described in the table below:

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	Card type and slot number	ONBD	Onboard
		MCx (x: 0 to1)	Expansion card
		IOx (x: 0 to 15)	I/O board
Controller	Controller number	0 to 1	Fixed to 0 (zero) when the card type is onboard or I/O board.
Port	Port number	0 to 7	-
MAC address	MAC address	XX:XX:XX:XX:XX:XX	Default Optional Physical MAC address
		* XX:XX:XX:XX:XX:XX	Optional Physical MAC address changed from the default

Item	Description of item	Value	Description of value
		----------	Not obtained the Optional Physical MAC address.
		(CONFLICT)	Detected multiple MAC addresses with the same value. Partition numbers with a conflict are shown at the bottom of the list.

If you enter [I] in the **Optional Physical MAC** menu, press **Enter**, and select a partition number to initialize the Optional Physical MAC address.

```
(S,I,E,H,[Q]) : I
Select partition (0-7,A=All,[Q=Quit]) : 5

Confirm? (Y,[N]) : Y
- <Partition5> Writing setting was completed.
Hit enter key.
```

If you enter E in the **Optional Physical MAC** menu, press **Enter**, and select a partition number, server blade number, card type, card number only for expansion cards and I/O boards, and controller number only for expansion cards, the Optional Physical MAC address can be edited.

```
(S,I,E,H,[Q]) : E
Select partition (0-7,[Q=Quit]) : 7
Select server blade (7,[Q=Quit]) : 7
Select card (0=Onboard,1=Mezzanine card,2=I/O adapter,[Q=Quit]) :
0
<Port0>
Additional MAC address : 00:00:87:C4:C5:7E
([Unchange]) : 00:00:87:AA:AA:AA
<Port1>

Additional MAC address : 00:00:87:C4:C5:7F
([Unchange]) : 00:00:87:BB:BB:BB
-- Additional MAC address --
P S Card Controller Port MAC address
- - ---- ---------- ---- -----------------
7 7 ONBD 0 0 *00:00:87:AA:AA:AA
7 7 ONBD 0 1 *00:00:87:BB:BB:BB
7 7 MC0 0 0 00:00:87:C4:C5:80
7 7 MC0 0 1 00:00:87:C4:C5:81
 .  .  .
7 7 IO1 0 6 00:00:87:C4:C5:AE
7 7 IO1 0 7 00:00:87:C4:C5:AF

Confirm? (Y,[N]) : Y
- <Partition7> Writing setting was completed.
Hit enter key.
```

If you enter H in the **Optional Physical MAC** menu, press **Enter** to show the Optional Physical MAC address change history.

```
(S,I,E,H,[Q]) : H
Date              P S Card Controller Port Before            After             From
----------------- - - ---- ---------- ---- ----------------- ----------------- -------
12-01-30 19:56:13 5 5 MC0           0    0 00:00:87:C4:1D:FC 00:1F:67:63:0B:FC Console
12-01-30 19:56:13 5 5 MC0           0    1 00:00:87:C4:1D:FD 00:1F:67:63:0B:FD Console
12-01-30 19:56:14 5 5 MC0           0    2 00:00:87:C4:1D:FE 00:1F:67:63:0B:FE Console

12-02-03 00:41:46 7 7 MC0           0    6 00:00:87:C4:C5:86 00:00:87:C5:AA:AA Console
12-02-03 00:41:46 7 7 MC0           0    7 00:00:87:C4:C5:87 00:00:87:C5:BB:BB Console
12-02-03 00:44:31 7 7 MC0           0    0 00:00:87:C4:AA:AA 00:00:87:C4:C5:80 Console
12-02-03 00:44:31 7 7 MC0           0    1 00:00:87:C4:BB:BB 00:00:87:C4:C5:81 Console
12-02-03 00:44:31 7 7 MC0           0    2 00:00:87:C4:CC:CC 00:00:87:C4:C5:82 Console
12-02-03 00:44:31 7 7 MC0           0    3 00:00:87:C4:DD:DD 00:00:87:C4:C5:83 Console
12-02-03 00:44:31 7 7 MC0           0    4 00:00:87:C4:EE:EE 00:00:87:C4:C5:84 Console
12-02-03 00:44:31 7 7 MC0           0    5 00:00:87:C4:FF:FF 00:00:87:C4:C5:85 Console
12-02-03 00:44:31 7 7 MC0           0    6 00:00:87:C5:AA:AA 00:00:87:C4:C5:86 Console
12-02-03 00:44:31 7 7 MC0           0    7 00:00:87:C5:BB:BB 00:00:87:C4:C5:87 Console
12-02-03 00:45:20 7 7 ONBD          0    0 00:00:87:C4:C5:7E 00:00:87:AA:AA:AA Console
12-02-03 00:45:20 7 7 ONBD          0    1 00:00:87:C4:C5:7F 00:00:87:BB:BB:BB Console

Hit enter key.
```

Items of the Optional Physical MAC address are described in the table below.

Item	Description of item	Value	Description of value
Date	Changed date	YY-MM-DD hh:mm:ss	Date when the Optional Physical MAC address is changed. YY: last 2digits of the year (AD); MM: month; DD: day; hh: hour; mm: minute; ss: second
P	Partition number	0 to 7	-
S	Server blade number	0 to 7	-
Card	Card type and slot number	ONBD	Onboard
		MCx (x: 0 to1)	Expansion card
		IOx (x: 0 to 15)	I/O board
Controller	Controller number	0 to 1	Fixed to 0 (zero) when the card type is onboard or I/O board.
Port	Port number	0 to 7	-
Before	Optional Physical MAC address before changed	XX:XX:XX:XX:XX:XX	-
After	Optional Physical MAC address after changed	XX:XX:XX:XX:XX:XX	-

Item	Description of item	Value	Description of value
From	Requested from	BSMx (x: 0 to 7	Change from BSM
		Console	Change from Console
		Unknown	Change from other than BSM/Console.

Partition management

❑ PR command

You can display and set the partition configuration. Enter `PR` at the prompt, and press **Enter**.

```
 SVP>PR

<< PR - Physical partition setting. >>

-- Power setting --
P Chassis power sync AC recovery Recovery wait(min)
- ------------------ ----------- ------------------
0 Sync               Stay off                     0
1 Sync               Power on                     5
2 Sync               Last state                  10
3 Ignore             Stay off                     0
4 Ignore             Stay off                     0
5 Ignore             Stay off                     0
6 Ignore             Stay off                     0
7 Ignore             Stay off                     0

-- Pre-configure setting --
                   Method          type              MAC type
P N+M cold standby Current Config Current    Config     Current    Config
- ---------------- ------- ------ ---------- ---------- ---------- ----------
0 Disable          PXE     PXE    Original   Original   Original   Original
1 Disable          Inline  Inline Additional Additional Original   Additional
2 Enable           Inline  Inline Additional Additional Additional Additional
3 Disable          Inline  PXE    Original   Original   Original   Original
4 Enable           Inline  Inline Additional Additional Original   Additional
5 Disable           -----  Inline  --------  Additional Original   Original
6 Disable           -----  Inline  --------  Additional Original   Original
7 Disable           -----  Inline  --------  Additional Original   Original

-- Partition setting menu --
    S. Show partition status.
    P. Edit power setting.
    R. Edit Pre-configure setting.
    C. Edit partition configuration.
    Q. Quit.
(S,P,R,C,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
S.	Show partition status.	Displays the partition status.
P.	Edit power setting.	Edits the power setting of .partitions.
R.	Edit pre-configure setting.	Edit the Smart Configure setting of partitions.
C.	Edit physical partition configuration.	Edits the Smart Configure of partitions.
Q.	Quit	Quits the PR command.

Power settings for partitions are described in the table below.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Chassis power sync	Power synchronization setting between chassis and partition (This item is not supported. To be synchronized with the power operation for the chassis regardless of this setting value.)	Synchronize	
		Ignore	Not synchronized.
		-------	Ineffective partition
AC recovery	Action setting when the power is restored	Stay off	Remain “OFF” when the power is restored.
		Power on	Turns on power when the power is restored.
		Last state	If the power is on before the failure, the power turns on when the power is restored.
		-------	Ineffective partition
Recovery wait (min)	Wait time to turn on the partition when the power is restored.	0 to 60	minute(s)
		-------	Ineffective partition

Partition Smart Configure setting are described in the table below,

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
N+M cold standby	Enable/Disable N+M cold standby	Enable	-
		Disable	-
		-------	Ineffective partition
		ERROR	Fails to obtain values.
Method (Current)	Operational value for Smart Configure method	PXE	Performs Smart Configure with PXE method.
		inline	Performs Smart Configure with inline method.
		-------	When an ineffective partition is initialized, no server blade is installed, the firmware configuration is improper, or the system is busy.
		ERROR	Fails to obtain values.

Item	Description of item	Value	Description of value
Method (Config)	Setting value for Smart Configure method	PXE	Performs Smart Configure with PXE method.
		inline	Performs Smart Configure with inline method.
		-------	Ineffective partition.
		ERROR	Fails to obtain values.
WWN type (Current)	-	additional	HBA uses Optional Physical WWN.
		original	HBA uses Default Physical WWN.
		-------	When an ineffective partition is initialized; no server blade is installed; the firmware configuration is improper; or the system is busy.
		ERROR	Fails to obtain values.
WWN type (Config)	-	additional	HBA uses Optional Physical WWN.
		original	HBA uses Default Physical WWN.
		-------	Ineffective partition.
		ERROR	Fails to obtain values.
MAC type (Current)	-	additional	LAN controller uses the Optional Physical MAC address.
		original	LAN controller uses the Default Physical MAC address.
		----------	Ineffective partition; partition in initialization; no server blade installed; improper hardware configuration; busy system.
		Error	Error in obtaining the setting value
MAC type (Config)	-	additional	LAN controller uses the Optional Physical MAC address.
		original	LAN controller uses the Default Physical MAC address.
		----------	Ineffective partition; partition in initialization; no server blade installed; improper hardware configuration; busy system
		Error	Error in obtaining the setting value.

If you enter S in the **PR command** menu and press **Enter**, you can display the partition status.

```
-- LP status --
P Mode  License
- ----- --------------
0 Basic Not Installed
1 Basic Enterprise
2  ---   ------------
3  ---   ------------
4 Basic Enterprise
5 LP   Enterprise
6 Basic Enterprise
7 Basic Enterprise

Hit enter key.
```

Items of the LP status are described in the table below: LP status.

Item	Description of item	Value	Description of value
Mode	Logical Partitioning mode	-------	No blade slot belongs to. No blade slot installed Currently in initialization
		LP	Logical Partitioning is Enabled: LPAR manager boots up.
		Basic	Logical Partitioning is Disabled: LPAR manager does not boot up.
		ERROR	Fails to obtain status due to an error.
LP License	-	-------	No blade slot belongs to. No blade slot installed Currently in initialization
		Installed	LPAR manager license is valid: LPAR manager 4.0 format.
		Not Installed	Sub version of the FRU format is the default value. LPAR manager license is invalid: LPAR manager 4.0 format.
		Essential	LPAR manager Essential model LPAR manager license is valid: LPAR manager 4.1 or later formats.
		Enterprise	LPAR manager Enterprise model LPAR manager license is valid: LPAR manager 4.1 or later formats.
		ERROR	Fails to obtain status due to an error.

If you enter P in the **PR command** menu and press **Enter**, you can set the partition. You are required to select a partition and the prompt is ready. Enter a partition number, and the current setting value of the partition in the following order: the prompt is ready. Press **Enter**, or input the setting value and press **Enter** to go to the next setting.

Displayed order	Item
1	Synchronization setting with chassis power operation.
2	Action setting when the power is restored.
3	Wait time to power on the partition when the power is restored.

If you enter a wait time to power-on the partition during power recovery, the new wait time is displayed. A confirmation message appears. Enter `Y` and press **Enter**, and the partition setting becomes effective. To cancel the setting, enter `N` and press **Enter** or just press **Enter** after the confirmation message appears.

```
Select partition (0-7,[Q=Quit]) : 0
Chassis power sync : Sync
(0=Sync,1=Ignore,[Unchange]) :
AC recovery        : Stay off
(0=Stay off,1=Power on,2=Last state,[Unchange]) :
Recovery wait(min) : 0
(0-60,[Unchange]) :

-- Power setting --
P Chassis power sync AC recovery Recovery wait(min)
- ------------------ ----------- ------------------
0 Sync               Stay off                     0
1 Sync               Stay off                     0
2 Sync               Stay off                     0
3 Sync               Stay off                     0
4 Sync               Stay off                     0
5 Sync               Stay off                     0
6  ----------------   ---------   ----------------
7 Sync               Stay off                     0

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

If you enter `R` in the **PR command** menu and press **Enter**, you can set the Smart Configure. You are required to select a partition at the prompt. Enter a partition number. Press **Enter**, or input the setting value and press **Enter** to go to the next setting.

Displayed order	Item
1	Setting to enable or disable the N+M cold standby
2	Setting for Smart Configure method
3	Setting a type of WWN used for Smart Configure
4	Setting a type of MAC

If you make changes to the setting, the new setting value is displayed. A confirmation message appears. Enter `Y`, and press **Enter**, and the partition setting becomes effective. To cancel the setting, enter `N` and press **Enter**, or just press **Enter** after the confirmation message appears.

```
 (S,P,R,C,[Q]) : R
Select partition (0-7,[Q=Quit]) : 2
N+M cold standby   : Enable
(0=Disable,1=Enable,[Unchange]) : 0
Method             : Inline
(0=PXE,1=Inline,[Unchange]) : 1
 type           : Additional
(0=Original,1=Additional,[Unchange]) : 0
MAC type           : Additional
(0=Original,1=Additional,[Unchange]) : 0

-- Pre-configure setting --
P N+M cold standby Method  type   MAC type
- ---------------- ------ ---------- ----------
0 Disable          PXE    Original   Original
1 Disable          Inline Additional Additional
2 Disable          Inline Original   Original
3 Enable           Inline Additional Additional
4 Enable           Inline Additional Additional
5 Disable          Inline Additional Original
6 Disable          Inline Additional Original
7 Disable          Inline Additional Original

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```



- Applicable type of WWN depends on whether N+M cold standby is enabled or disabled, and what type of Smart Configure method is used.

Item	Description of item	Value	Description of value
Enable	Inline	Additional	When N+M cold standby is enabled, the Optional Physical WWN is used regardless of Smart Configure method.
	PXE		
Disable	Inline	additional	Can select a type of WWN with the inline method.
		original	
	PXE	original	The Default Physical WWN is used with the PXE method

- Applicable type of MAC depends on what type of Smart Configure method is used.

Description of item	Value	Description of value
Inline	Additional	A type of MAC can be selected with In-line method.
	original	
PXE	original	Default Physical MAC is used with PXE method.

If you enter C in the **PR command** menu and press **Enter**, you can edit the partition configuration on the screen.

```
-- Partition configuration --
  Server blade
P Power                0 1 2 3 4 5 6 7
- -------------------- ---------------
                       S S - S - - - S
- -------------------- ---------------
0 Off                  X - - - - - - -
1 Off                  - X - - - - - -
2  ------------------  - - X - - - - -
3 Off                  - - - X - - - -
4  ------------------  - - - - X - - -
5  ------------------  - - - - - X X -
6  ------------------  - - - - - - - -
7 Off                  - - - - - - - X

-- Edit partition configuration. --
    C. Configure partition.
    W. Write configuration.
    Q. Quit.
(C,W,[Q]) : C
Select partition (0-7,[Q=Quit]) : 0
Input blade count (1,2,D=Delete partition,[Q=Quit]) : 2

-- Partition configuration --
  Server blade
P Power                0 1 2 3 4 5 6 7
- -------------------- ---------------
                       S S - S - - - S
- -------------------- ---------------
0 Off                  X X - - - - - - (Modified)
1 Off                  - - - - - - - - (Deleted)
2  ------------------  - - X - - - - -
3 Off                  - - - X - - - -
4  ------------------  - - - - X - - -
5  ------------------  - - - - - X X -
6  ------------------  - - - - - - - -
7 Off                  - - - - - - - X

WARNING : If confirm, partition1 is deleted.

Confirm? (Y,[N]) : Y

-- Partition configuration --
  Server blade
P Power                0 1 2 3 4 5 6 7
- -------------------- ---------------
                       S S - S - - - S
- -------------------- ---------------
0 Off                  X X - - - - - - (Modified)
1 Off                  - - - - - - - - (Deleted)
2  ------------------  - - X - - - - -
3 Off                  - - - X - - - -
4  ------------------  - - - - X - - -
5  ------------------  - - - - - X X -
6  ------------------  - - - - - - - -
```

```
7 Off                  - - - - - - - X

-- Edit partition configuration. --
    C. Configure partition.
    W. Write configuration.
    Q. Quit.
(C,W,[Q]) : W

-- Partition configuration --
-- Current configuration --
  Server blade
P Power                0 1 2 3 4 5 6 7
- -------------------- ---------------
                       S S - S - - - S
- -------------------- ---------------
0 Off                  X - - - - - - -
1 Off                  - X - - - - - -
2  ------------------  - - X - - - - -
3 Off                  - - - X - - - -
4  ------------------  - - - - X - - -
5  ------------------  - - - - - X X -
6  ------------------  - - - - - - - -
7 Off                  - - - - - - - X

-- Edited configuration --
  Server blade
P Power                0 1 2 3 4 5 6 7
- -------------------- ---------------
                       S S - S - - - S
- -------------------- ---------------
0 Off                  X X - - - - - - (Modified)
1 Off                  - - - - - - - - (Deleted)
2  ------------------  - - X - - - - -
3 Off                  - - - X - - - -
4  ------------------  - - - - X - - -
5  ------------------  - - - - - X X -
6  ------------------  - - - - - - - -
7 Off                  - - - - - - - X

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Power	Current power status	-------	No blade slot assigned. No blade slot installed.
		On	Power is on.
		Processing power-off	Power is being turned off.
		Off	Power is off.
		Processing power-on	Power is being turned on.
		ERROR	ERROR occurred during attempt to obtain system status.

Item	Description of item	Value	Description of value
0-7	Inter-blade SMP connection board	S	Installed in the server blade.
		=	Blades sandwich this symbol install this board.
Server blade X	Partition to belong	X	Belongs to.
		-	Does not belong to.
	Editing status per partition	(Created)	Initializes the setting to create it.
		(Modified)	Takes over the setting to change it.
		(Deleted)	Deletes the partition
		None	Nothing is edited.

Select a menu item from the following list to perform the function.

Menu		Description
C.	Configure partition	Edits the partition configuration.
W.	Write configuration	Applies the partition configuration.
Q.	Quit	Returns to the previous menu.

If you enter `C` in the **PR command** menu and press **Enter**, you can change the partition configuration. You are required to select a partition at the prompt. Enter a partition number, and the number of server blade slots that can belong to the partition. Input the setting value and press **Enter** to go on the next setting. To delete the partition, enter `D`.

Repeat the procedure to achieve your planned partition configuration. Then enter `W` in the menu and press **Enter** to apply the configuration. A confirmation message appears. Enter `Y` and press **Enter**, and the partition setting becomes effective. To cancel the setting, enter `N` and press **Enter** or just press **Enter** after the confirmation message appears.

Partition configuration can be applied only when the selected partition is powered off.

❑ PC command

You can display and operate partitions. Enter `PC` at the prompt, and press **Enter**.

```
SVP>PC

<< PC - Partition control. >>


-- Partition status --
P Power        Condition     LID lamp Mode  Auto power on
- ------------ ------------- -------- ----- --------------
0 Off          Normal        Off      Basic Synchronized
1 Off          Normal        Off      Basic Synchronized
2 Off          Normal        Off      Basic Synchronized
3 Off          Normal        Off      Basic Synchronized
4  ----------   -----------   ------   ---   ------------
5  ----------   -----------   ------   ---   ------------
6 Off          Normal        Off      Basic Synchronized
7  ----------   -----------   ------   ---   ------------

-- Pre-configure status --
P Autorun Run status Result
- ------- ---------- ------------
0 Disable Not get    Not Complete
1 Disable Not get    Complete
2 Disable Not get    Complete
3 Disable Not get    Complete
4 Disable  --------   ----------
5 Disable  --------   ----------
6 Disable Not get     ----------
7 Disable  --------   ----------

-- Partition control menu --
    P. Power control.
    L. LID lamp control.
    Q. Quit.
(P,L,[Q]) : :
```

Select a menu item from the following list, and execute it.

Menu		Description
P.	Power control.	Operates the partition power.
L.	LID lamp control.	Operates the partition identification light emitting diode (LED) lamp.
Q.	Quit	Quits the PC command.

Partition status is described in the table below: Dictionary status information.

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Power	Power status	----------	No blade slot assigned No blade slot installed, which is assigned
		On	Power-on status
		Processing power off	Power is being turned off.
		Off	Power-off status
		Processing power on	Power is being turned on
		ERROR	Error occurs.
Condition	Whether a user can operate or not; Fail status.	----------	No blade slot assigned No blade slot installed, which is assigned
		Normal	No problem: Available for users
		FAIL	Initialization fails, or the partition fails.
		Initializing	Just initializing.
		ERROR	Error occurs.
LID lamp	Status of the location LED of the primary blade	----------	No blade slot assigned No blade slot installed, which is assigned
		On	LED is on.
		Off	LED is off.
		ERROR	Error occurs.
Mode	Logical Partitioning	----------	No blade slot that it belongs to No blade slot installed, which is belonged to
		LP	Logical Partitioning is Enabled: LPAR manager boots.
		Basic	Logical Partitioning is Disabled: LPAR manager does not boot.
Auto power on	Current status of the power synchronization	Initializing	Under initialization Waiting to complete initialization.
		Delaying (Remain Xmin.)	Delaying the power on Shows how many minutes will take to power on automatically in parentheses. If the time left is less than 1 minute, “Remain 0min.” is displayed.
		Waiting	Waiting to power-on. Not all modules with the AC power recovery setting enabled are supplied with power
		Synchronized	Auto power-on is executed. Synchronized with power supply to the power supply modules with the AC power recovery setting enabled, the auto power-on has already been executed.

Item	Description of item	Value	Description of value
		----------	No blade slot assigned Any blade slot that's assigned

Configuration Status information on partitions is described in the table below:

Item	Description of item	Value	Description of value
P	Partition number	0 to 7	-
Autorun	Run automatically	Enable	Valid
		Disable	Invalid
Run Status	Smart Configure is being executed.	Configured	Enabled
		No information	Nothing is obtained.
		Not Configured	No setting
		In Progress	
		In Progress	
		----------	No blade installed. Autorun is disabled
		ERROR	Error occurs.
Result	Result of Smart Configure	Complete	
		Not Complete	Aborted.
		----------	No blade installed. Autorun is disabled
		ERROR	Error occurs.

If you enter `P` in the **PC command** menu and press **Enter**, the **partition control** menu is displayed.

```
(P,L,[Q]) : P

-- Partition status --
P Power        Condition     LID lamp Mode  Auto power on
- ------------ ------------- -------- ----- --------------
0 Off          Normal        Off      Basic Synchronized
1 Off          Normal        Off      Basic Synchronized
2 Off          Normal        Off      Basic Synchronized
3 Off          Normal        Off      Basic Synchronized
4  ----------   -----------   ------   ---   ------------
5  ----------   -----------   ------   ---   ------------
6 Off          Normal        Off      Basic Synchronized
7  ----------   -----------   ------   ---   ------------

-- Pre-configure status --
P Autorun Run status Result
- ------- ---------- ------------
0 Disable Not get    Not Complete
1 Disable Not get    Complete
2 Disable Not get    Complete
3 Disable Not get    Complete
4 Disable  --------   ----------
5 Disable  --------   ----------
6 Disable Not get     ----------
7 Disable  --------   ----------

-- Power control menu --
    P. Power on.
    S. Shutdown.
    F. Force power off.
    C. Run pre-configure.
    R. Restart.
    H. Hard reset.
    N. Generate NMI.
    D. Cancel delayed power on.
    Q. Quit.
(P,S,F,C,R,H,N,D,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
P.	Power on.	Turns on power to the partition.
S.	Shutdown.	Shuts down the partition
F.	Force power off.	Turns off the partition forcibly.
C.	Run pre-configure.	Executes Smart Configure.
R.	Restart.	Restarts the partition.
H.	Hard reset.	Performs the partition hard reset.
N.	Generate NMI.	
D.	Cancel delayed power-on	Cancels the delayed power-on to the partition.
Q.	Quit.	Returns to the previous menu.

If you enter `L` in the **PC command** menu and press **Enter**, the LID lamp control menu is displayed.

```
(P,L,[Q]) : L

-- Partition status --
P Power        Condition     LID lamp Mode  Auto power on
- ------------ ------------- -------- ----- --------------
0 Off          Normal        Off      Basic Synchronized
1 Off          Normal        Off      Basic Synchronized
2 Off          Normal        Off      Basic Synchronized
3 Off          Normal        Off      Basic Synchronized
4  ----------   -----------   ------   ---   ------------
5  ----------   -----------   ------   ---   ------------
6 Off          Normal        Off      Basic Synchronized
7  ----------   -----------   ------   ---   ------------

-- Pre-configure status --
P Autorun Run status Result
- ------- ---------- ------------
0 Disable Not get    Not Complete
1 Disable Not get    Complete
2 Disable Not get    Complete
3 Disable Not get    Complete
4 Disable  --------   ----------
5 Disable  --------   ----------
6 Disable Not get     ----------
7 Disable  --------   ----------

-- LID lamp control menu --
    T. Turn on
    F. Turn off
    Q. Quit.
(T,F,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
T.	Turn on	Turns on the LID lamp of the server blade that belongs to the partition.
F.	Turn off	Turns off the LID lamp of the server blade that belongs to the partition.
Q.	Quit.	Returns to the previous menu.

❑ UTL command

You can release the power-on request suppress setting to the partition with this command. Enter `UTL` at the prompt, and press **Enter**.

```
SVP> UTL (Enter)
<< UTL - Utility. >>

-- Utility menu --
   C. Change power on request suppress setting.
   Q. Quit.
(C,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Change power-on request suppress setting.	
Q.	Quit.	Quits the UTL command.

Network management

❑ LC command

You can display and set the network information with this command. Enter `LC` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> LC (Enter)

<< LC - LAN configuration. >>

-- Management LAN setting menu --
  C. Show management LAN setting.
  M. Edit management module setting.
  P. Edit partition setting.
 SW. Edit switch module setting.
  V. Edit VLAN setting.
  Q. Quit
(C,M,P,SW,V,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Show management LAN setting.	Shows the settings configured with the LC command such as the network setting of the management module.
M.	Edit management module setting.	
P.	Edit partition setting.	Edit the network setting of the partition.
SW.	Edit switch module setting.	
V.	Edit VLAN setting.	
Q.	Quit	Quits the LC command.

If you enter C in the **LC command** menu and press **Enter**, the current LC command setting value is displayed.

```
(C,M,P,SW,V,[Q]) : C (Enter)
-- Management module LAN interface setting --
IP address      Subnetmask      Default gateway Ext port
--------------- --------------- --------------- --------
172. 16.201.  1 255.255.  0.  0   0.  0.  0.  0 MGMT-0

-- Management module DNS setting --
D IP address
- ---------------
0   0.  0.  0.  0
1   0.  0.  0.  0
2   0.  0.  0.  0

-- Partition network setting --
P IP address      Subnetmask      Default gateway Ext port
- --------------- --------------- --------------- --------
0 172. 16.201. 10 255.255.  0.  0   0.  0.  0.  0 MGMT-0
1 172. 16.201. 11 255.255.  0.  0   0.  0.  0.  0 MGMT-0
2 172. 16.201. 12 255.255.  0.  0   0.  0.  0.  0 MGMT-0
3 172. 16.201. 13 255.255.  0.  0   0.  0.  0.  0 MGMT-0
4 172. 16.201. 14 255.255.  0.  0   0.  0.  0.  0 MGMT-0
5 172. 16.201. 15 255.255.  0.  0   0.  0.  0.  0 MGMT-0
6 172. 16.201. 16 255.255.  0.  0   0.  0.  0.  0 MGMT-0
7 172. 16.201. 17 255.255.  0.  0   0.  0.  0.  0 MGMT-0

-- Switch module current network setting --
SW IP address      Subnetmask      Default gateway
-- --------------- --------------- ---------------
 0  -------------   -------------   -------------
 1  -------------   -------------   -------------
 2  -------------   -------------   -------------
 3  -------------   -------------   -------------
 4  -------------   -------------   -------------
 5  -------------   -------------   -------------

-- Switch module network setting --
SW Ext  IP address       Subnetmask      Default gateway Ext port Synchronize
-- ---- ---------------- --------------- --------------- -------- -----------
 0 Ext    0.  0.  0.  0    0.  0.  0.  0   0.  0.  0.  0 MGMT-0   No
 1 Int   --------------   -------------   -------------   ------   ---------
 2 Int   --------------   -------------   -------------   ------   ---------
 3 Int   --------------   -------------   -------------   ------   ---------
 4 Int   --------------   -------------   -------------   ------   ---------
 5 Int   --------------   -------------   -------------   ------   ---------
```

```
 -- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X X - - X X X X X X X X X X
Untag1  MGMT-1   - - - - - - - - - - - - - -
1000    MGMT-0   - - X - - - - - - - - - - -
1001    MGMT-0   - - - X - - - - - - - - - -
2000    MGMT-0   - - - - - - - - - - - - - -

Hit enter key. (Enter)
```

If you enter M in the **LC command** menu and press **Enter**, the network setting of the management module is displayed.

```
(C,M,P,SW,V,[Q]) : M (Enter)
-- Management module LAN interface setting --
IP address      Subnetmask      Default gateway Ext port
--------------- --------------- --------------- --------
192.168. 0.     1 255.255.255. 0  0. 0. 0. 0    MGMT-0

-- Management module DNS setting --
D IP address
- ---------------
0  0. 0. 0. 0
1  0. 0. 0. 0
2  0. 0. 0. 0

-- Management LAN setting menu --
   L. Edit management module setting.
   Q. Quit.
(L,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
L.	Edit management module setting	Edits the network setting of the management module.
Q.	Quit	Returns to the previous menu.

If you enter L in the **network setting** menu of the management module and press **Enter** key, the current values appear in the following numerical order shown in the table below. At the prompt, press **Enter**, or enter a setting value and press **Enter**, and the screen will go to the next setting.

Menu	Description
1	IP address of the management module
2	Subnetmask of the management module
3	Default gateway of the management module

Menu	Description
4	IP address of the DNS server 0
5	IP address of the DNS server 1
6	IP address of the DNS server 2

If you enter the IP address of DNS server 2, the changed value is displayed. A warning appears after the change is reflected saying that the connection to the management module may be disconnected. A message to confirm the change is displayed. At the prompt, enter `Y` and press **Enter**. The network setting is reflected on the management module. When the IP address of the management module is changed, the session connected by specifying the former IP address is disconnected. To cancel the network setting in the management module, press `N` and press **Enter**, or simply press **Enter** to confirm the new setting value.

```
(L,[Q]) : L (Enter)
IP address : 192.168. 0. 1
([Unchange]) : 192.168.0.10 (Enter)
Subnetmask : 255.255.255. 0
([Unchange]) : 255.255.254.0 (Enter)
Default gateway : 0. 0. 0. 0
([Unchange]) : (Enter)
DNS0 : 0. 0. 0. 0
([Unchange]) : (Enter)
DNS1 : 0. 0. 0. 0
([Unchange]) : (Enter)
DNS2 : 0. 0. 0. 0
([Unchange]) :
-- Management module LAN interface setting --
IP address      Subnetmask      Default gateway Ext port
--------------- --------------- --------------- --------
192.168. 0. 10  255.255.254. 0   0. 0. 0. 0     MGMT-0

-- Management module DNS setting --
D IP address
- ---------------
0  0. 0. 0. 0
1  0. 0. 0. 0
2  0. 0. 0. 0

WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter P in the **LC command** menu and press **Enter**, the network setting of the partition is displayed.

```
(C,M,P,SW,V,[Q]) : P (Enter)
-- Partition network setting --
P IP address      Subnetmask      Default gateway Ext port
- --------------- --------------- --------------- --------
0   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------
1   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------
2   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------
3   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------
4   0. 0. 0. 0     0  0. 0. 0      0. 0. 0. 0      ------
5   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------
6   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0     ------
7   0. 0. 0. 0     0. 0. 0. 0      0. 0. 0. 0      ------

-- Partition network setting --
  A. Edit all partition setting in one network.
  N. Edit one partition setting.
  Q. Quit.
(A,N,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Edit all partition settings in one network.	
N.	Edit one partition setting.	Edits the network setting of the individual partition.
Q.	Quit	Returns to the previous menu.

If you enter A in the **partition setting** menu and press **Enter**, the current values appear in the numerical order listed in the table below. Press **Enter**, or enter a setting value and press **Enter**, and the screen will go to the next setting.

Menu	Description
1	Subnetmask
2	Default gateway
3	IP address of the partition 0
4	IP address of the partition 1
5	IP address of the partition 2
6	IP address of the partition 3
7	IP address of the partition 4
8	IP address of the partition 5
9	IP address of the partition 6
10	IP address of the partition 7

If you enter the IP address of partition 7, the changed value is displayed. A warning appears saying that the connection to the partition may be disconnected. A confirmation message appears. Enter `Y`, and press **Enter**. The network setting is saved on the partition. When the IP address of the partition is changed, the session connected by specifying the former IP address is disconnected. To cancel the network setting in the partition, enter `N` and press **Enter** or just press **Enter** to confirm the new setting value.

```
(A,N,[Q]) : A (Enter)
Subnetmask : 0. 0. 0. 0
([Unchange]) : 255.255.254.0 (Enter)
Default gateway : 0. 0. 0. 0
([Unchange]) : (Enter)
<Partition0>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.1 (Enter)
<Partition1>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.2 (Enter)
<Partition2>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.3 (Enter)
<Partition3>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.4 (Enter)
<Partition4>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.5 (Enter)
<Partition5>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.6 (Enter)
<Partition6>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.7 (Enter)
<Partition7>
IP address : 0. 0. 0. 0
([Unchange]) : 192.168.1.8 (Enter)
```

```
-- Partition network setting --
P IP address      Subnetmask      Default gateway Ext port
- --------------- --------------- --------------- --------
0 192.168. 1. 1   255.255.254. 0   0. 0. 0. 0     MGMT-0
1 192.168. 1. 2   255.255.254. 0   0. 0. 0. 0     MGMT-0
2 192.168. 1. 3   255.255.254. 0   0. 0. 0. 0     MGMT-0
3 192.168. 1. 4   255.255.254. 0   0. 0. 0. 0     MGMT-0
4 192.168. 1. 5   255.255.254. 0   0. 0. 0. 0     MGMT-0
5 192.168. 1. 6   255.255.254. 0   0. 0. 0. 0     MGMT-0
6 192.168. 1. 7   255.255.254. 0   0. 0. 0. 0     MGMT-0
7 192.168. 1. 8   255.255.254. 0   0. 0. 0. 0     MGMT-0

WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Writing setting was completed.
- <Partition1> Writing setting was completed.
- <Partition2> Writing setting was completed.
- <Partition3> Writing setting was completed.
- <Partition4> Writing setting was completed.
- <Partition5> Writing setting was completed.
- <Partition6> Writing setting was completed.
- <Partition7> Writing setting was completed.
Hit enter key. (Enter)
```

If you enter `N` in the **partition setting** menu and press **Enter**, you are asked to select a partition. Enter the IP address of the specified partition, and the current subnetmask of the specified partition is displayed. Enter the default gateway of the specified partition, and the changed setting value is displayed. A warning message indicating that the connection to the specified partition may be disconnected is displayed after the changed setting is saved. A confirmation message is displayed. At the prompt, enter `Y` and press **Enter** to save the network setting. The session connected by specifying the former IP address is disconnected. To cancel the setting change, enter `N` and press **Enter**, or just press **Enter**.

```
(A,N,[Q]) : N (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)
IP address : 192.168. 1. 1
([Unchange]) : 192.168.1.10 (Enter)
Subnetmask : 255.255.254. 0
([Unchange]) : (Enter)
Default gateway : 0. 0. 0. 0
([Unchange]) : (Enter)
-- Partition network setting --
P IP address      Subnetmask      Default gateway Ext port
- -------------- --------------- --------------- --------
0 192.168. 1. 10  255.255.254. 0   0. 0. 0. 0     MGMT-0
1 192.168. 1. 2   255.255.254. 0   0. 0. 0. 0     MGMT-0
2 192.168. 1. 3   255.255.254. 0   0. 0. 0. 0     MGMT-0
3 192.168. 1. 4   255.255.254. 0   0. 0. 0. 0     MGMT-0
4 192.168. 1. 5   255.255.254. 0   0. 0. 0. 0     MGMT-0
5 192.168. 1. 6   255.255.254. 0   0. 0. 0. 0     MGMT-0
6 192.168. 1. 7   255.255.254. 0   0. 0. 0. 0     MGMT-0
7 192.168. 1. 8   255.255.254. 0   0. 0. 0. 0     MGMT-0

WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Writing setting was completed.
Hit enter key. (Enter)
```

If you enter `SW` in the **LC command** menu and press **Enter**, the network setting of the switch module is displayed.

```
(C,M,P,SW,V,[Q]) : SW
-- Switch module network setting --
SW Ext  IP address       Subnetmask      Default gateway Ext port
Synchronize
-- ---- ---------------- --------------- --------------- -------- ----------
-
 0 Ext    0.  0.  0.  0    0.  0.  0.  0   0.  0.  0.  0 MGMT-0   No
 1 Int   --------------   -------------   -------------   ------   ---------
 2 Int   --------------   -------------   -------------   ------   ---------
 3 Int   --------------   -------------   -------------   ------   ---------
 4 Int   --------------   -------------   -------------   ------   ---------
 5 Int   --------------   -------------   -------------   ------   ---------

-- Switch module network setting menu --
    A. Edit all switch module setting.
    N. Edit one switch module setting.
    S. Show switch module current network setting.
    W. Synchronize network setting to switch module.
    Q. Quit.
(A,N,S,W,[Q]) : (Enter)
```

Switch module network setting is described in the table below: Network setting information on a switch module.

Item	Description of item	Value	Description of value
SW	Slot number of the switch module	0 to 5	-
Ext	Option to connect the management interface for internal devices of the switch module to the output port for external devices.	Int	Internal connection only Connection from the external output port is not available.
		Ext	Connection from the external output port is available. For 10 Gb DCB SW, internal connection is simultaneously available with values Ext for Ext, Yes for Synchronize, and not 0.0.0.0 for IP address. In this case, only information on connection from external output ports is shown.
		IOSW	IOSW: input output switch Ethernet port of the switch module For 10 Gb DCB SW, no Ethernet port of the switch module exists. When it is specified, neither internal connection nor connection from external output ports is available.
IP address	IP address of the management interface in the switch module	IP address format	-
		IP address format *	Interface to view and update the management interface LAN setting: - Not supported by the switch module. - Supported by the switch module but an error has occurred.
		-------	Internal connection is set.
Subnetmask	Subnetmask to the management interface in the switch module	IP address format	-
		-------	Internal connection is set.
Default gateway	Default gateway to the management interface in the switch module	IP address format	-
		-------	Internal connection is set.
Ext port	External port connected to the management interface in the switch module	MGMT-0	Management LAN port0
		MGMT-1	Management LAN port1
		-------	Internal connection is set.

Item	Description of item	Value	Description of value
Synchronize	Apply the management module setting to the switch module	Yes	Applies the setting held by the management to the switch module. - No switch module installed or - Interface to view and update the management interface LAN setting is supported by the switch module and the switch module and management module have the same setting.
		Yes!	Applies the setting held by the management to the switch module. - Interface to view and update the management interface LAN setting is supported by the switch module and the switch module and management module have the different settings.
		No	Does not apply the setting held by the management module to the switch module.
		-------	Internal connection is set.

Select a menu item from the following list to execute it.

Menu		Description
A.	Edit all switch module setting.	Sets the network setting of all switch modules.
N.	Edit one switch module setting.	Edits the network setting of the individual switch module.
S.	Show the switch module current network setting.	Displays the current setting of the switch module.
W.	Synchronize network setting to switch module.	Applies the setting held by the management module to the switch module.
Q.	Quit	Returns to the previous menu.

If you enter `A` and press **Enter**, the prompt for setting the switch module connection is ready. Enter a setting value and press **Enter**, and then go to the next setting.

When you set the Ext setting to `Int` or `LOSW`, the other settings of the switch module are automatically filled in.

When you set the Ext setting to `Ext` and the Synchronize setting to `No`, the other settings of the switch module are automatically filled in.

When you set the Ext setting to `Ext`, the Synchronize setting to `Yes`, and IP address to 0.0.0.0, the other settings of the switch module are automatically filled in.

Then the new setting value is displayed. A message to confirm the setting is displayed. At the prompt, enter `Y` and press **Enter**, and the network setting is saved in the switch module. To cancel the setting, enter `N` and press **Enter** or just press **Enter** to confirm.

```
(A,N,S,W,[Q]) : A
<Switch module0>
Ext setting      : Ext
(0=Int,1=Ext,2=IOSW,[Unchange]) : 0

<Switch module1>
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) : 2

<Switch module2>
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) : 1
Synchronize      : No
(0=No,1=Yes,[Unchange]) : 0

<Switch module3>
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) : 1
Synchronize      : No
(0=No,1=Yes,[Unchange]) : 1
IP address       :   0.  0.  0.  0
([Unchange]) : 192.168.0.111
Subnetmask       :   0.  0.  0.  0
([Unchange]) : 255.255.255.0
Default gateway  :   0.  0.  0.  0
([Unchange]) : 192.168.0.112

<Switch module4>
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) : 1
Synchronize      : No
(0=No,1=Yes,[Unchange]) : 1
IP address       :   0.  0.  0.  0
([Unchange]) : 0.0.0.0

<Switch module5>
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) :

-- Switch module network setting --
SW Ext  IP address       Subnetmask      Default gateway Ext port Synchronize
-- ---- --------------- --------------- --------------- -------- -----------
 0 Int   --------------   -------------   -------------   ------   ---------
 1 IOSW  --------------   -------------   -------------   ------   ---------
 2 Ext    0.  0.  0.  0    0.  0.  0.  0   0.  0.  0.  0 MGMT-0   No
 3 Ext  192.168.  0.111  255.255.255.  0 192.168.  0.112 MGMT-0   Yes
 4 Ext    0.  0.  0.  0    0.  0.  0.  0   0.  0.  0.  0 MGMT-0   Yes
 5 Int   --------------   -------------   -------------   ------   ---------
```

```
WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) :
- <Switch module0> Writing setting was completed.
- <Switch module1> Writing setting was completed.
- <Switch module2> Writing setting was completed.
- <Switch module3> Writing setting was completed.
- <Switch module4> Writing setting was completed.
- <Switch module5> Writing setting was completed.
Hit enter key. (Enter)
```

If you enter N in the **switch module setting** menu and press **Enter**, you are asked to select a switch module. At the prompt, enter the slot number of a switch module, and the current network setting of the specified switch module is displayed. Enter the network setting of the specified switch module, press **Enter**, and go to the next setting.

When you set the Ext setting to Int or LOSW, the other settings of the switch module are automatically filled in.

When you set the Ext setting to Ext and the Synchronize setting to No, the other settings of the switch module are automatically filled in.

When you set the Ext setting to Ext, the Synchronize setting to Yes, and IP address to 0.0.0.0, the other settings of the switch module are automatically filled in.

Enter the connection setting to the specified switch module, and the changed setting value is displayed. A message to confirm the change is displayed and the prompt is ready. Enter Y and press **Enter**, and the network setting is saved. To cancel the setting change, enter N and press **Enter** or just press **Enter**.

```
(A,N,S,W,[Q]) : N
Select switch module (0-5,[Q=Quit]) : 0
Ext setting      : Int
(0=Int,1=Ext,2=IOSW,[Unchange]) : 1
Synchronize      : No
(0=No,1=Yes,[Unchange]) : 1
IP address       :   0.  0.  0.  0
([Unchange]) : 192.168.1.111
Subnetmask       :   0.  0.  0.  0
([Unchange]) : 255.255.255.0
Default gateway  :   0.  0.  0.  0
([Unchange]) : 192.168.1.128
-- Switch module network setting --
SW Ext  IP address       Subnetmask      Default gateway Ext port Synchronize
-- ---- ---------------- --------------- --------------- -------- -----------
 0 Ext  192.168.  1.111  255.255.255.  0 192.168.  1.128 MGMT-0   Yes
 1 Int   --------------   -------------   -------------   ------   ---------
 2 Int   --------------   -------------   -------------   ------   ---------
 3 Int   --------------   -------------   -------------   ------   ---------
 4 Int   --------------   -------------   -------------   ------   ---------
 5 Int   --------------   -------------   -------------   ------   ---------


WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) : Y
- <Switch module0> Writing setting was completed.
Hit enter key. (Enter)
```

When Network OS version 3.0.0 is on a Brocade 10 Gb DCB switch module, the default gateway setting from the management module does not take effect on the switch module. Log in to the switch module and configure it using the ip route command. See the *Network OS Administrator's Guide* for details. If Network OS version 2.0.1 is on the switch module, you cannot configure the gateway.

If you enter S in the **switch module setting** menu and press **Enter**, the current switch module setting is displayed.

```
(A,N,S,W,[Q]) : S
-- Switch module current network setting --
SW IP address      Subnetmask      Default gateway
-- --------------- --------------- ---------------
 0 192.168.  1.111 255.255.255.  0 192.168.  1.128
 1  -------------   -------------   -------------
 2  -------------   -------------   -------------
 3  -------------   -------------   -------------
 4  -------------   -------------   -------------
 5  -------------   -------------   -------------

Hit enter key.
```

If you enter W in the **switch module setting** menu and press **Enter**, the switch module setting held by the management module is displayed and you are asked to select a switch module at the prompt.

Enter the slot number of the switch module, and a message to confirm the change is displayed. At the prompt, enter Y and press **Enter**, and the switch module setting held by the management module is applied to the network setting of the switch module. To cancel the setting change, enter N and press **Enter** or just press **Enter**.

```
(A,N,S,W,[Q]) : W
-- Switch module network setting --
SW Ext  IP address       Subnetmask      Default gateway Ext port Synchronize
-- ---- ---------------- --------------- --------------- -------- -----------
 0 Ext  192.168.  1.111  255.255.255.  0 192.168.  1.128 MGMT-0   Yes
 1 Int   --------------   -------------   -------------   ------   ---------
 2 Int   --------------   -------------   -------------   ------   ---------
 3 Int   --------------   -------------   -------------   ------   ---------
 4 Int   --------------   -------------   -------------   ------   ---------
 5 Int   --------------   -------------   -------------   ------   ---------

Select switch module (0-5,A=All,[Q=Quit]) : 0
Confirm? (Y,[N]) : Y
- <Switch module0> Writing setting was completed.
Hit enter key.
```

If you enter V in the **LC command** menu and press **Enter**, the VLAN setting is displayed.

```
(C,M,P,SW,V,[Q]) : V (Enter)
-- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X X X X X X X X X X X X X X
Untag1  MGMT-1   - - - - - - - - - - - - - - -

-- VLAN setting --
   M. Move port.
   C. Create VLAN.
   D. Delete VLAN.
   Q. Quit.
(M,C,D,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
M.	Move port.	Moves ports between virtual local area networks (VLANs)
C.	Create VLAN.	
D.	Delete VLAN.	
Q.	Quit	Returns to the previous menu.

If you enter M in the **VLAN setting** menu and press **Enter**, the current VLAN setting appears, and a prompt for the target port to be selected appears. If you connect the target port to a partition or switch module, specify the partition number and switch module slot number. When the target port for transfer is selected, the prompt appears for a VLAN ID. Enter the VLAN ID, and the changed setting value is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the VLAN setting is saved. To cancel the setting change, enter N and press **Enter**, or just press **Enter**.

```
(M,C,D,[Q]) : M (Enter)
-- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X X X X X X X X X X X X X X
Untag1  MGMT-1   - - - - - - - - - - - - - - -
Select target (0=Management module,1=Partition,2=Switch
module,[Q=Quit]) : 0
(Enter)
VLAN ID (Z=Untag0,G=Untag1,2-4000,[Unchange]) : G (Enter)
-- VLAN setting --
                    Partition      Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0   MGMT-0  X X X X X X X X X X X X X X
Untag1   MGMT-1  - - - - - - - - - - - - - - -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter C in the **VLAN setting** menu and press **Enter**, the current VLAN setting is displayed. At the prompt, enter the VLAN ID, and the setting value with no setting of external connection ports is displayed. At the prompt, enter an external connection port, and the new setting value is displayed. A confirmation message appears. Enter Y and press **Enter**, and the VLAN setting is saved. To cancel the setting change, enter N and press **Enter**, or just press **Enter**.

```
(M,C,D,[Q]) : C (Enter)
-- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X - X X X X X X X X X X X X
Untag1  MGMT-1   - X - - - - - - - - - - - -

VLAN ID (2-4000,[Q=Quit]) : 2 (Enter)
Ext port : MGMT-0
(0=MGMT-0,1=MGMT-1,[Unchange]) : 0 (Enter)
-- VLAN setting --
                    Partition      Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X - X X X X X X X X X X X X
Untag1  MGMT-1   - X - - - - - - - - - - - -
   2    MGMT-0   - - - - - - - - - - - - - -
   3
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter D in the **VLAN setting** menu and press **Enter**, the current VLAN setting appears. At the prompt, enter the VLAN ID, and the changed setting value is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the VLAN setting is saved. To cancel the setting change, enter N and press **Enter**, or just press **Enter**.

```
(M,C,D,[Q]) : D (Enter)
-- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X - X X X X X X X X X X X X
Untag1  MGMT-1   - X - - - - - - - - - - - -
   2    MGMT-0   - - - - - - - - - - - - - -

Select VLAN ([Q=Quit]) : 2 (Enter)
-- VLAN setting --
                   Partition       Switch module
VLAN ID Ext port M 0 1 2 3 4 5 6 7 0 1 2 3 4 5
------- -------- - --------------- -----------
Untag0  MGMT-0   X - X X X X X X X X X X X X
Untag1  MGMT-1   - X - - - - - - - - - - - -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

❑ LFT command

You can set redundancy at the management LAN port. Enter `LFT` at the prompt, and press **Enter**. (LFT: Link Fault Tolerance)

```
5713RF0 NNNNN(0)SVP> LFT (Enter)
<< LFT - Link Fault Tolerance setting. >>

-- Link Fault Tolerance setting --
Ext port Management module LFT     Down(s) Up(s)
-------- ----------------- ------- ------- -----
MGMT-0   Active            Enable        3   180
MGMT-1   Active            Enable        3   180
MNT      Active            Enable        3   180

-- Link Fault Tolerance setting menu --
    Z. Edit management0 port setting.
    O. Edit management1 port setting.
    Q. Quit.
(Z,O,[Q]) :
```

Select a menu item in the table below to execute the function.

Menu		Description
Z.	Edit management 0 port setting.	Edit redundancy setting on MGMT0 port of the management module.
O.	Edit management1 port setting.	Edit redundancy setting on MGMT1 port of the management module.
Q.	Quit.	Quits the LFT command.

Items on the screen are described in the table below.

Menu	Description
Ext port	External output port MGMT-0: MGMT0 port; MTGMT-1: MGMT1 port; MNT: MAINT port
Management module	Which management module has open ports: Active or Standby
LFT	Redundancy function of the management LAN port: Enable or Disable
Down(s)	How many seconds it takes to ascertain that the external output port is linkdown: specify 1 to 3600 seconds.
Up(s)	How many seconds it takes to ascertain that the external output port is linkup: specify 1 to 3600 seconds.

If you enter Z in the **LFT command** menu and press **Enter**, the current redundancy setting in the MGMT0 port of the management LAN port appears. At the prompt, enter the redundancy setting of the management LAN port, and the current time to ascertain linkdown is displayed in seconds. At the next prompt, enter a time to ascertain linkdown in seconds. At the next prompt, enter a setting in seconds to ascertain linkup, and the changed setting value is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the VLAN setting is saved. To cancel the setting change, enter N and press **Enter**, or just press **Enter**.

```
(Z,O,[Q]) : Z (Enter)
LFT : Enable
(0=Disable,1=Enable,[Unchange]) : 0 (Enter)
Down(s) : 3
(1-3600,[Unchange]) : 10 (Enter)
Up(s) : 180
(1-3600,[Unchange]) : 1800 (Enter)

-- Link Fault Tolerance setting --
Ext port Management module LFT     Down(s) Up(s)
-------- ----------------- ------- ------- -----
MGMT-0   Active            Disable      10  1800
MGMT-1   Active            Enable        3   180
MNT      Active            Enable        3   180

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter O in the **LFT command** menu and press **Enter**, you can change the redundancy setting in the management LAN port of the MGMT1 port.

For the MAINT port, you can only display the setting.

❑ LS command

You can display the MAC address of the management module and server blade. Enter `LS` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> LS (Enter)

<< LS - LAN controller discriminating information. >>

-- LAN controller information menu --
   M. Show MAC address of controller on management module.
   B. Show MAC address of controller on server blade.
   O. Show MAC address of controller on management module and server
      blade.
   Q. Quit.
(M,B,O,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
M.	Show MAC address of controller on management module.	
B.	Show MAC address of controller on server blade.	
O.	Show MAC address of controller on management module and server blade.	
Q.	Quit	Quits the LS command.

If you enter `M` in the **LS command** and press **Enter**, the MAC address of the management module is displayed.

```
(M,B,O,[Q]) : M (Enter)

-- MAC addresses on management module --
M controller0        controller1
- ------------------ ------------------
0 00:00:87:12:84:4A  00:00:87:12:84:4B
1 00:00:87:12:84:2E  00:00:87:12:84:2F

Hit enter key. (Enter)
```

If you enter B in the **LS command** and press **Enter**, the MAC address of the server blade is displayed.

```
(M,B,O,[Q]) : B (Enter)

-- MAC addresses on server blade --
S Onboard0           Onboard1           I/O Controller     BMC
- ------------------ ------------------ ------------------ ------------------
0 00:30:48:D0:ED:82  00:30:48:D0:ED:83  00:30:48:D0:ED:84  00:30:48:D0:ED:85
1 00:30:48:D0:ED:96  00:30:48:D0:ED:97  00:30:48:D0:ED:98  00:30:48:D0:ED:99
2 00:30:48:D0:EC:C2  00:30:48:D0:EC:C3  00:30:48:D0:EC:C4  00:30:48:D0:EC:C5
3 00:30:48:D0:ED:1A  00:30:48:D0:ED:1B  00:30:48:D0:ED:1C  00:30:48:D0:ED:1D
4 00:30:48:D0:ED:26  00:30:48:D0:ED:27  00:30:48:D0:ED:28  00:30:48:D0:ED:29
5 00:30:48:D0:ED:6A  00:30:48:D0:ED:6B  00:30:48:D0:ED:6C  00:30:48:D0:ED:6D
6 00:30:48:D0:EC:B6  00:30:48:D0:EC:B7  00:30:48:D0:EC:B8  00:30:48:D0:EC:B9

Hit enter key. (Enter)
```

If you enter O in the **LS command** and press **Enter**, the MAC address of the management module and server blade is displayed.

```
(M,B,O,[Q]) : O (Enter)

-- MAC addresses on management module --
M controller0        controller1
- ------------------ ------------------
0 00:00:87:12:84:4A  00:00:87:12:84:4B
1 00:00:87:12:84:2E  00:00:87:12:84:2F

-- MAC addresses on server blade --
S Onboard0           Onboard1           I/O Controller     BMC
- ------------------ ------------------ ------------------ ------------------
1 00:30:48:D0:ED:96  00:30:48:D0:ED:97  00:30:48:D0:ED:98  00:30:48:D0:ED:99
2 00:30:48:D0:EC:C2  00:30:48:D0:EC:C3  00:30:48:D0:EC:C4  00:30:48:D0:EC:C5
3 00:30:48:D0:ED:1A  00:30:48:D0:ED:1B  00:30:48:D0:ED:1C  00:30:48:D0:ED:1D
4 00:30:48:D0:ED:26  00:30:48:D0:ED:27  00:30:48:D0:ED:28  00:30:48:D0:ED:29
5 00:30:48:D0:ED:6A  00:30:48:D0:ED:6B  00:30:48:D0:ED:6C  00:30:48:D0:ED:6D
6 00:30:48:D0:EC:B6  00:30:48:D0:EC:B7  00:30:48:D0:EC:B8  00:30:48:D0:EC:B9
7 00:30:48:D0:ED:8E  00:30:48:D0:ED:8F  00:30:48:D0:ED:90  00:30:48:D0:ED:91

Hit enter key. (Enter)
```

❑ XD command

You can execute diagnostics. Enter XD at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> XD (Enter)

<< XD - Execute diagnostics. >>

-- Diagnostics menu --
    I. ICMP Ping.
    Q. Quit.
(I,[Q]) :
```

Select a menu item in the table below to execute the function.

Menu		Description
I.	ICMP Ping.	Check the network connection using the Internet Control Message Protocol (ICMP) Ping.
Q.	Quit	Quits the XD command.

If you enter [I] in the **XD command** menu and press **Enter**, the prompt is ready for the IP address. When pressing **Enter** during the prompt for IP address, the screen goes back to the **XD command** menu. Enter the IP address at the prompt. A confirmation message appears to confirm executing diagnostics. At the prompt, enter Y and press **Enter**. Diagnostics are executed and the result is displayed. To cancel diagnostics, enter N and press **Enter**, or just press **Enter**.

```
(I,[Q]) : I (Enter)
Input IP address ([Q=Quit]) : 192.168.0.253 (Enter)

Confirm? (Y,[N]) : Y

PING 192.168.0.253 (192.168.0.253): 56 data bytes
64 bytes from 192.168.0.253: icmp_seq=0 ttl=64 time=3.2 ms
64 bytes from 192.168.0.253: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 192.168.0.253: icmp_seq=2 ttl=64 time=0.2 ms

--- 192.168.0.253 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/1.2/3.2 ms

Hit enter key. (Enter)
```

❑ MLC command

You can display the network setting for maintenance. Enter `MLC` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> MLC (Enter)

<< MLC - Maintenance LAN setting. >>

-- Management module --
M IP address      Subnetmask
- ---------------- ---------------
0 192.168.254.  1 255.255.255. 0
1 192.168.254.  2 255.255.255. 0

-- static route --
Network address   : 0. 0. 0. 0
Subnetmask        : 0. 0. 0. 0
Router IP address : 0. 0. 0. 0

-- Maintenance LAN setting menu --
    Q. Quit.
([Q]) :
```

Select a menu item from the table below to execute it.

Menu		Description
Q.	Quit	Quits the MLC command.

Items per management module on the screen are described in the table below.

Menu	Description
IP address	IP address of the interface for the maintenance network of the management module.
Subnetmask	Subnetmask of the interface for the maintenance network of the management module.

Items of the static route are described in the table below.

Menu	Description
Network address	Network address of a network targeted for static routing.
Subnetmask	Subnetmask of a network targeted for static routing.
Router IP address	IP address of a router transferring to targeted network for static routing.

❑ ILC command

You can set the internal network setting. Enter `ILC` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> ILC (Enter)

<< ILC - Internal LAN setting. >>

-- Internal network --
Network address : 192.168.253. 0
Subnetmask      : 255.255.255. 0

-- Internal network menu --
E. Edit setting.
Q. Quit.
(E,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
E.	Edit setting.	Sets the internal network.
Q.	Quit	Quits the ILC command.

Items displayed on the screen are described in the table below.

Item	Description
Network address	Network address of internal network Default value: 192.168.253.0
Subnetmask	Subnetmask of internal network Default value: 255.255.255.0



Do not set the internal network address to 192.168.0.0 or 192.168.254.0 in the internal network setting.

If you enter E in the **ILC command** menu and press **Enter**, the current setting is displayed. At the prompt, enter an internal network address, and the changed setting value is displayed. Then a warning message is displayed saying that the management module will restart after the setting change. A confirmation message appears. At the prompt, enter Y and press **Enter**. The internal network setting is saved. Then the management module will restart. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(E,[Q]) : E(Enter)
Network address : 192.168.253. 0
([Unchange]) : 192.168.200.0(Enter)

-- Internal network --
Network address : 192.168.200. 0
Subnetmask      : 255.255.255. 0

WARNING : If confirm, management module restart and this connect is lost.

Confirm? (Y,[N]) : Y(Enter)
- <Management module0> Restarting
```



Do not change the internal network address while the server blade is operating, which causes the management module to restart. If you do, error events, which have occurred while the management module is restarting, may not be detected.

When changing the internal address while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

External server connection manager

❑ BSM command

You can display and set the connection setting to ServerConductor/Blade Server Manager (SC/BSM). Enter BSM at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> BSM (Enter)

<< BSM - SC/BSM setting. >>

-- Manager setting --
No. Name            IP address       Alert level
--- --------------- ---------------- -----------
0   BSM_0           192.168. 0.254   All
1   -------------    -------------    ---------
2   -------------    -------------    ---------
3   -------------    -------------    ---------

-- SC/BSM setting menu --
   M. Edit manager setting.
   D. Delete manager setting.
   DB. Show/Edit basis detail setting.
   DM. Show/Edit manager detail setting.
   T. Test N+M cold standby.
   Q. Quit.
```

Select a menu item from the table below to execute the function.

Menu		Description
M.	Edit manager setting	Edits SC/BSM connection setting.
D.	Delete manager setting	Deletes SC/BSM connection setting.
DB.	Show/Edit basis detail setting.	Shows and edits the processing details about accepting requests from SC/BSM.
DM.	Show/Edit manager detail setting.	Shows and edits details about SC/BSM connection setting.
T.	Test N+M cold standby.	Issues the alert to test the switch of the N+M cold standby environment.
Q.	Quit	Quits the BSM command.

Items displayed on the screen are described in the table below.

Item	Description
No.	SC/BSM connection setting number
Name	SC/BSM name
IP address	IP address of SC/BSM
Alert level	Alert level notified to SC/BSM All: all alerts are notified. Alert: alerts in the error level are notified. Information: alerts in the information level are notified. Disable: no alert is notified.

If you enter `M` in the **BSM command** menu and press **Enter**, you are asked to select the SC/BSM connection setting. At the prompt, enter a SC/BSM connection setting number, and the current setting is displayed in the following numerical order, or the recommended value is displayed. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	SC/BSM name
2	SC/BSM IP address
3	Alert level to notify SC/BSM

If you enter an alert level, the changed setting value is displayed. A confirmation message appears. At the prompt, enter `Y` and press **Enter**. The edited SC/BSM connection setting is saved. To cancel the setting, enter `N` and press **Enter**, or just press **Enter**.

```
(M,D,DB,DM,T,[Q]) : M (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
Name : BSM_1
([Unchange]) : (Enter)
IP address   : 0. 0. 0. 0
([Unchange]) : 192.168.0.253 (Enter)
Alert level  : All
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : 1 (Enter)

-- Manager setting --
No. Name            IP address      Alert level
--- --------------- --------------- -----------
  0 BSM_0           192.168. 0.254  All
  1 BSM_1           192.168. 0.253  Alert
  2  -------------   -------------   ---------
  3  -------------   -------------   ---------

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter D in the **BSM command** menu and press **Enter**, you are asked to select SC/BSM connection setting. At the prompt, enter a SC/BSM connection setting number, and the changed setting is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the deleted SC/BSM connection setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(M,D,DB,DM,T,[Q]) : D (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
-- Manager setting --
No. Name            IP address      Alert level
--- --------------- --------------- -----------
0 BSM_0             192.168. 0.254  All
1  -------------     -------------   ---------
2  -------------     -------------   ---------
3  -------------     -------------   ---------

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter DB in the **BSM command** menu and press **Enter**, the current setting is displayed.

```
(M,D,DB,DM,T,[Q]) : DB (Enter)
-- Basis detail setting --
Command port : 21001

-- Basis setting menu --
  S. Edit setting.
  Q. Quit.
(S,[Q]) :
```

Select a menu item from the table below to execute it.

Menu		Description
S.	Edit setting.	Edits SC/BSM setting related to command requests.
Q.	Quit	Returns to the previous menu.

If you enter S in the **BSM command** menu and press **Enter**, the current port number setting that receives requests from SC/BSM appears. At the prompt, press **Enter** or enter a port number and press **Enter**. The changed setting value is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the port number setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

The port used for connecting to SC/BSM will be closed when you perform the following setting.

1. Delete all managers for notification set in the management module.
2. Type 0 into the port number set in the management module to receive requests from SC/BSM.

```
(S,[Q]) : S (Enter)
Command port : 21001
(1-65535,[Unchange]) : 21002 (Enter)

-- Basis detail setting --
Command port : 21002

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter DM in the **BSM command** menu and press **Enter**, you are asked to select SC/BSM connection setting. At the prompt, enter the SC/BSM connection setting number specified, and the current setting is displayed.

```
(M,D,DB,DM,T,[Q]) : DM (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
-- Manager detail setting --
No. : 1
Name : BSM_1
IP address           : 192.168. 0.253
Alert port           : 20079
Alert level          : Alert
Retry interval (sec) : 5
Retry duration (min) : 10

-- Manager setting menu --
   S. Edit setting.
   Q. Quit.
(S,[Q]) :
```

Select a menu item in the table below to execute the function.

Menu		Description
S.	Edit setting.	Edits details of SC/BSM connection setting.
Q.	Quit	Returns to the previous menu.

If you enter S in the **BSM command** menu and press **Enter**, the current setting is displayed in numerical order shown in the table below. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	SC/BSM name
2	SC/BSM IP address
3	SC/BSM alert report number
4	Alert level to notify SC/BSM
5	Intervals between connection retries: 5 to 50 seconds
6	Interval duration: 4 to 20 minutes

If you enter a duration period for connection retries, the changed setting is displayed. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the SC/BSM connection setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(S,[Q]) : S (Enter)
Name : BSM_1
([Unchange]) : BSM_01 (Enter)
IP address : 192.168. 0.253
([Unchange]) : 192.168.0.254 (Enter)
Alert port : 20079
(1-65535,[Unchange]) : 20078 (Enter)
Alert level : Alert
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : 0 (Enter)
Retry interval (sec) : 5
(5-50,[Unchange]) : 6 (Enter)
Retry duration (min) : 10
(4-20,[Unchange]) : 5 (Enter)

-- Manager detail setting --
No. : 1
Name : BSM_01
IP address : 192.168. 0.254
Alert port : 20078
Alert level : All
Retry interval (sec) : 6
Retry duration (min) : 5

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```



Do not perform an N+M cold standby switching test by issuing an alert in this screen together with LPAR migration targeted to that partition. See Chapter 12: Logical partitioning manager for further information.

❑ SNM command

You can set Simple Network Management Protocol (SNMP) of the management module. Enter `SNM` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SNM (Enter)

<< SNM - SNMP setting. >>

-- SNMP agent setting --
Agent            : Enable
Contact name     : contact
Location         : location
Port number      : 161
Trap level       : All
SNMP version     : v1/v2c/v3
Engine ID string : engineid
Engine ID        : 8000007404656E67696E656964

-- SNMP manager setting --
<Manager0>
SNMP version            : v1/v2c
Hostname                : host
Port number             : 162
Community name          : com
<Manager1>
SNMP version            : v3
Hostname                : snmp.esd.hitachi.com
Port number             : 162
User name               : user
Access type             : AuthPriv
Authentication type     : MD5
Authentication password : *****
Encryption type         : DES
Encryption password     : *****
<Manager2>
SNMP version            : v1/v2c
Hostname                : ---
Port number             : 162
Community name          : ---
<Manager3>
SNMP version            : v1/v2c
Hostname                : 0.0.0.0
Port number             : 162
Community name          : ---

-- MIB information --
Version : 00-02

-- SNMP setting menu --
    A. Edit agent setting.
    M. Edit manager setting.
   DA. Delete agent setting.
   DM. Delete manager setting.
    T. SNMP trap test.
    C. Copy MIB file.
    H. Change trap message.
    Q. Quit.
(A,M,DA,DM,T,C,H,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
A.	Edit agent setting.	Sets SNMP agents.
M.	Edit manager setting.	Configures the setting necessary for SNMP manager connection.
DA.	Delete agent setting.	Deletes agent settings.
DM.	Delete manager setting.	Deletes manager settings.
T.	SNMP trap test.	Transmits the SNMP trap for tests.
C.	Copy MIB file.	Copies Management Information Base (MIB) files.
H.	Change trap message.	Selects a trap message.
Q.	Quit	Quits the SNM command.

Items of SNMP agent setting are described in the table below:

Item	Description of item	Value	Description of value
Agent	SNMP agent function	Enable	Valid
		Disable	Invalid
Contact name	System contact name (System administrator name)	Character string in ASCII	Up to 60 characters in ASCII
Location	System location: installation site	Character string in ASCII	Up to 60 characters in ASCII
Port number	Port number for SNMP agent to use	Integer	Integer between 1 and 65535: However, the value 162 is not available.
Trap level	Levels notified in SNMP trap	Disable	Nothing notified.
		Alert	Notifies reports in non-recoverable and serious level.
		Information	Notifies reports in information level.
		All	All levels are notified.
SNMP version	SNMP version	Character string in ASCII	SNMP version used by SNMP manager.* Value: v1/v2c or v1/v2c/v3
Engine ID string	A string forming an engine ID	Character string in ASCII	Available only when the SNMP version is v1/v2c/v3. A character string forming an engine ID used by agents Printable 1-byte alphanumeric characters are available: at least 1 and up to 27 characters.
Engine ID	Engine ID	Character string in ASCII	Available only when the SNMP version is v1/v2c/v3. Engine ID used by agents: automatically created with the engine ID string.

(*) When the Security strength is set to High, SNMP v3 is the only available protocol

Items of SNMP manager setting are described in the table below:

Item	Description of item	Value	Description of value
SNMP version	SNMP version	Character string in ASCII	SNMP version used by the SNMP manager. Value: v1/v2c or v3
IP address	IP address of the SNMP manager	IP address	Up to 4 IP addresses of the SNMP manager can be registered. Setting for the manager is disabled by specifying 0.0.0.0.
Port number	Port number of the SNMP manager	Integer	Integer between 1 and 65535: However, the value 161 is not available.
User Name	User name	Character string in ASCII	Available only when the SNMP version is v3. Character string in ASCII: at least 1; up to 32 characters
Access type	Access type	noAuthnoPriv	Available only when the SNMP version is v3. No authentication and encryption
		AuthnoPriv	Available only when the SNMP version is v3. With authentication but no encryption
		AuthPriv	Available only when the SNMP version v3. With authentication and encryption
Authentication type	Authentication type	MD5	Available only when the SNMP version is v3. Type: MD5
		SHA	Available only when the SNMP version is v3. Type: SHA
Authentication password	Authentication password	Character string in ASCII	Available only when the SNMP version is v3. String comprised of 8 to 64 characters in ASCII
Encryption type	Encryption type	PEM	Available only when the SNMP version is v3. Type: PEM
		DER	Available only when the SNMP version is v3. Type: DER
Encryption password	Encryption password	Character string in ASCII	Available only when the SNMP version is v3. String comprised of 8 to 64 characters in ASCII
Community name	Community name of the SNMP manager	Character string in ASCII	Available only when the SNMP version is v1/v2c. Up to 60 characters in ASCII

(*)When the Security strength is set to High, SNMP v3 is the only available protocol

MIB setting information is described in the table below.

Item	Description of item	Value	Description of value
Version	MIB file version	Character string in ASCII	-

If you enter A in the **SNMP command** menu and press **Enter**, you can set the SNMP agent setting. Required setting items are different depending on SNMP versions.

When you enter the required information, a message to confirm the SNMP agent setting appears. At the prompt, enter Y and press **Enter**, and the SNMP agent setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : A
Agent             : Disable
(0=Disable,1=Enable,[Unchange]) : 1
Contact name      :
([Unchange]) : Administrator
Location          :
([Unchange]) : A3F
Port number       : 161
(1-65535,[Unchange]) : 8161
Trap level        : All
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : 2
SNMP version      : v1/v2c
(0=v1/v2c,1= v1/v2c/v3,[Unchange]) : 1
Engine ID string : zzzzzzzzzzz
([Unchange]) : xxxxxxxxxxxxx

-- SNMP agent setting --
Agent             : Enable
Contact name      : Administrator
Location          : A3F
Port number       : 8161
Trap level        : Information
SNMP version      : v1/v2c/v3
Engine ID string : xxxxxxxxxxxxx
Engine ID         : yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

If you enter M in the **SNMP command** menu and press **Enter**, you can set the SNMP manager setting. When you enter the required information, a message to confirm the SNMP manager setting appears. At the prompt, enter Y and press **Enter**, and the SNMP agent setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : M
Select manager (0-3,[Q=Quit]) : 0
SNMP version   : v1/v2c
(0=v1/v2c,1=v3,[Unchange]) : 1
Hostname       : 0.0.0.0
([Unchange]) : 192.168.0.22
Port number    : 162
(1-65535,[Unchange]) : 8162
User name      : xxxxxx
([Unchange]) : UserName
Access type    : noAuthnoPriv
(0=noAuthnoPriv,1=AuthnoPriv,2=AuthPriv,[Unchange]) : 2
Authentication type : MD5
(0=MD5,1=SHA,[Unchange]) : 1
Authentication password : *****
([Unchange]) :
Encryption type : DES
(0=DES,1=AES,[Unchange]) : 1
Encryption password : *****
([Unchange]) :

-- SNMP manager setting --
<Manager0>
SNMP version            : v3
Hostname                : 0.0.0.0
Port number             : 162
User name               : UserName
Access type             : AuthPriv
Authentication type     : SHA
Authentication password : *****
Encryption type         : AES
Encryption password     : *****

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

If you enter DA in the **SNMP command** menu and press **Enter**, you can delete SNMP agent settings. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the SNMP agent is deleted. To cancel the deletion, enter N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : DA
-- SNMP agent setting --
Agent            : Disable
Contact name     :
Location         :
Port number      : 161
Trap level       : All
SNMP version     : v1/v2c
Engine ID string :  ---
Engine ID        :  ---

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

If you enter DM in the **SNMP command** menu and press **Enter**, you can delete SNMP manager settings. Select a manager number to delete, and a confirmation message appears. At the prompt, enter Y and press **Enter**, and the SNMP manager setting is deleted. To cancel the deletion, enter N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : DM
Select manager (0-3,[Q=Quit]) : 0

-- SNMP manager setting --
<Manager0>
SNMP version            : v1/v2c
Hostname                : 0.0.0.0
Port number             : 162
Community name          :  ---

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

If you enter T in the **SNMP command** menu and press **Enter**, an SNMP trap for test is sent. Enter Y in the message to confirm the test transmission and press **Enter**, and the SNMP trap for test is transmitted. To cancel the test, enter N and press **Enter**, or just press **Enter**.

```
(A,M,T,C,[Q]) : T (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Sending SNMP trap was completed.
Hit enter key. (Enter)
```

If you enter C in the **SNMP command** menu and press **Enter**, a copy of the MIB file is mirrored into the user directory. Enter Y in the message to confirm the copy execution, and press **Enter** to copy it. To cancel the copy process, enter N and press **Enter**, or just press **Enter**.

```
(A,M,T,C,[Q]) : C (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Copying MIB file was completed.
Hit enter key. (Enter)
```

Enter H in the **SNMP command** menu and press **Enter** to set a trap message. When you select BSM or HCSM on which the trap message is based on, **Confirm?** is shown. Enter Y and press **Enter** to set the trap message. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
Trap message : BSM
(0=BSM,1=HCSM,[Unchange]) : 1

Confirm? (Y,[N]) : Y
- Changing trap message was completed.
Hit enter key.
```

❑ MI command

You can set e-mail notification settings. Enter `MI` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> MI (Enter)

<< MI - E-mail notification. >>

-- E-mail setting menu --
    C. Show e-mail setting.
    E. Edit e-mail notification setting.
    A. Edit e-mail address.
    M. Send e-mail notification.
    Q. Quit.
(C,E,A,M,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
C.	Show e-mail setting.	Displays the e-mail settings.
E.	Edit e-mail notification setting.	Sets the e-mail notification.
A.	Edit e-mail address.	
M.	Send e-mail notification.	
Q.	Quit.	Quits the MI command.

If you enter C in the **MI command** menu and press **Enter**, you can display the e-mail notification settings.

```
(C,E,A,M,[Q]) : C (Enter)
-- E-mail notification setting --
Notification : Enable
Address      : dish@hitachi.com
Host (FQDN)  : bs2kfw.com
Comment      : test
SMTP server  : 192.168.0.76
Port number  : 25

-- E-mail authentication setting --
Authentication : Enable
Name           : auth
Method         : PLAIN

-- E-mail encryption setting --
Encryption   : Disable
Protocol     : SSL

-- E-mail address --
<Address0>
Nickname  : user0
Address   : user0@one8647.com
Attach    : Yes
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Hit enter key. (Enter)
```

If you enter E in the **MI command** menu and press **Enter**, you can display the **e-mail notification setting** menu.

```
(C,E,A,M,[Q]) : E (Enter)
-- E-mail notification setting menu --
    E. Edit notification setting.
    R. Reset notification setting.
    Q. Quit.
(E,R,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
E	Edit notification setting.	
R.	Reset notification setting.	
Q.	Quit	Returns to the previous menu.

E-mail notification settings are described in the table below.

Item	Description of item	Value	Description of value
Notification	Enable or Disable the e-mail notification	Enable	Valid
		Disable	Invalid
Address	e-mail address of the system administrator	Character string in ASCII	Up to 64 characters in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “_”, “.”, “[”, “]”. Make sure to specify the system administrator’s e-mail address when the e-mail notification function is enabled.
Host (FQDN)	Host name (FQDN)	Character string in ASCII	Host name of the management module. Enter the full qualified domain name. Up to 64 characters in ASCII Make sure to specify the host name when the e-mail notification function is enabled.
Comment	Comment for information to identify a customer	Character string in ASCII	Up to 32 characters in ASCII
SMTP server	SMTP server	Character string in ASCII	IP address of the SMTP server or the SMTP server host name Up to 64 characters in ASCII Make sure to specify the SMTP server when the e-mail notification function is enabled.
Authentication	SMTP authentication	Enable	Valid
		Disable	Invalid
Name	Account name for SMTP authentication	Character string in ASCII	Account name that is registered in the SMTP server Up to 64 characters in ASCII Make sure to specify an account name for SMTP authentication when the SMTP authentication function is enabled.
Password	Password for SMTP authentication	Character string in ASCII	Password for the account that is registered in the SMTP server. Up to 64 characters in ASCII Make sure to specify a password for SMTP authentication when the SMTP authentication function is enabled.

Item	Description of item	Value	Description of value
Method	SMTP authentication method	PLAIN	Plain text method for authentication: The account name and password are sent together.
		LOGIN	Plain text method for authentication: The account name and password are sent separately.
		CRAM-MD5	Challenge-response method authentication mechanism Uses MD5 when a message digest is created.
Encryption		Enable	Valid
		Disable	Invalid
Protocol	Protocol used when encryption is enabled	SSL	Secure Socket Layer
		TSL	Transport Layer Security
Port number	Port number of the SMTP server	Integer	1 to 65535

If you enter E and press **Enter** in the **e-mail notification setting** menu, you can change and delete the e-mail notification setting.

The current setting is displayed in numerical order shown in the table below. At the prompt, to proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	Enable or Disable the e-mail notification.
2	e-mail address of the system administrator
3	Host name (FQDN)
4	Comment for information to identify a customer
5	SMTP server
6	Enable or Disable SMTP authentication.
7	Account name for SMTP authentication
8	Password for SMTP authentication
9	Method for SMTP authentication
10	Enable or Disable for encryption function.
11	Method for encryption
12	Port number for a SMTP server
Note: When you disable the e-mail notification, no prompt is available for menu items 2 to 12.. When you disable SMTP authentication, no prompt is available for menu items 7 to 9. When you disable encryption, no prompt is available for menu item 11.	

After the input, the new setting value is displayed. When the retry notification is scheduled, a message appears to show that the notification will be processed with the latest setting. A confirmation message appears. At the prompt, enter `Y` and press **Enter**, and the e-mail notification setting is saved. To cancel the setting, enter `N` and press **Enter**, or just press **Enter**.

```
(E,R,[Q]) : E (Enter)
Notification : Enable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Address :
([Unchange]) : dish@hitachi.com (Enter)
Host (FQDN) :
([Unchange]) : bs2kfw.com (Enter)
Comment :
([Unchange]) : test (Enter)
SMTP server :
([Unchange]) : 192.168.0.76 (Enter)
Authentication : Disable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Name          :
([Unchange]) : admin (Enter)
Password      : *****
([Unchange]) :
Method        : PLAIN
(0=PLAIN,1=LOGIN,2=CRAM-MD5,[Unchange]) : 2 (Enter)
Encryption    : Disable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Protocol      : SSL
(0=SSL,1=TLS,[Unchange]) : 1 (Enter)
Set port number to 587? (Y,[N]) : N (Enter)
Port number :
(1-65535,[Unchange]) : 25 (Enter)

-- E-mail notification setting --
Notification : Enable
Address : dish@hitachi.com
Host (FQDN) : bs2kfw.com
Comment : test
SMTP server : 192.168.0.76
Port number : 25

-- E-mail authentication setting --
Authentication : Enable
Name           : admin
Method         : CRAM-MD5

-- E-mail encryption setting --
Encryption    : Enable
Protocol      : TLS

WARNING : If e-mail notification is scheduled to retry, the latest
setting will be in effect.

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter R and press **Enter** in the **e-mail notification setting** menu, you can initialize the e-mail notification setting.

A setting value and notification retry are scheduled. A message appears showing that the notification will be processed with the latest setting. A confirmation message appears. At the prompt, enter Y and press **Enter**, and the e-mail notification setting is saved. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(E,R,[Q]) : R (Enter)
-- E-mail notification setting --
Notification : Disable
Address      :
Host (FQDN)  :
Comment      :
SMTP server  :
Port number  : 25

-- E-mail authentication setting --
Authentication : Disable
Name           :
Method         : PLAIN

-- E-mail encryption setting --
Encryption   : Disable
Protocol     : SSL

WARNING : If e-mail notification is scheduled to retry, the latest
setting will be in effect.

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter A in the **MI command** menu and press **Enter**, the e-mail address setting menu is displayed.

```
(C,E,A,M,[Q]) : A (Enter)
-- E-mail address setting menu --
   E. Edit e-mail address.
   D. Delete e-mail address.
   Q. Quit.
(E,D,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
E.	Edit e-mail address.	
D.	Delete e-mail address.	
Q.	Quit	Returns to the previous menu.

E-mail address settings are described in the table below.

Item	Description of item	Value	Description of value
Nickname	Nickname of the destination to send notification	Character string in ASCII	Nickname of the address: up to 15 characters in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “ _ ”, “ . ”, “[”, “]”.
Address	E-mail address of the destination to send notification	Character string in ASCII	Up to 64 characters in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “ _ ”, “ . ”, “[”, “]”.
Attach	With or Without a log file: notification to the destination	Yes	Notification with a log file to be sent to the destination
		No	Notification without a log file to be sent to the destination

If you enter E in the **e-mail notification** menu and press **Enter**, you can edit the e-mail address.

The current address list is displayed, and the prompt is ready for an address number. Enter an address number. The current setting is displayed in numerical order as shown in the following table. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	Address name for notification to be sent
2	e-mail address for notification to be sent
3	With or without a log file: notification to the address

Enter `Yes` or `No` to attach a log file to the e-mail, and the changed value is displayed. A confirmation message appears. At the prompt, enter `Y` and press **Enter**, and the setting is saved. To cancel the setting change, enter `N` and press **Enter**, or just press **Enter**.

```
(E,D,[Q]) : E (Enter)
-- E-mail address --
<Address0>
Nickname : user0
Address  : user0@one8647.com
Attach   : Yes
<Address1>
Nickname : ----------
Address  : ----------
Attach   : No
<Address2>
Nickname : ----------
Address  : ----------
Attach   : No
<Address3>
Nickname : ----------
Address  : ----------
Attach   : No

Select address (0-3,[Q=Quit]) : 0 (Enter)

Nickname  : user0
([Unchange]) : USER0 (Enter)
Address   : user0@one8647.com
([Unchange]) : (Enter)
Attach   : Yes
(0=No,1=Yes,[Unchange]) : (Enter)

-- E-mail address --
<Address0>
Nickname : USER0
Address : user0@one8647.com
Attach  : Yes
<Address1>
Nickname : ----------
Address  : ----------
Attach   : No
<Address2>
Nickname : ----------
Address  : ----------
Attach   : No
<Address3>
Nickname : ----------
Address  : ----------
Attach : No

Confirm? (Y,[N]) : Y (Enter)
- <Address0> Writing setting was completed.
Hit enter key. (Enter)
```

If you enter D in the **e-mail address** menu and press **Enter**, you can delete an e-mail address.

The list including the current addresses is displayed and the prompt is ready for an address number. Enter an address number to delete an e-mail address. A confirmation message appears. At the prompt, enter Y and press **Enter**. The selected address is deleted. To cancel the setting change, enter N and press **Enter**, or just press **Enter**.

```
(E,D,[Q]) : D (Enter)
-- E-mail address --
<Address0>
Nickname : user0
Address  : user0@one8647.com
Attach   : Yes
<Address1>
Nickname : -----------
Address  : -----------
Attach   : No
<Address2>
Nickname : -----------
Address  : -----------
Attach   : No
<Address3>
Nickname : -----------
Address  : -----------
Attach   : No

Select address (0-3,[Q=Quit]) : 0 (Enter)

-- E-mail address --
<Address0>
Nickname : -----------
Address  : -----------
Attach   : No
<Address1>
Nickname : -----------
Address  : -----------
Attach   : No
<Address2>
Nickname : -----------
Address  : -----------
Attach   : No
<Address3>
Nickname : -----------
Address  : -----------
Attach   : No

Confirm? (Y,[N]) : Y (Enter)
- <Address0> Writing setting was completed.
Hit enter key. (Enter)
```

If you enter M in the **MI command** menu and press **Enter**, the manual e-mail notification menu is displayed.

```
(C,E,A,M,[Q]) : M (Enter)
-- Manual e-mail notification menu --
   N. Send latest log data.
   H. Select from notification history.
   Q. Quit.
(N,H,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
N.	Send latest log data.	Collects the latest log data and sends them via e-mail.
H.	Select from notification history.	Selects a log from the notification history and sends e-mail notification.
Q.	Quit	Returns to the previous menu.

If you enter N in the manual **e-mail notification** menu and press **Enter**, the address list, including addresses currently registered, is displayed. When you specify an address, a message indicating that it takes a few minutes to put out the log to the file is displayed. Then a message appears to confirm the e-mail transmission. At the prompt, enter Y and press **Enter**, and the log is put out to the file; the e-mail will be sent to the selected address. To cancel the e-mail transmission, enter N and press **Enter**, or just press **Enter**.

```
(N,H,[Q]) : N (Enter)
-- E-mail address --
<Address0>
Nickname : USER0
Address  : user0@mail.hitachi.com
Attach   : Yes
<Address1>
Nickname : -----------
Address  : -----------
Attach   : No
<Address2>
Nickname : -----------
Address  : -----------
Attach   : No
<Address3>
Nickname : -----------
Address  : -----------
Attach   : No

Select address (0-3,A=All,[Q=Quit]) : A (Enter)

WARNING : If confirm, it will take few minutes to dump log to file.

Confirm? (Y,[N]) : Y (Enter)

- <Address0> Sending e-mail notification was completed.

Hit enter key. (Enter)
```

If you enter `H` in the **manual e-mail notification** menu and press **Enter**, the notification history is displayed. When you specify a number from the notification history, the e-mail notification text, including the currently registered addresses, is displayed. Select an address number at the prompt. When you specify an address, a confirmation message appears. At the prompt, enter `Y` and press **Enter**, and the file containing the log corresponding to the notification history is sent out; the e-mail will be sent to the selected address. To cancel the e-mail transmission, enter `N` and press **Enter**, or just press **Enter**.

```
(N,H,[Q]) : H (Enter)
-- Notification history --
                                          Result
No. Timestamp           System event log      0123
--- ------------------- --------------------- ------
  0 2009-02-26 09:30:13 6100 04 0932 0BA5FFFF CCCC
  1 2009-02-26 09:33:01 6100 04 0205 01599988 CCCC
  2 2009-02-26 11:07:19 6100 04 0932 0BA5FFFF O---
  3 2009-02-26 11:24:11 6100 04 0932 0BA5FFFF X---
  4 2009-02-26 11:45:43 6100 04 0932 0BA5FFFF CCCC
  5 2009-02-26 11:52:19 6100 04 0932 0BA5FFFF CCCC
  6 2009-02-26 11:56:29 6100 04 0932 0BA5FFFF O---
  7 2009-02-26 12:54:51 6100 04 0932 0BA5FFFF X---
  8 2009-02-26 13:06:08 6100 04 0932 0BA5FFFF X---
  9 2009-02-26 13:14:47 6100 04 0932 0BA5FFFF X---
 10 2009-02-26 13:35:10 6100 04 0932 0BA5FFFF X---
 11 2009-02-26 14:04:42 6100 04 0932 0BA5FFFF X---
 12 2009-02-26 14:09:48 6100 04 0932 0BA5FFFF X---
 13 2009-02-26 14:20:11 6100 04 0932 0BA5FFFF X---
 14 2009-02-26 14:30:37 6100 04 0932 0BA5FFFF X---
 15 2009-02-27 09:25:39 6100 04 0932 0BA5FFFF X---
 16 2009-02-27 10:10:20 6100 04 0932 0BA5FFFF X---
 17 2009-02-27 10:44:17 6100 04 0932 0BA5FFFF X---
 18 2009-02-27 10:50:34 6100 04 0932 0BA5FFFF X---
 19 2009-02-27 13:51:38 6100 04 0932 0BA5FFFF X---
 20 2009-02-27 15:15:56 6100 04 0932 0BA5FFFF X---
 21 2009-02-27 16:16:36 6100 04 0932 0BA5FFFF X---
 22 2009-02-27 20:39:17 6100 04 0932 0BA5FFFF X---
 23 2009-03-02 14:02:02 6100 04 0932 0BA5FFFF X---
 24 2009-03-02 14:13:25 6100 04 0932 0BA5FFFF X---
 25 2009-03-02 14:25:35 6100 04 0932 0BA5FFFF X---
 26 2009-03-02 14:40:51 6100 04 0932 0BA5FFFF X---
 27 2009-03-02 15:48:02 6100 04 0932 0BA5FFFF X---
 28 2009-03-02 16:46:08 6100 04 0932 0BA5FFFF X---
 29 2009-03-02 17:44:30 6100 04 0932 0BA5FFFF X---
 30 2009-03-02 18:02:52 6100 04 0932 0BA5FFFF X---
 31 2009-03-02 18:15:40 6100 04 0932 0BA5FFFF X---


Select No. (0-31,[Q=Quit]) : 31 (Enter)

The trouble occurred by the following device.

--- Server chassis ---
Part/Model Number : aaa
Serial Number     : 1
Model ID          : BS2000 (00)
Backplane ID      : Basic Model (00)
Chassis ID        : svp #2

+------------------------------+
| MARLOG (2009-05-17 22:31:59) |
+------------------------------+
-- CALL FACTOR INFORMATION --
Reason : 09
Impact : UU

-- RC INFORMATION --
EVENT         : 0000 02 5F90104A 6100 04 0932 0BA5FFFF
RC            : 10 6201 10 09320000 0BA5FFFF
RC NAME       : PSM REDUNDANCY
COMMENT       : Power Supply module#z: Operated without Redundancy (<N)

(1) Check the AC input, (2) Check the Power Supply configuration, (3)
Replace Power Supply module which is determined from previous SEL.
```

```
-- FRU INFORMATION --
+---+-------------------------------------------------------------------+
| 1 | UNIT         : OTHER              FRU MNEMONIC : BUNDEN           |
|   | PARTS NAME   :  -                 REV          :  -               |
|   | ACTION       : CHK                WEIGHT       : 50               |
|   | DRAWING NO   : MAP_CHECK          SERIAL NO    :  -               |
+---+-------------------------------------------------------------------+
| 2 | UNIT         : SYS                FRU MNEMONIC : PSALL            |
|   | PARTS NAME   :  -                 REV          :  -               |
|   | ACTION       : CHK                WEIGHT       : 50               |
|   | DRAWING NO   : MAP_CHECK          SERIAL NO    :  -               |
+---+-------------------------------------------------------------------+


-- E-mail address --
<Address0>
Nickname : USER0
Address : user0@mail.hitachi.com
Attach  : Yes
<Address1>
Nickname : ------------
Address  : ------------
Attach   : No
<Address2>
Nickname : ------------
Address  : ------------
Attach   : No
<Address3>
Nickname : ------------
Address  : ------------
Attach   : No

Select address (0-3,A=All,[Q=Quit]) : A (Enter)

WARNING : If confirm, it will take few minutes to dump log to file.

Confirm? (Y,[N]) : Y (Enter)

- <Address0> Sending e-mail notification was completed.

Hit enter key. (Enter)
```

Notification history items are described in the table below.

Item	Description of item	Value	Description of value
No.	Notification history number	Integer	Serial number: 0 to 31
Timestamp	When the event to trigger e-mail notification happens.	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second

Item	Description of item	Value	Description of value
System Event Log		gggg ee ssSS ee11223344	gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3
Result	E-mail notification result	-	Not targeted
		O	Notification is successful.
		X	Notification fails.
		R	Notification fails: Wait for a retry.
		C	Collecting logs.

❑ HA command

This command cannot function with this system equipment.

❑ LDAP command

You can display and set the connection to the directory service. Enter `LDAP` at the prompt, and press **Enter**.

```
<< LDAP - Directory service setting. >>

-- Directory service setting menu --
    D. Show directory service setting.
    C. Edit connection setting.
    S. Edit directory search setting.
    A. Edit group authentication setting.
    R. Reset directory service setting.
    Q. Quit.
(D,C,S,A,[Q]) :
```

Select a menu item in the table below to execute a function.

Menu		Description
D.	Show directory service setting.	-
C.	Edit connection setting.	Edits the connection setting among directory service settings.
S.	Edit directory search setting.	Edits the search setting among directory service settings.
A.	Edit group authentication setting.	Edits the group authentication setting among directory service settings.
R.	Reset directory service setting.	Initializes the directory service settings.
Q.	Quit	Quits the LDAP command.

Select D from the menu to display the directory service settings.

```
-- connection setting --
LDAP          : Enable
LDAP server 0 : esdadmin@hitachi.com
LDAP server 1 : 192.168.1.200
LDAP server 2 :
Port number   : 636
Bind DN       : bind

-- directory search setting --
Base DN            : testname
Login ID attribute : loginid_attribute
Role attribute     : role_attribute

-- group authentication setting --
Group member attribute : member_attribute
Group DN 0             : GDN1
Group DN 1             : GDN2
Group DN 2             : GDN3
Group DN 3             :
Group DN 4             :

Hit enter key.
```

LDAP connection information items are described in the table below.

Item	Description of item	Value	Description of value
LDAP	Enable or Disable LDAP	Enable/Disable	Setting values, Enable and Disable, are saved and displayed, including settings for connection, directory, and group.
LDAP server 0 to 2	LP address of LDAP servers	A string in FQDN or IPv4 format	IP address of the LDAA server: Up to 127 characters A blank space is not available for the head and end of the string. Available characters: alphabet [A-Z; a-z], numbers [0-9], hyphen “-“, and period “.”.
Port number	-	1-65535	Port number used with the LDAP function.
Bind DN	-	A string in ASCII	Bind DN in the LDAP server: Up to 256 characters A blank space is not available for the head and end of the string.
Password	Bind password	Character(s) in ASCII	Password used for bind to the LDAP server: From one to 32 character(s) including a blank space.
Retype password	Bind password to retype	Character(s) in ASCII	Retyping the bind password above.

Items of the directory search setting are described in the table below:

Item	Description of item	Value	Description of value
Base DN	-	Character(s) in ASCII	Base DN in the LDAP server: 1 up to 256 characters A blank space is not available for the head and end of the string.
Login ID attribute	Attributes to show the login ID	Character(s) in ASCII	Attributes to the login ID: 1 to up to 64 characters A blank space is not available for the head and end of the string. Available for the 1st character: an alphabet [A-Z; a-z] For the other characters: alphanumeric [0-9] and [A-Z; a-z].
Role attribute	Attributes to express the role	Character(s) in ASCII	Attributes to the role: 1 to up to 64 character(s) A blank space is not available for the head and end of the string. Available for the 1st character: an alphabet [A-Z; a-z] For the other characters: alphanumeric [0-9] and [A-Z; a-z].

Items of the group authentication setting are described in the table below.

Item	Description of item	Value	Description of value
Group member	Attributes to show group members	Character(s) in ASCII	Attributes to group members: 1 up to 64 characters A blank space is not available for the head and end of the string. Available for the 1st character: an alphabet [A-Z; a-z] For the other characters: alphanumeric [0-9] and [A-Z; a-z].
Group DN 0 to 4	Group DN 0 to 4 with permission to log in.	Character(s) in ASCII	Group DN allowed to login: 1 up to 256 character(s) A blank space is not available for the head and end of the string.

Type C from the menu and press **Enter** to edit the directory service connection settings. For port numbers, you can set whether or not to set the default value. For bind DN, you can select whether or not to set Anonymous connection. After setting those, the new setting and the confirmation message are displayed. To apply the new directory service connection setting, enter Y and press **Enter**. To cancel settings, enter N, or just press **Enter**.

```
LDAP          : Enable
(0=Disable,1=Enable,[Unchange]) : 1
LDAP server 0 : esdadmin@hitachi.com
([Unchange]) : esdadmin@hitachi.com
LDAP server 1 : 192.168.1.200
([Unchange]) : 192.168.1.200
LDAP server 2 :
([Unchange]) :
Set port number to 636? (Y,[N]) : N
Port number   : 636
(1-65535,[Unchange]) : 636
Set Bind DN to Anonymous? (Y,[N]) : N
Bind DN       : bind
([Unchange]) : bind
Password       : *****
([Unchange]) : (will not echo back.)
Retype password : (will not echo back.)

-- connection setting --
LDAP          : Enable
LDAP server 0 : esdadmin@hitachi.com
LDAP server 1 : 192.168.1.200
LDAP server 2 :
Port number   : 636
Bind DN       : bind

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Type `S` from the menu and press **Enter** to edit the directory search settings. After setting it, the new setting and the confirmation message are displayed. To apply the new directory search setting, enter `Y` and press **Enter**. To cancel settings, enter `N` or just press **Enter**.

```
Base DN  : testname
([Unchange]) : testname
Login ID attribute: loginid_attribute
([Unchange]) : loginid_attribute
Role attribute : role_attribute
([Unchange]) : role_attribute

-- directory search setting --
Base DN            : testname
Login ID attribute : loginid_attribute
Role attribute     : role_attribute

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key
```

Type A from the menu and press **Enter** to edit the group authentication settings. You can select whether or not to use group member attributes. After setting it, the new setting and confirmation message are displayed. To apply the new group authentication setting, enter Y and press **Enter**. To cancel settings, enter N, or just press **Enter**.

```
Set Group member attribute to unuse? (Y,[N]) : N
Group member attribute: member_attribute
([Unchange]) : member_attribute
Group DN 0   : GDN1
([Unchange]) : GDN1
Group DN 1   : GDN2
([Unchange]) : GDN2
Group DN 2   : GDN3
([Unchange]) : GDN3
Group DN 3   :
([Unchange]) :
Group DN 4   :
([Unchange]) :

-- group authentication setting --
Group member attribute : member_attribute
Group DN 0             : GDN1
Group DN 1             : GDN2
Group DN 2             : GDN3
Group DN 3             :
Group DN 4             :

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key
```

Type R from the menu and press **Enter** to go to the reset menu. To reset the directory service connection setting, type C; to reset directory search setting, D; to reset group authentication setting, type G; to reset all LDAP settings, type A. After setting it, the new setting and the confirmation message are displayed. To reset the setting, enter Y and press **Enter**. To cancel settings, enter N, or just press **Enter**.

```
--- Reset directory service setting menu ---
    C. Connection setting.
    D. Directory search setting.
    G. Group authentication setting.
    A. All LDAP setting.
    Q. Quit.
(C,D,G,A,[Q]) :C

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

❑ HCSM command

You can set the HCSM (Hitachi Compute Server Manager). Enter `HCSM` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> HCSM (Enter)

<< HCSM - HCSM setting. >>

-- HCSM service setting --
HCSM           : Enable
Access control : Disable
Port number    : 443
Account        : Compute

-- HCSM server setting --
                                                Retry    Retry
No. IP address      Alert port Alert level      interval Duration Session
--- --------------- ---------- ------------- -------- -------- -------------
  1 192.168.  0. 20      26119 Warning              2       10 Connected
  2 192.168.  0. 51      26119 All                  2       10 Not connected

-- HCSM setting menu --
    A. Edit HCSM service.
    M. Edit HCSM server.
    D. Disconnect session.
    S. Send alert.
    Q. Quit.
(A,M,D,S[Q]) :
```

Select a menu item from the following list, and execute it.

Menu		Description
A.	Edit HCSM service.	Sets the HCSM service.
M.	Edit HCSM server.	Sets the HCSM server.
D.	Disconnect session.	Disconnects the session.
S.	Send alert.	Sends a test alert.
Q.	Quit.	Quits the HCSM command.

HCSM service settings are described in the table below:

Item	Description of item	Value	Description of value
HCSM	Enable or Disable HCSM	Enable	Enables HCSM.
		Disable	Disables HCSM.
Access control	Access control	Enable	Responds to a discovery only from the registered HCSM server.
		Disable	Responds to a discovery from HCSM servers, both registered and not-registered.
Port number	Port number used by HTTP/HTTPS server	Integer	Integer: 1 up to 65535
Account	HCSM account	A string in ASCII	ASCII characters: 1 up to 32

HCSM server settings are described in the table below:

Item	Description of item	Value	Description of value
No.	Number	Integer	Serial number
IP address	-	IP address format	HCSM server IP address
Alert level	-	All	Notifies all alerts including Warning, Failure, and Information.
		Warning	Notifies alerts including Warning and Failure.
		Failure	Notifies Failure alerts.
		Do not notify	Notifies no alert.
Retry interval	Retry interval for alert notification attempts	Integer	Integer: 1 up to 4 (minutes)
Retry duration	Retry duration for an alert notification attempt	Integer	Integer: 4 up to 15 (minutes)
Session	-	Connected	Being connected
		Not connected	Disconnected

Type A in the **HCSM command** menu and press **Enter** to set HCSM service. Current values are shown in the following order. Press **Enter** or type a new value and press **Enter** to go to the next item.

Order	Setting item
1	HCSM
2	Access control

A message asks whether or not to use default account settings for HCSM account and password; the prompt is ready. To apply the default values to HCSM account and password, type Y and press **Enter**. To set a new account and password, type N and press **Enter** or just press **Enter**.

When the account and password are entered, HCSM service settings will be shown. Confirm is displayed and the prompt is ready. To apply the HCSM service settings, type Y and press **Enter**. To cancel the settings, type N and press **Enter**.

```
HCSM                : Enable
(0=Disable,1=Enable,[Unchange]) : 0
Access control      : Disable
(0=Disable,1=Enable,[Unchange]) : 1
Use default account setting (Y,[N]) : N
Account             : Compute
([Unchange]) : Hitachi
Password            :
Retype password     :

-- HCSM service setting --
HCSM           : Enable
Access control : Disable
Port number    : 443
Account        : Compute

Confirm (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Type M in the **HCSM command** menu, and press **Enter** to display the HCSM server setting menu.

```
-- HCSM server setting -

                                          Retry    Retry
No. IP address      Alert port Alert level   interval Duration Session
--- --------------- ---------- ------------- -------- -------- -------------
  1 192.168.  0. 20      26119 Warning              2       10 Connected
  2 192.168.  0. 51      26119 All                  2       10 Not connected

-- HCSM server setting menu --
    A. Add HCSM server.
    M. Modify HCSM server.
    D. Delete HCSM server.
    Q. Quit.
(A,M,D,[Q]) :
```

Select a menu item from the following list, and execute it.

Menu		Description
A.	Add HCSM server.	Adds the HCSM server.
M.	Modify HCSM server.	Modifies the HCSM server.
D.	Delete HCSM server.	Deletes the HCSM server.
Q.	Quit.	Quits the LDAP command.

Type A in the **Modify HCSM server** menu and press **Enter** to add the HCSM server settings. Type values for IP address, Alert port, Alert level, Retry interval (min), Retry duration (min) to display HCSM sever settings to add. Confirm is displayed and the prompt is ready. To add the HCSM server, type Y and press **Enter**. To cancel it, type N and press **Enter**.

```
IP address           : 192.168.0.110
Alert port           : 26119
(1-65535,[Unchange]) : 12345
Alert level          : All
(0=All,1=Warning,2=Failure,3=Do not notify,[Unchange]) : 0
Retry interval (min) : 2
(1-4,[Unchange]) : 1
Retry duration (min) : 10
(4-15,[Unchange]) : 15

-- HCSM server setting --
IP address           : 192.168.  0.110
Alert port           : 12345
Alert level          : All
Retry interval (min) : 1
Retry duration (min) : 15

Confirm (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Type M in the **Modify HCSM server** menu and press **Enter** to modify HCSM server settings. Select an HCSM server number to modify, and type values for IP address, Alert port number, Alert level, Retry interval (min), Retry duration (min) to display the new HCSM sever settings. Confirm is displayed and the prompt is ready. To confirm the new HCSM server settings, type Y and press **Enter**. To cancel it, type N and press **Enter**.

```
-- HCSM server setting --
                                          Retry    Retry
No. IP address      Alert port Alert level  interval Duration Session
--- --------------- ---------- ------------ -------- -------- -------------
  1 192.168.  0. 20      26119 Warning             2       10 Connected
  2 192.168.  0. 51      26119 All                 2       10 Not connected

Select HCSM server (1-2,[Q=Quit]) : 2
Alert port           : 26119
(1-65535,[Unchange]) : 12345
Alert level          : All
(0=All,1=Warning,2=Failure,3=Do not notify,[Unchange]) : 3
Retry interval (min) : 2
(1-4,[Unchange]) : 1
Retry duration (min) : 10
(4-15,[Unchange]) : 15

-- HCSM server setting --
                                          Retry    Retry
No. IP address      Alert port Alert level  interval Duration Session
--- --------------- ---------- ------------ -------- -------- -------------
  1 192.168.  0. 20      26119 Warning             2       10 Connected
  2 192.168.  0. 51      12345 Failure             1       15 Not connected

Confirm (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Type D in the **Modify HCSM server** menu and press **Enter** to delete HCSM server settings. Select an HCSM server number to delete. Confirm is displayed and the prompt is ready. To delete the HCSM server, type Y and press **Enter**. To cancel it, type N and press **Enter**.

```
-- HCSM server setting --
                                              Retry    Retry
No. IP address      Alert port Alert level    interval Duration Session
--- --------------- ---------- ------------- -------- -------- -------------
  1 192.168.  0. 20      26119 Warning              2       10 Connected
  2 192.168.  0. 51      26119 All                  2       10 Not connected

Select HCSM server (1-2,[Q=Quit]) : 1

Confirm (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Type D in the **HCSM command** menu and press **Enter** to disconnect an HCSM session. When you select an HCSM server number to disconnect, Confirm is displayed and the prompt is ready. To disconnect the HCSM server, type Y and press **Enter**. To cancel it, type N and press **Enter**.

```
-- HCSM server setting --
                                              Retry    Retry
No. IP address      Alert port Alert level    interval Duration Session
--- --------------- ---------- ------------- -------- -------- -------------
  1 192.168.  0. 20      26119 Warning              2       10 Connected
  2 192.168.  0. 51      26119 All                  2       10 Not connected

Select HCSM server (1-2,[Q=Quit]) : 0

Confirm (Y,[N]) : Y
- Disconnect session was completed.
Hit enter key.
```

Type S in the **HCSM command** menu and press **Enter** to show the Send alert menu.

```
(A,M,D,S,[Q]) : S (Enter)

-- Partition status --
P Power        Condition      LID lamp Mode  Auto power on
- ------------ -------------- -------- ----- --------------
0 Off          Normal         On       Basic Synchronized
1 On           Normal         Off      Basic Synchronized
2  ----------   ------------   ------   ---   ------------
3 Off          Initializing   Off       ---  Synchronized
4 Powering on  Normal         Off      Basic Synchronized
5 Powering off Normal         On       LP    Synchronized
6 On           Normal         Off      Basic Synchronized
7 Off          FAIL           Off      Basic Synchronized

-- Send alert menu --
    I . N+M immediate.
    D . N+M delayed.
    Q . Quit.
(I,D,[Q]) : I (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)

WARNING : If confirm, partition0 will be powered off.

Confirm (Y,[N]) : Y (Enter)
- <Partition 0> Send alert was completed.
Hit enter key.
```

Select a menu you require from the following list, and execute it.

Menu		Description
I.	N+M immediate.	Sends an immediate failover.
D.	N+M delayed.	Sends a delayed failover.
Q.	Quit	Returns to the previous menu.

Type [I] in the menu and press **Enter** to send an immediate failover. You are prompted to enter a partition number: the prompt is ready. When you have entered a partition number, a confirmation message is displayed: the prompt is ready. To send the immediate failover, type Y and press **Enter**. To cancel the immediate failover, type N and press **Enter** or just press **Enter** after the confirmation message.

Type D and press **Enter** to send a delayed failover. You are prompted to enter a partition number: the prompt is ready. When you have entered a partition number, a confirmation message is displayed: the prompt is ready. To send the delayed failover, type Y and press **Enter**. To cancel the delayed failover, type N and press **Enter** or just press **Enter** after the confirmation message.

❑ ST Command

You can set Syslog Transfer of management modules. Type `ST` at the prompt and press **Enter**.

```
<< ST - Syslog Transfer. >>
-- Syslog transfer setting --
Syslog transfer             : Enable
Hostname of syslog server   : 192.168.0.100
Notification of audit event : Enable

-- Syslog transfer menu --
    E. Edit syslog transfer setting.
    Q. Quit.
(E,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
E.	Edit Syslog transfer setting.	Changes the Syslog transfer setting...
Q.	Quit	Quits the ST command..

Items of Syslog transfer setting are described in the following table.

Item	Description of item	Value	Description of value
Syslog transfer	Syslog transfer setting	Enable	Executes Syslog transfer.
		Disable	Not execute Syslog transfer.
Hostname of syslog server	IP address/host name for destination syslog server	Character string	Character string from one to 255; available characters: alphanumerics, period ".", and hyphen "-".
		------	Syslog transfer is disabled.
Notification of audit event	Notification setting for audit event	Enable	Executes Syslog transfer: An Audit event occurs, and the related log is sent by Syslog transfer.
		Disable	Not execute Syslog transfer.
		------	Syslog transfer is disabled.

If you enter `E` in the ST command and press **Enter**, you can edit the Syslog transfer setting. Current setting values are displayed in the following order, and the prompt is ready. Just press **Enter**, or type a setting value and press **Enter**. You will go on to the next item.

No.	Item
1	Syslog transfer
2	Host name of syslog server
3	Notification of audit event

New settings are displayed after setting is complete. A confirmation message is displayed, and the prompt is ready. To save the settings, type `Y` and press **Enter**. To cancel the settings, type `N` and press **Enter** or just press **Enter** after the confirmation message.

```
(E,[Q]) : E
Syslog transfer             : Enable
(0=Disable,1=Enable,[Unchange]) : 1
Hostname of syslog server   : 192.168.0.100
([Unchange]) : 192.168.0.120
Notification of audit event : Enable
(0=Disable,1=Enable,[Unchange]) : 0

-- Syslog transfer setting --
Syslog transfer             : Enable
Hostname of syslog server   : 192.168.0.120
Notification of audit event : Disable

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```

Managing security

❑ CER command

You can operate tasks related to public keys. Enter `CER` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> CER (Enter)

<< CER - Public key. >>

-- Public key menu --
    S. SSH host key.
    C. SSL private key and certificate.
    Q. Quit.
(S,C,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
S.	SSH host key	Operates the host key pairs of the SSH server.
C.	SSL private key and certificate	Operates the host key pairs and certificate of the SSL.
Q.	Quit	Quits the CER command.

If you enter `S` and press **Enter**, the following menu screen is displayed.

```
(S,C,[Q]) : S (Enter)
-- SSH host key menu --
   G. Generate host key.
   H. Show host key information.
   B. Backup.
   R. Restore.
   Q. Quit.
(G,H,B,R,[Q])   :
```

Select a menu item from the table below to execute the function.

Menu		Description
G.	Generate host key.	Generates host key pairs for the SSH server
H.	Show host key information.	Display information about the host key of the SSH server.
B.	Backup.	Back up the host key pairs of the SSH server.
R.	Restore.	Restore the host key pairs of the SSH server.
Q.	Quit	Return to the previous menu.

If you enter G in the **SSH host** key menu and press **Enter**, you can generate the host key pair of the SSH server. A confirmation message appears. To generate the host key pair, enter Y and press **Enter**. To cancel the host key pair, enter N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : G (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Generating host key was completed.
Hit enter key. (Enter)
```

If you enter H in the **SSH host key** menu and press **Enter**, the host key information on the SSH server is displayed.

```
(G,H,B,R,[Q]) : H (Enter)

-- Host key information --
Key length : 1024
Fingerprint : b6:16:6f:15:74:d6:89:95:86:76:b3:82:ba:89:be:b7

Hit enter key. (Enter)
```

The host key information items are described in the table below.

Item	Description of item	Value	Description of value
Key length	Host key length	Integer	Unit: bit
Fingerprint	Host key fingerprint	XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX	“XX” stands for two hexagonal figures. Alphabets from ‘a’ to ‘f’ is shown in lower case.

If you enter B in the **SSH host key** menu and press **Enter**, you can save the host key pair of the SSH server. You are prompted to enter characters used for a file name to be generated when saving. Enter the characters for the file name, and a confirmation message appears. To save the host key pair, enter Y and press **Enter**. To cancel the save, enter N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : B (Enter)

Input backup file name ([Q=Quit]) : key_000000 (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is pub-key_000000.backup.
Hit enter key. (Enter)
```

When you save the host key, the host key of the SSH server is saved in the user directory in the management module. The host key name is displayed. Press **Enter**, and the screen returns to the **SSH host key** menu. You can take out the host key file via FTP.

If you enter R in the **SSH host key** menu and press **Enter**, you can restore the host key of the SSH server. The host key list stored in the user directory is displayed. You are prompted to select a file to be restored. To restore the host key, enter Y and press **Enter**. To cancel the restore, enter N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : R (Enter)

-- Backup file list --
<File0>
pub-key_000000.backup
<File1>
pub-test.backup

Select backup file (0-1,[Q=Quit]) : 0 (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Restoring backup data was completed.
Hit enter key. (Enter)
```

If you enter C in the **CER command** menu and press **Enter**, the following menu screen appears.

```
(S,C,[Q]) : C

-- SSL private key and certificate menu --
   S. Generate private key and self-signed certificate.
   C. Generate private key and certificate signing request(CSR).
   H. Show certificate Information.
   I. Import certificate file.
   P. Copy certificate file.
   B. Backup.
   R. Restore.
   Q. Quit.
(S,C,H,I,P,B,R,[Q]) :
```

Select a menu item from the table below to set the switch module firmware information.

Menu		Description
S.	Generate private key and self-signed certificate	Generates a pair of SSL keys and self-signed certificate.
C.	Generate private key and certificate signing request (CSR)	Generates a CSR to request the signed server certificate to a certificate authority.
H.	Show certificate Information	Shows SSL certificate information.
I.	Import certificate file.	Imports the signed server certificate.
P.	Copy certificate file.	Outputs the currently used server certificate to an area where FTP is available.

B.	Backup	Backs up the SSL key pairs and certificate.
R.	Restore	Restores the SSL key pairs and certificate.
Q.	Quit	Returns to the previous menu.

If you enter S in the **SSL private key and certificate** menu and press **Enter**, you can generate private key pairs and a self-signed certificate. When you enter required information, a message to confirm the key pairs and self-signed certificate is displayed. To generate the SSL key pairs and certificate, enter Y and press **Enter**. To cancel the process, enter N and press **Enter**, or just press **Enter**.

When you already have the encryption keys and server certificate, just overwrite them.

If communication is executed via the HTTPS server, regenerating key pairs disconnects the communication.

```
(S,C,H,I,P,B,R,[Q]) : S
Set key algorithm to RSA(1024bit)? (Y/[N]) : N
Select key algorithm
(0=RSA:1024bit,1=RSA:2048bit,2=DSA:1024bit,[Q=Quit]) : 1
Common Name ([localhost]) : p99.blade.com

Input other subject information of certificate? (Y,[N]) : Y
Country : JP
State or province : Kanagawa
Locality : Hadano
Organization : Hitachi Company Limited
Organizational unit : ESD
E-mail address : p99@mail.blade.com
DN qualifier : Qualifier-01
Surname : Hitachi
Given name : Taro
Initials : T.H

-- Self-signed certificate information --
Key algorithm       : RSA(2048bit)
Common name         : p99.blade.com
Country             : JP
State or Province   : Kanagawa
Locality            : Hadano
Organization        : Hitachi Company Ltd
Organizational unit : ESD
E-mail address      : p99@mail.blade.com
DN qualifier        : Qualifier-01
Surname             : Hitachi
Given name          : Taro
Initials            : T.H

Confirm? (Y,[N]) : Y
- Generating private key and self-signed certificate was completed.
Hit enter key.
```

You can enter values for each item as shown in the following table.

Required information for SSL server self-signed certificate			
Item	**Item in detail**	**Value**	**Value in detail**
Key algorithm	Key algorithm and bit-length	RSA (1024/ 2048 bit)	RSA: key bit-length is 1024 or 2048.
		DSA (1024 bit)	DSA: key bit-length is 1024.
Common name	Domain name when connected to svp	Character string	Up to 60 characters (*1) Default: localhost
Country	-	Character string	2 English capital letters (*2)
State or Province	-	Character string	Up to 60 characters (*2) (*3)
Locality	City, area	Character string	Up to 60 characters (*2) (*3)
Organization	Organization / Company name	Character string	Up to 60 characters (*2) (*3)
Organizational Unit	Department / Section name	Character string	Up to 60 characters (*2) (*3)
E-mail address	-	Character string	Up to 60 characters: printable character string in ASCII (*2)
DN qualifier	DN qualifier	Character string	Up to 60 characters (*2) (*3)
Surname	-	Character string	Up to 60 characters (*2) (*3)
Given name	-	Character string	Up to 60 characters (*2) (*3)
Initials	-	Character string	Up to 30 characters (*2) (*3)

(*1) Alphanumeric characters, hyphens (-), and periods (.) are available.

(*2) If nothing is entered, the item is not displayed by default.

(*3) Alphanumeric characters, space ( ), single quotation (‘), (“,”), plus (+), comma (,), hyphen (-), period (.), slash (/), colon (:), equal (=), and question mark (?) are available.

If you enter C in the **SSL private key and certificate** menu and press **Enter**, you can generate private key pairs and a CSR. When you enter required information, a file name, and the file type, a message to confirm the key pairs and CSR is displayed. To generate the SSL key pairs and CSR, enter Y and press **Enter**. To cancel the process, enter N and press **Enter**, or just press **Enter**.

When you already have the SSL key pairs and CSR, just overwrite them.

When you import the server certificate, consistency check with the key at the CSR generation is required. Thus, regenerating a CSR may prevent importing.

```
(S,C,H,I,P,B,R,[Q]) : C
Set key algorithm to RSA(1024bit)? (Y/[N]) : N
Select key algorithm
(0=RSA:1024bit,1=RSA:2048bit,2=DSA:1024bit,[Q=Quit]) : 1
Common Name ([localhost]) : p99.blade.com

Set other subject information of certificate? (Y,[N]) : Y
Country : JP
State or province : Kanagawa
Locality : Hadano
Organization : Hitachi Company Limited
Organizational unit : ESD
E-mail address : p99@mail.blade.com
DN qualifier : Qualifier-01
Surname : Hitachi
Given name : Taro
Initials : T.H
Unstructured name : Unofficial-01
Challenge password : password

Input CSR file name ([20090831-123456]) : XXXXXX
Set CSR file type to PEM? (Y/[N]) : N
Select CSR file type (0:PEM,1:DER,[Q=Quit]) : 0

-- Certificate signing request information --
Key algorithm       : RSA(2048bit)
Common name         : p99.blade.com
Country             : JP
State or Province   : Kanagawa
Locality            : Hadano
Organization        : Hitachi Company Ltd
Organizational unit : ESD
E-mail address      : p99@mail.blade.com
DN qualifier        : Qualifier-01
Surname             : Hitachi
Given name          : Taro
Initials            : T.H
Unstructured name   : Unofficial-01
Challenge password  : password

Confirm? (Y,[N]) : Y
- Generating certificate signing request was completed.
- CSR file name is csr-XXXXXX.csr.
Hit enter key.
```

You can enter values for each item as shown in the following table.

Required information for SSL server self-signed certificate			
Item	**Item in detail**	**Value**	**Value in detail**
Key algorithm	Key algorithm and bit-length	RSA (1024/ 2048bit)	RSA: key bit-length is 1024 or 2048.
		DSA (1024bit)	DSA: key bit-length is 1024.

Required information for SSL server self-signed certificate			
Item	**Item in detail**	**Value**	**Value in detail**
Common name	Domain name when connected to svp	Character string	Up to 60 characters (*1) Default: localhost
Country	-	Character string	2 English capital letters (*2)
State or Province	-	Character string	Up to 60 characters (*2) (*3)
Locality	City, area	Character string	Up to 60 characters (*2) (*3)
Organization	Organization / Company name	Character string	Up to 60 characters (*2) (*3)
Organizational Unit	Department / Section name	Character string	Up to 60 characters (*2) (*3)
E-mail address	-	Character string	Up to 60 characters (*2)
DN qualifier	DN modifier	Character string	Up to 60 characters (*2) (*3)
Surname	-	Character string	Up to 60 characters (*2) (*3)
Given name	-	Character string	Up to 60 characters (*2) (*3)
Initials	-	Character string	Up to 30 characters (*2) (*3)
Unstructured name	Unofficial name	Character string	Up to 60 characters (*2) (*3)
Challenge password	Password to delete a certificate	Character string	Up to 30 characters (*2) (*3)
File name	File name of a server certificate	Character string	Not available signs: slash (/), backslash (\), double quotation (“), single quotation (‘), colon (:), semicolon (;), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), and (|).
file type	Output file type	PEM	Base64 encoded text format from DER format.
		DER	Binary format Distinguished Encoding Rules (DER) encoded with X509 standard

(*1) Alphanumeric characters, hyphens (-), and periods (.) are available.

(*2) If nothing is entered, the item is not displayed by default.

(*3) Alphanumeric characters, space ( ), single quotation (‘), (“,”), plus (+), comma (,), hyphen (-), period (.), slash (/), colon (:), equal (=), and question mark (?) are available.

If you enter H in the **SSL private key and certificate** menu and press **Enter**, you can display the SSL certification information.

```
(S,C,H,I,P,B,R,[Q]) : H
-- SSL certificate information --
Version               : 3
Serial number         :
00:ff:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:66:77:88:99:00
Key algorithm         : RSA(2048bit)
Validity (Not Before) : 2009-05-08 12:34:56 UTC
Validity (Nor After)  : 2029-05-08 12:34:56 UTC
Issuer                : LocalCA
Common name           : p99.blade.com
Country               : JP
State or Province     : Kanagawa
Locality              : Hadano
Organization          : Hitachi Company Ltd
Organizational unit   : ESD
E-mail address        : p99@mail.blade.com
DN qualifier          :
Surname               :
Given name            :
Initials              :
Fingerprint (SHA1)    :
11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff:00:11:22:33:44

Hit enter key.
```

Items of the SSL certificate information are described in the table below.

Status of SSL server certificate			
Item	**Item in detail**	**Value**	**Value in detail**
Version	-	Numerical value	Value from 1 to 3 at RFC5280
Serial number	-	xx:xx: …:xx	Serial number in hexadecimal number
Key algorithm	Public key algorithm and key length	RSA (xxxx bit)	Public key algorithm: RSA Key length: xxxx bits
		DSA (xxxx bit)	Public key algorithm: DSA Key length: xxxx bits
Validity (Not Before)	Issued date and time of a certificate	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Validity (Not After)	Expiration date and time of a certificate	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second

Status of SSL server certificate			
Item	**Item in detail**	**Value**	**Value in detail**
Issuer	Certificate authority	Character string	A string contains up to 60 characters
		UTF-8 code is not displayed.	-
Country	-	Character string	2 English capital letters
State or Province	-	Character string	Up to 60 characters
Locality	City, area	Character string	Up to 60 characters
Organization	Organization/Company name	Character string	Up to 60 characters
Organizational Unit	Department/Section name	Character string	Up to 60 characters
E-mail address	-	Character string	Up to 60 characters
DN qualifier	-	Character string	Up to 60 characters
Surname	-	Character string	Up to 60 characters
Given name	-	Character string	Up to 60 characters
Initials	-	Character string	Up to 30 characters
Fingerprint (SHA1)	Certificate fingerprint	XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX	Fingerprint for a certificate: 20-byte hash value using SHA1 algorithm

If you enter [l] in the **SSL private key and certificate** menu and press **Enter**, you can import the SSL server certificate. To start importing the file, enter `Y` and press **Enter**. To cancel the process, enter `N` and press **Enter**, or just press **Enter**.

The currently used server certificate will be overwritten by the import.

If communication is executed via the HTTPS server, regenerating key pairs disconnects the communication.

When the management module and server certificate have different key pairs during SCR generation, importing is not available.

```
(S,C,H,I,P,B,R,[Q]) : I
-- file list --
<file0>
ssl-TEST.backup
<file1>
SignedCertificate.cer

Select backup file (0-1,[Q=Quit]) : 1
Select certificate file type (0:PEM,1:DER,[Q=Quit]) : 0

-- ssl certificate information –
[SSL certificate information is displayed.]

Confirm? (Y,[N]) : Y
- Importing certificate was completed.
Hit enter key.
```

If you enter P in the **SSL private key and certificate** menu and press **Enter**, you can copy the SSL server certificate to a download location. To start copying the file, enter Y and press **Enter**. To cancel the process, enter N and press **Enter**, or just press **Enter**.

```
(S,C,H,I,P,B,R,[Q]) : P
Input certificate file name ([20090831-123456]) : XXXXXX
Select certificate file type (0:PEM,1:DER,[Quit]) : 0

Confirm? (Y,[N]) : Y
- Copying certificate file was completed.
- Certficate file name is cer-XXXXXXX.cer.
Hit enter key.
```

If you enter B in the **SSL private key and certificate** menu and press **Enter**, you can back up the SSL private key pairs and certificate. You are prompted to enter the string for a file name used for the backup. When you enter the file name, a confirmation message appears. To start creating the backup, enter Y and press **Enter**. To cancel the process, enter N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : B (Enter)

Input backup file name ([Q=Quit]) : key_000000 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is ssl-key00000.backup.
Hit enter key. (Enter)
```

The SSL key pairs and certificate that you have backed up will be stored in a file in the user directory of the management module. Press **Enter**, and the screen returns to the **SSL private key and certificate** menu. You can take out the SSL key pairs and certificate files via FTP.

If you enter R in the **SSL private key and certificate** menu and press **Enter**, you can restore the SSL private key pairs and certificate. The list of files of the SSL key pairs and certificate is displayed. You are prompted to select a file for restoration. When you specify a file number, a confirmation message appears. To start the restoration, enter Y and press **Enter**. To cancel the process, enter N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : R (Enter)

-- Backup file list --
<File0>
ssl-test.backup
<File1>
ssl-key_000000.backup
Select backup file (0-1,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Restoring backup data was completed.
Hit enter key. (Enter)
```

❑ SEC command

You can set the network service. Enter SEC at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SEC (Enter)

<< SEC - Service setting. >>

-- Service setting menu --
   F. FTP setting.
   T. HTTP/HTTPS setting.
   S. SSH setting.
   E. Telnet setting.
   H. Connection allowed network setting for all of above protocols.
   A. Show all service setting.
   Q. Quit.
(F,T,S,E,H,A,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
F.	FTP setting.	Sets the FTP server.
T.	HTTP/HTTPS setting.	Sets the HTTP server.
S.	SSH setting.	Sets the SSH server.
E.	Telnet setting.	Sets the Telnet server.
H.	Connection allowed network setting for all of above protocols.	Sets the permitted network settings for all four protocols (FTP, HTTP, SSH, and Telnet).
A.	Show all service setting.	Displays the current values of all settings set by the SEC command.
Q.	Quit	Quits the SEC command.

If you enter `F` in the **SEC command** menu, and then press **Enter**, you can set the permissible network settings for connecting an FTP server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask. To save the permissible setting for the network, enter `Y` and press **Enter**. To cancel the setting, enter `N` and press **Enter**, or just press **Enter**.

```
(F,T,S,E,H,A,[Q])  : F (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N])  : N (Enter)
Network address : 192. 0. 0. 0
([Unchange]) : (Enter)
Subnetmask      : 255. 0. 0. 0
([Unchange]) : (Enter)

-- FTP setting --
Allow : Allow
Network address : 192. 0. 0. 0
Subnetmask      : 255. 0. 0. 0

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter `T` in the **SEC command** menu, and then press **Enter**, you can set the permissible network settings for connecting an HTTP/HTTPS server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask. Settings for HTTP include disabling HTTP/HTTPS, enabling HTTP, and enabling HTTPS. To save the permissible setting for the network, enter `Y` and press **Enter**. To cancel the setting, enter `N` and press **Enter**, or just press **Enter**.

```
(F,T,S,E,H,A,[Q]) : T (Enter)

HTTP : HTTP
(0=Disable,1=HTTP, 2=HTTPS,[Unchange]) : 1 (Enter)
Set port number to 80? (Y,[N]) : Y (Enter)
Allow all? (Y,[N]) : Y (Enter)

-- HTTP setting --
HTTP            : HTTP
Port number     : 80
Allow : Allow
Network address : ALL
Subnetmask      : -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter `S` in the **SEC command** menu, and then press **Enter**, you can set the permissible network settings for connecting an SSH server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask. To save the permissible setting for the network, enter `Y` and press **Enter**. To cancel the setting, enter `N` and press **Enter**, or just press **Enter**.

```
(F,T,S,E,H,A,[Q]) : S (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N])  : N (Enter)
Network address    : 0. 0. 0. 0
([Unchange]) : (Enter)

-- SSH setting --
Allow : Allow
Network address  : ALL
Subnetmask       : -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter E in the **SEC command** menu, and then press **Enter**, you can set the permissible network settings for connecting a Telnet server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask.

When you enter a setting, a confirmation message appears. To save the permissible setting for the network, enter Y and press **Enter**. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(F,T,S,E,H,A,[Q]) : E (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N])  : N (Enter)
Network address : 0. 0. 0. 0
([Unchange]) : (Enter)

-- Telnet setting --
Allow           : Allow
Network address : ALL
Subnetmask      : -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter H in the **SEC command** menu, and then press **Enter**, you can set the same permissible network settings for connecting to all four protocol servers (FTP, HTTP, SSH, and Telnet). You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask.

When you enter a setting, a confirmation message appears. To save the permissible setting for all protocols: FTP, HTTP, SSH, and Telnet, enter Y and press **Enter**. To cancel the setting, enter N and press **Enter**, or just press **Enter**.

```
(F,T,S,E,H,A,[Q]) : H (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N]) : N (Enter)
Input Network address : 0.0.0.0 (Enter)

-- Allowed network setting --
Allow           : Allow
Network address : ALL
Subnetmask      : -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was canceled.
Hit enter key. (Enter)
```

If you enter A in the **SEC command** menu, and then press **Enter**, you can display all the current setting values set by the SEC command.

```
(F,T,S,E,H,A,[Q]) : A (Enter)

-- FTP setting --
Allow : Allow
Network address : 192. 0. 0. 0
Subnetmask      : 255. 0. 0. 0

-- HTTP/HTTPS setting --
HTTP : HTTP
Port number     : 80
Allow           : Allow
Network address : ALL
Subnetmask      : -----

-- SSH setting --
Allow           : Allow
Network address : ALL
Subnetmask      : -----

-- Telnet setting --
Allow : Allow
Network address : ALL
Subnetmask      : -----

Hit enter key. (Enter)
```

❑ SO command

You can display and set account and role information. Enter SO at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SO (Enter)

<< SO - Security setting. >>

-- Security setting menu --
   A. Account setting.
   R. Role setting.
   Q. Quit.
(A,R,[Q]) :
```

Select a menu item from the table below to execute the function.

Menu		Description
A.	Account setting.	Sets accounts.
R.	Role setting.	Sets roles
Q.	Quit	Quits the SO command.

If you enter A in the **SO command** menu and press **Enter**, the current account setting information is displayed.

```
(A,R,[Q]) : A (Enter)

-- Account setting --
ID Name                              Status  Role
-- --------------------------------- ------- ---------------
 0 administrator                      Enable  Administrator
 1 -----                              -----   -----
 2 -----                              -----   -----
 3 -----                              -----   -----
 4 -----                              -----   -----
 5 -----                              -----   -----
 6 -----                              -----   -----
 7 -----                              -----   -----
 8 -----                              -----   -----
 9 -----                              -----   -----
10 -----                              -----   -----
11 -----                              -----   -----
12 -----                              -----   -----
13 -----                              -----   -----
14 -----                              -----   -----
15 -----                              -----   -----
16 -----                              -----   -----
17 -----                              -----   -----
18 -----                              -----   -----
19 -----                              -----   -----
20 -----                              -----   -----
21 -----                              -----   -----
22 -----                              -----   -----
23 -----                              -----   -----

-- Account menu --
   A. Add account.
   D. Delete account.
   E. Edit account detail information.
   Q. Quit.
(A,D,E,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
A.	Add account.	
R.	Delete account.	
E.	Edit account detail information	
Q.	Quit	Returns to the previous menu.

If you enter A in the **account menu** and press **Enter**, you are prompted to enter an account name, password, status, and role settings. When you have done so, the list of accounts is updated to include the account you intend to add, and a message appears prompting you to confirm the new account. To add the account, enter Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or simply press **Enter**.

If you enter D in the **account** menu and press **Enter**, you are prompted to enter an account number. When you have done so, the account settings are displayed without the account you intend to delete, and a message appears prompting you to confirm deletion of the account. To delete the account, enter Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or simply press **Enter**.

If you enter E in the **account** menu and press **Enter**, you are prompted to enter an account number. When you enter an account number, detailed information about the account is displayed, and the menu from which you can perform detailed account settings appears.

```
(A,D,E,[Q]) : E (Enter)

Select account (0-23,[Q=Quit]) : 1 (Enter)

-- Specified account setting --
ID                     : 1
Name                   : user0
Status                 : Enable
Role                   : Administrator
Key                    : Not installed
Console                : System console
Inactivity timer(min) : 10
Prompt : Chassis ID and Slot Number

-- Account detail setting menu --
    N. Edit account name.
    S. Edit account status.
    R. Edit account role.
    P. Edit account password.
    K. Edit account public key.
    C. Edit account console.
    I. Edit account inactivity timer.
    M. Edit account prompt.
    Q. Quit.
(N,S,R,P,K,C,I,M,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
N.	Edit account name.	
S.	Edit account status.	
R.	Edit account role.	
P.	Edit account password.	
K.	Edit account public key.	
C.	Edit account console.	Edit the console settings used for the account.
I.	Edit account inactivity timer.	Edit the inactivity timer settings for the account.
M.	Edit account prompt.	Edit the prompt setting for the account.
Q.	Quit	Returns to the previous menu.

If you enter `N` in the **account detail setting** menu and press **Enter**, you can change the account name. You cannot change the account name if a user is logged in to the account.

If you enter `S` in the **account detail setting** menu and press **Enter**, you can change the account status. You cannot change the account status if a user is logged in to the account.

If you enter `R` in the **account detail setting** menu and press **Enter**, you can change the role assigned to the account. You cannot change the role if a user is logged in to the account.

If you enter `P` in the **account detail setting** menu and press **Enter**, you can change the role assigned to the account. When changing the password of the currently logged-in account, you must enter the old and new passwords. When changing the password of an account for which you have editing permission other than the currently logged-in account, only the new password is required.

If you enter `K` in the **account detail setting** menu and press **Enter**, you can set public keys for the account password.

```
(N,S,R,P,K,C,I,M,[Q]) : K (Enter)

-- Public key status --
Key:                    Not installed.

-- Account public key menu --
    I. Install public key.
    U. Uninstall public key.
    Q. Quit.
(I,U,[Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
I.	Install public key.	
U.	Uninstall public key.	
Q.	Quit	Returns to the previous menu.

If you enter [I] and press **Enter**, you can install the public key for the account. The file list stored in the user directory is displayed. You are prompted to select a file from the list. When you specify the number of a file, the public key algorithm, key length, and fingerprint are displayed - the prompt is ready. To start installing the public key, enter `Y` and press **Enter**. To cancel the installation, enter `N` after the confirmation message and press **Enter**, or just press **Enter**.

```
(I,U,[Q]) : I (Enter)

-- File list --
<File0>
id_dsa.pub
<File1>
id_rsa.pub

Select file (0-1,[Q=Quit]) : 0 (Enter)
-- Public key information --
<Public key0>
Algorithm   : DSA
Key length  : 1024
Fingerprint : 1f:90:2d:5e:16:a5:72:90:d8:b0:93:54:48:2b:2f:4e

Confirm? (Y,[N]) : Y (Enter)
- Installing public key was completed.
Hit enter key. (Enter)
```



- Only OpenSSH public key file format is supported.
- Up to five public keys can be installed in one account.
- RSA and DSA are supported. A public key with SSH version 1 is not supported.
- Check the fingerprint of the public key and confirm that the fingerprint is identical to the fingerprint displayed before installation.
- Backup the public key beforehand by yourself.

If you enter `U` in the **account public key** menu and press **Enter**, you can uninstall the account public key. A confirmation message appears. To start uninstalling the public key, enter `Y` and press **Enter**. To cancel the installation, enter `N` after the confirmation message and press **Enter**, or just press **Enter**.

```
(I,U,[Q]) : U (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Uninstalling public key was completed.
Hit enter key. (Enter)
```

If you enter C in the **account detail setting** menu and press **Enter**, you can change the settings of the character-based console used for the account.

If you enter [l] in the **account detail setting** menu and press **Enter**, you can change the inactivity timer setting for the account. Specify a value from 0 to 1440 (minutes). To disable the inactivity timer, specify 0. The new setting takes effect the next time the user logs in to the account.

If you enter M in the **account detail setting** menu and press **Enter**, you can change the account prompt settings. You can select from two formats: "[chassis ID (management module slot number) SVP> (chassis ID and slot number)"; or "SVP> (fixed)".

If you enter R and press **Enter** at the prompt for the **SO command** menu, you can display the current role settings.

```
(A,R,[Q]) : R (Enter)

-- Role setting --

                            P        SW
No. Name            Status  01234567 012345 Net Chassis Account
--- --------------- ------- -------- ------ --- ------- -------
  0 Administrator   Enable  XXXXXXXX XXXXXX X   X       X
  1 -----            -----  -------- ------ -   -       -
  2 -----            -----  -------- ------ -   -       -
  3 -----            -----  -------- ------ -   -       -
  4 -----            -----  -------- ------ -   -       -
  5 -----            -----  -------- ------ -   -       -
  6 -----            -----  -------- ------ -   -       -
  7 -----            -----  -------- ------ -   -       -
  8 -----            -----  -------- ------ -   -       -
  9 -----            -----  -------- ------ -   -       -
 10 -----            -----  -------- ------ -   -       -
 11 -----            -----  -------- ------ -   -       -
 12 -----            -----  -------- ------ -   -       -
 13 -----            -----  -------- ------ -   -       -
 14 -----            -----  -------- ------ -   -       -
 15 -----            -----  -------- ------ -   -       -
 16 -----            -----  -------- ------ -   -       -
 17 -----            -----  -------- ------ -   -       -
 18 -----            -----  -------- ------ -   -       -
 19 -----            -----  -------- ------ -   -       -
 20 -----            -----  -------- ------ -   -       -
 21 -----            -----  -------- ------ -   -       -
 22 -----            -----  -------- ------ -   -       -
 23 -----            -----  -------- ------ -   -       -

-- Role menu --
   A. Add role.
   D. Delete role.
   E. Edit role.
   Q. Quit.
(A,D,E,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
A.	Add role.	
D.	Delete role.	
E.	Edit role.	
Q.	Quit	Returns to the previous menu.

If you enter `A` in the **role menu** and press **Enter**, the system awaits input of settings in the order shown in the table below. To proceed to the next setting, press **Enter**, or enter a value and then press **Enter**. Before you set individual partition and switch module permissions, you are prompted to select the option of granting permission to all partitions and all switch modules. If you choose to grant permission to all partitions, you do not need to set permissions for individual partitions. Likewise, you do not need to set permissions for individual switch modules if you grant permission to all switch modules.

Order	Item
1	Role name
2	Partition 0 permission
3	Partition 1 permission
4	Partition 2 permission
5	Partition 3 permission
6	Partition 4 permission
7	Partition 5 permission
8	Partition 6 permission
9	Partition 7 permission
10	Switch module 0 permission
11	Switch module 1 permission
12	Switch module 2 permission
13	Switch module 3 permission
14	Switch module 4 permission
15	Switch module 5 permission
16	Network permission
17	Server chassis permission
18	Account permission

When you set new account permission, the list of role settings is updated to reflect the change, and a confirmation message appears. To apply the new settings, enter `Y` and then press **Enter**. To cancel the operation, enter `N` and then press **Enter**, or just press **Enter**.

```
(A,D,E,[Q]) : A (Enter)
Enter role name ([Quit]) : admin (Enter)
Select all partition? (Y,[N]) : Y (Enter)
Select all switch module? (Y,[N]) : Y (Enter)
Add network authority? (Y,[N]) : Y (Enter)
Add server chassis authority? (Y,[N]) : Y (Enter)
Add account authority? (Y,[N]) : Y (Enter)

-- Role setting --

P SW
No. Name            Status  01234567 012345 Net Chassis Account
--- --------------- ------- -------- ------ --- ------- -------
  0 Administrator   Enable  XXXXXXXX XXXXXX X   X       X
  1 admin           Enable  XXXXXXXX XXXXXX X   X       X
  2 -----            -----  -------- ------ -   -       -
  3 -----            -----  -------- ------ -   -       -
  4 -----            -----  -------- ------ -   -       -
  5 -----            -----  -------- ------ -   -       -
  6 -----            -----  -------- ------ -   -       -
  7 -----            -----  -------- ------ -   -       -
  8 -----            -----  -------- ------ -   -       -
  9 -----            -----  -------- ------ -   -       -
 10 -----            -----  -------- ------ -   -       -
 11 -----            -----  -------- ------ -   -       -
 12 -----            -----  -------- ------ -   -       -
 13 -----            -----  -------- ------ -   -       -
 14 -----            -----  -------- ------ -   -       -
 15 -----            -----  -------- ------ -   -       -
 16 -----            -----  -------- ------ -   -       -
 17 -----            -----  -------- ------ -   -       -
 18 -----            -----  -------- ------ -   -       -
 19 -----            -----  -------- ------ -   -       -
 20 -----            -----  -------- ------ -   -       -
 21 -----            -----  -------- ------ -   -       -
 22 -----            -----  -------- ------ -   -       -
 23 -----            -----  -------- ------ -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter D in the **role** menu and press **Enter**, you are prompted to enter the number of the role that you want to delete. When you have done so, the list of role settings is updated, and a message appears prompting you to confirm the deletion. To delete the role, enter Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or just press **Enter**.

```
(A,D,E,[Q]) : D (Enter)
(0-23,[Q=Quit]) : 1 (Enter)

-- Role setting --
                              P        SW
No. Name             Status   01234567 012345 Net Chassis Account
--- ---------------- -------- -------- ------ --- ------- -------
  0 Administrator    Enable   XXXXXXXX XXXXXX X   X       X
  1 -----             -----   -------- ------ -   -       -
  2-----              -----   -------- ------ -   -       -
  3 -----             -----   -------- ------ -   -       -
  4 -----             -----   -------- ------ -   -       -
  5 -----             -----   -------- ------ -   -       -
  6 -----             -----   -------- ------ -   -       -
  7 -----             -----   -------- ------ -   -       -
  8 -----             -----   -------- ------ -   -       -
  9 -----             -----   -------- ------ -   -       -
 10 -----             -----   -------- ------ -   -       -
 11 -----             -----   -------- ------ -   -       -
 12 -----             -----   -------- ------ -   -       -
 13 -----             -----   -------- ------ -   -       -
 14 -----             -----   -------- ------ -   -       -
 15 -----             -----   -------- ------ -   -       -
 16 -----             -----   -------- ------ -   -       -
 17 -----             -----   -------- ------ -   -       -
 18 -----             -----   -------- ------ -   -       -
 19 -----             -----   -------- ------ -   -       -
 20 -----             -----   -------- ------ -   -       -
 21 -----             -----   -------- ------ -   -       -
 22 -----             -----   -------- ------ -   -       -
 23 -----             -----   -------- ------ -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you enter E in the **role** menu and press **Enter**, you are prompted to enter the number of the role that you want to edit. After entering the role number, the current settings are displayed in the order shown in the table below, and the system awaits your input. To proceed to the next setting, press **Enter**, or enter a value and then press **Enter**.

Order	Item
1	Role name
2	Partition 0 permission
3	Partition 1 permission
4	Partition 2 permission
5	Partition 3 permission
6	Partition 4 permission
7	Partition 5 permission
8	Partition 6 permission
9	Partition 7 permission
10	Switch module 0 permission
11	Switch module 1 permission
12	Switch module 2 permission
13	Switch module 3 permission
14	Switch module 4 permission
15	Switch module 5 permission
16	Network permission
17	Server chassis permission
18	Account permission

If you enter the account permission settings, the role settings are updated to reflect the changes, and a confirmation message appears. To apply the changes, enter Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or simply press **Enter**.

```
(A,D,E,[Q]) : E (Enter)
(0-23,[Q=Quit]) : 0 (Enter)
Role name : Administrator
([Unchange]) : (Enter)
Partition0 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition1 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition2 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition3 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition4 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition5 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition6 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Partition7 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module0 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module1 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module2 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module3 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module4 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Switch module5 : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Network authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Server chassis authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Account authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)

-- Role setting --
                            P        SW
No. Name             Status  01234567 012345 Net Chassis Account
--- ---------------- ------- -------- ------ --- ------- -------
  0 Administrator    Enable  XXXXXXXX XXXXXX X   X       X
  1 -----             -----  -------- ------ -   -       -
  2 -----             -----  -------- ------ -   -       -
  3 -----             -----  -------- ------ -   -       -
  4 -----             -----  -------- ------ -   -       -
  5 -----             -----  -------- ------ -   -       -
  6 -----             -----  -------- ------ -   -       -
  7 -----             -----  -------- ------ -   -       -
  8 -----             -----  -------- ------ -   -       -
  9 -----             -----  -------- ------ -   -       -
 10 -----             -----  -------- ------ -   -       -
 11 -----             -----  -------- ------ -   -       -
 12 -----             -----  -------- ------ -   -       -
 13 -----             -----  -------- ------ -   -       -
 14 -----             -----  -------- ------ -   -       -
 15 -----             ---- - -------- ------ -   -       -
 16 -----             -----  -------- ------ -   -       -
 17 -----             -----  -------- ------ -   -       -
 18 -----             -----  -------- ------ -   -       -
 19 -----             -----  -------- ------ -   -       -
 20 -----             -----  -------- ------ -   -       -
 21 -----             -----  -------- ------ -   -       -
 22 -----             -----  -------- ------ -   -       -
 23 -----             -----  -------- ------ -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

❑ SC Command

You can set a security strength level and enable/disable a Transport Layer Security (TLS) version. Enter `SC` in the prompt and press **Enter**.

```
<< SC - Security configuration. >>
-- Security strength of management module --
Security strength : High

-- Security strength of partition --
P Security strength BMC status
- ----------------- --------------
0 High              High
1 High              High
2 High              High
3 High              High
4 Default           Default
5 Default           Default
6 Default           Default
7 Default           Default

-- TLS version of management module --
TLS 1.2  : Enable
TLS 1.1  : Enable
TLS 1.0  : Enable
SSL 3.0  : Enable

-- Security strength setting menu --
    C. Edit security strength of chassis.
    M. Edit security strength of management module.
    P. Edit security strength of partition.
    T. Edit TLS version of management module.
    Q. Quit.
(C,M,P,T,[Q]) :
```

Security strength of management module shows the following item.

Menu	Description
Security strength	Security strength levels of management modules High Default

Security strength of partition shows the following items.

Menu	Description
P	Partition number
Security strength	Partition status for security strength High Default -----: Disabled partition
BMC status	BMC status for security strength: whether or not the partition's level has been applied to. High: Matched with the partition's High. Default: Matched with the partition's Default. Unmatch: With Symmetric Multiprocessing (SMP) configuration, the partition includes server blades with High and Default. Not installed: No server blade installed. Not supported: Security strength is not supported by BMC. Initializing: Partition is being initialized. FAIL: Partition initialization has aborted. -----: Disabled partition

TLS version of management module shows the following items.

Menu	Description
TLS 1.2	Enables or disables TLS version 1.2: Enable/Disable
TLS 1.1	Enables or disables TLS version 1.1: Enable/Disable
TLS 1.0	Enables or disables TLS version 1.0: Enable/Disable
SSL 3.0	Enables or disables SSL version 3.0: Enable/Disable

Select a menu you require from the following list, and execute it.

Menu		Description
C.	Edit security strength of chassis.	Edits security strength of the overall chassis.
M.	Edit security strength of management module.	Edits security strength of the management module.
P.	Edit security strength of partition.	Edit security strength of the partition.
T.	Edit TLS version of management module.	Enables/disables Transport Layer Security (TLS)/ Secure Socket Layer (SSL) versions of the management module.
Q.	Quit	Quits the SC command.

If you enter C in the **SC command** menu and press **Enter**, the current settings for security strength of management modules and all partitions are displayed. At the prompt, enter the security strength levels. The new setting values are displayed. Warning messages, showing the management module restart and BMC restart against the partition with the setting to be changed, display. A confirmation message displays, prompting you to confirm the new setting. To add the setting, enter Y and then press **Enter**. The management module will restart to disconnect the active console. To cancel the operation, enter N and then press **Enter**, or just press **Enter**.

```
-- Security strength of management module --
Security strength : High

-- Security strength of partition --
P Security strength
- -----------------
0 High
1 High
2 High
3 High
4 Default
5 Default
6 Default
7 Default

Security strength (0=Default,1=High,[Q=Quit]) : 1

-- Security strength of management module --
Security strength : High

-- Security strength of partition --
P Security strength
- -----------------
0 High
1 High
2 High
3 High
4 High
5 High
6 High
7 High

WARNING : If confirm, management module restart and this connect is lost.
WARNING : <Partition4> BMC restart automatically.
WARNING : <Partition5> BMC restart automatically.
WARNING : <Partition6> BMC restart automatically.
WARNING : <Partition7> BMC restart automatically.
Confirm? (Y,[N]) : Y
```



If a partition is powered on or has not been initialized, you cannot set the security strength. For a server blade with N+M cold standby enabled, make sure to execute Smart configure after the management module has restarted.

If you enter M in the **SC command** menu and press **Enter**, the current settings for security strength of management modules are displayed. At the prompt, enter a security strength level. The new setting value is displayed. A warning message showing the management module restart appears. A confirmation message displays, prompting you to confirm the new setting. To add the setting, enter Y and then press **Enter**. The management module will restart to disconnect the active console. To cancel the operation, enter N and then press **Enter**, or just press **Enter**.

```
-- Security strength of management module --
Security strength : High
Security strength (0=Default,1=High,[Q=Quit]) : 0

-- Security strength of management module --
Security strength : Default

WARNING : If confirm, management module restart and this connect is lost.
Confirm? (Y,[N]) : Y
```



If a partition is powerd on or has not been initializated, you cannot set the security strength. For a server blade with N+M cold standby enabled, make sure to execute Smart configure after the management module has restarted.

If you enter P at the **SC command** menu and press **Enter**, the current settings for security strength of all partitions are displayed. At the prompt, enter a partition number and security strength level. The new setting values are displayed. A warning message showing BMC restart displays if the partition setting is changed. A confirmation message displays, prompting you to confirm the new setting. To add the setting, enter Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or simply press **Enter**.

```
-- Security strength of partition --
P Security strength
- -----------------
0 High
1 High
2 High
3 High
4 High
5 High
6 High
7 High

Select partition (0-7,A=All,[Q=Quit]) : 0
Security strength (0=Default,1=High,[Q=Quit]) : 0
```

```
-- Security strength of partition --
P Security strength
- ------------------
0 Default
1 High
2 High
3 High
4 High
5 High
6 High
7 High

WARNING : <Partition0> BMC restart automatically.
Confirm? (Y,[N]) : Y
- <PartitionX> Writing setting was completed.
Hit enter key.
```



You cannot set security strength to a powered-on partition or not-completely-initialized one.

If you enter `T` at the **SC command** menu and press **Enter**, the current settings display for TSL versions, TLS 1.2, TLS 1.1, TLS 1.0, and SSL 3.0. At the prompt, enter **Enable** or **Disable**. The new setting values are displayed. A confirmation message displays, prompting you to confirm the new settings. To add the setting, enter `Y` and then press **Enter**. To cancel the operation, enter `N` and then press **Enter**, or simply press **Enter**.

```
TLS 1.2   : Enable
(0=Disable,1=Enable,[Unchange]) : 0
TLS 1.1   : Enable
(0=Disable,1=Enable,[Unchange]) :
TLS 1.0   : Enable
(0=Disable,1=Enable,[Unchange]) :
SSL 3.0   : Enable
(0=Disable,1=Enable,[Unchange]) :

-- TLS version of management module --
TLS 1.2   : Disable
TLS 1.1   : Enable
TLS 1.0   : Enable
SSL 3.0   : Enable

Confirm? (Y,[N]) : Y
- Writing setting was completed.
Hit enter key.
```



You cannot disable all TLS/SSL versions. When security strength of the management module is high, you neither enable nor disable TLS/SSL versions. Only TLS 1.2 can be used.

Managing switch modules

❑ SWC command

Performs tasks related to switch modules. Enter `SWC` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)SVP> SWC(Enter)

<< SWC - Switch module control. >>

-- Switch module status --
SW Type              Power Condition     LID lamp
-- ----------------- ----- ------------- --------
0  1G LANSW          On    Normal        Off
1  1G LANSW          On    Normal        Off
2  1/10G LANSW       On    Normal        Off
3  1/10G LANSW       On    Normal        Off
4  1/10G LANSW       On    Normal        Off
5  1/10G LANSW       On    Normal        Off

-- Switch module control menu --
   P. Power control.
   L. LID lamp control.
   Q. Quit.
(P,L,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
P.	Power control.	Control the power supply to the switch modules.
L.	LID lamp control.	Control the LID LEDs of the switch modules.
Q.	Quit	Quits the SWC command.

Items displayed on the screen are described in the table below.

Item	Description
SW	Slot number of the switch module
Type	Type of the switch module 1G LANSW: 1Gbps LAN switch module 1/10G LANSW: 1/10Gbps LAN switch module 8G FCSW: 8 Gbps FC switch module 1G LANPT: 1 Gb LAN pass through module 10G LANPT: 10 Gb LAN pass through module 10G DCBSW: Brocade10 Gb DCB switch module
Power	Power status: On: the power is on; Off: the power is off.
Condition	Status NORMAL: Working normally; Booting: Just booting or during CONFIG; ERROR: configured incorrectly; WARNING: Exceeds the warning threshold value of the sensor FAIL: Exceeds the failure threshold value of the sensor.

	FATAL: Error status
LID lamp	LED status: On: the LID lights solid; Off: The LID does not light.

If you enter `P` at the **SWC command** menu and press **Enter**, the status of the switch modules is displayed.

```
(P,L,[Q]) : P (Enter)
-- Switch module status --
SW Type              Power Condition     LID lamp
-- ---------------- ----- ------------- --------
0  1G LANSW          On    Normal        Off
1  1G LANSW          On    Normal        Off
2  1/10G LANSW       On    Normal        Off
3  1/10G LANSW       On    Normal        Off
4  1/10G LANSW       On    Normal        Off
5  1/10G LANSW       On    Normal        Off

-- Power control menu --
   P. Power on.
   F. Power off.
   Q. Quit.
(P,F,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
P.	Power-on	Turns on power to the switch module.
F.	Power-off.	Turns off power to the switch module.
Q.	Quit	Returns to the previous menu.

When you enter `P` at the **switch module power control** menu and press **Enter**, you are prompted to select a switch module.

```
(P,F,[Q]) : P (Enter)
Select switch module (0-5,[A=All]) : A (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Switch module0> Power on was completed.
- <Switch module1> Power on was completed.
- <Switch module2> Power on was completed.
- <Switch module3> Power on was completed.
- <Switch module4> Power on was completed.
- <Switch module5> Power on was completed.
Hit enter key. (Enter)
```

When you enter F at the **switch module power control** menu and press **Enter**, you are prompted to select a switch module.

```
(P,F,[Q]) : F (Enter)
Select switch module (0-5,[A=All]) : A (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Switch module0> Power off was completed.
- <Switch module1> Power off was completed.
- <Switch module2> Power off was completed.
- <Switch module3> Power off was completed.
- <Switch module4> Power off was completed.
- <Switch module5> Power off was completed.
Hit enter key. (Enter)
```

If you enter L at the **SWC command menu** and press **Enter**, the status of the switch modules is displayed.

```
(P,L,[Q]) : L (Enter)
-- Switch module status --
SW Type              Power Condition     LID lamp
-- ----------------- ----- ------------- --------
0  1G LANSW          On    Normal        Off
1  1G LANSW          On    Normal        Off
2  1/10G LANSW       On    Normal        Off
3  1/10G LANSW       On    Normal        Off
4  1/10G LANSW       On    Normal        Off
5  1/10G LANSW       On    Normal        Off

-- LID lamp control menu --
    T. Turn on
    F. Turn off
    Q. Quit.
(T,F,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
T.	Turn on.	Turns on the switch module LID.
F.	Turn off.	Turns off the switch module LID.
Q.	Quit	Returns to the previous menu.

If you enter `T` at the **ID LED control** menu and press **Enter**, you are prompted to select a switch module.

```
(T,F,[Q]) : T (Enter)

Select switch module (0-5,[A=All]) : A (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Switch module0> Turn on LID lamp was completed.
- <Switch module1> Turn on LID lamp was completed.
- <Switch module2> Turn on LID lamp was completed.
- <Switch module3> Turn on LID lamp was completed.
- <Switch module4> Turn on LID lamp was completed.
- <Switch module5> Turn on LID lamp was completed.
Hit enter key. (Enter)
```

If you enter `F` at the **ID LED control** menu and press **Enter**, you are prompted to select a switch module.

```
(T,F,[Q]) : F (Enter)

Select switch module (0-5,[A=All]) : A (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Switch module0> Turn off LID lamp was completed.
- <Switch module1> Turn off LID lamp was completed.
- <Switch module2> Turn off LID lamp was completed.
- <Switch module3> Turn off LID lamp was completed.
- <Switch module4> Turn off LID lamp was completed.
- <Switch module5> Turn off LID lamp was completed.
Hit enter key. (Enter)
```

Backing up and restoring settings

❑ DC command

Restores settings to factory defaults. For server blades, only information that is set on the following screens of the server blade Web console is initialized.

Language setting

Configuration of network

User account settings

Enter DC at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> DC(Enter)

<< DC - Restore factory setting. >>

-- Restore setting menu --
   R. Restore factory setting.
   B. Reset server blade web console setting.
   H. Reset LP setting.
   Q. Quit.
(R,B,H,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
R.	Restore factory setting.	Restores the settings of the management module to the factory defaults.
B.	Reset server blade web console setting.	Resets the settings for the server blade web console. Information set on the following screens is reset. - Language setting - Configuration of network - User account settings
H.	Reset LP setting.	Reset the LPAR manager configuration information to the factory settings.
Q.	Quit	Quits the DC command.

If you enter R at the **DC command** menu and press **Enter**, a warning message appears indicating that if you proceed, the current session will be terminated and the management module will restart with the factory defaults. To restore the management module to the defaults and restart, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, at the confirmation prompt, enter N and then press **Enter**, or simply press **Enter**.

```
(R,B,H,[Q]) : R (Enter)

WARNING : If confirm, this connect is lost.

Confirm? (Y,[N]) : Y (Enter)
- <Management module0> Restarting
```

If you enter B at the **DC command** menu and press **Enter**, you are prompted to select a partition. After you enter a partition number and press **Enter**, a confirmation message appears. To reset the server blade web console to the defaults, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(R,B,H,[Q]) : B (Enter)

Select partition (0-7,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Resetting server blade web console setting was completed.
Hit enter key. (Enter)
```

If you enter H at the **DC command** menu and press **Enter**, you are prompted to select a partition. After you enter a partition number and press **Enter**, a confirmation message appears. To reset the LPAR manager configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(R,B,H,[Q]) : H (Enter)

Select partition (0-7,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Resetting LP setting was completed.
Hit enter key. (Enter)
```



Do not perform H. Reset LP setting of this command to a partition on which LPAR migration has been performed. See Chapter 12: Logical partitioning manager for further information.

❑ UBR command

Backs up, restores, or deletes a range of configuration information. Enter `UBR` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)SVP> UBR(Enter)

<< UBR - Backup and restore setting. >>

-- Backup and restore setting menu --
   M. Management module.
   B. BMC.
   E. EFI.
   F. FRU of Server blade.
   V. LP.
   H. Fibre Channel HBA.
   D. Delete backup data of server blade.
   Q. Quit.
(M,B,E,F,V,H,D,[Q]) :
```

Select a menu from the following list to execute the function.

Menu		Description
M.	Management module.	Back up and restore the management module configuration information.
B.	BMC	Restore the BMC configuration information.
E.	EFI	Restore the EFI configuration information.
F.	FRU of Server blade	Restore the FRU data of the server blade.
V.	LP.	Back up and restore the LPAR manager configuration information.
H.	Fibre-channel HBA.	Back up the Fibre-channel card settings. HBA: host bus adapter
D.	Delete backup data of server blade.	The operations in this sub-menu are unavailable.
Q.	Quit	Quits the UBR command.

If you enter `M` at the **UBR command** menu and press **Enter**, the menu for backing up and restoring the management module configuration information is displayed.

```
(M,B,E,F,V,H,D,[Q]) : M(Enter)

-- Management module menu --
B. Backup.
R. Restore.
Q. Quit.
(B,R,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
B.	Backup	Saves management module configuration information.
R.	Restore.	Restores management module configuration information.
Q.	Quit	Returns to the previous menu.

If you enter B at the **UBR command** menu and press **Enter**, you are prompted to enter characters used for the file name. To save the configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,R,[Q]) : B (Enter)

Input backup file name ([Q=Quit]) : conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is svp-conf.backup.
Hit enter key. (Enter)
```

When the file finished saving the configuration information, the file name is displayed. Press **Enter** and the screen returns to the **management module configuration** menu. That file is stored in the user directory in the management module. You can take out the file via FTP or SFTP. The account name and password for connection via FTP or SFTP are the same as when you log in to the system console.

If you enter R at the **UBR command** menu and press **Enter**, the list of files containing the management module configuration is stored in the user directory. You are prompted to select a file to be restored. When you enter the number to specify a file, a warning message indicating that the management module restarts after restoring the configuration is displayed. A confirmation message appears. To restore the configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,R,[Q]) : R (Enter)

-- Backup file list --
<File0>
svp-conf.backup

Select backup file (0,[Q=Quit]) : 0 (Enter)
WARNING : If confirm, this connect is lost.

Confirm? (Y,[N]) : Y (Enter)
- <Management module0> Restarting
```

Do not restore the management module backup file while the server blade is in operation. Proper operation may not be available due to the inconsistency between the restored configuration and the configuration when the server blade operates.

When restoring the backup file while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

If you enter B at the **UBR command** menu and press **Enter**, the menu for restoring BMC configuration information is displayed.

```
(M,B,E,F,V,H,D,[Q]) : B(Enter)

-- BMC menu --
  R. Restore.
  Q. Quit.
(R,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
R.	Restore.	Restores BMC configuration information.
Q.	Quit	Returns to the previous menu.

If you enter R at the **BMC configuration** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, the history list for storing BMC configuration information appears, and you are prompted to select a datum to be restored. When you enter the number to specify the history, a confirmation message appears. To restore the configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(R,[Q]) : R (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)

-- Backup file list --
No. Time
--- -------------------
  0 2009-03-10 15:58:30
  1 2009-03-11 19:49:39
  2 2009-03-13 15:21:04
  3 2009-03-13 17:03:26
  4 2009-03-13 17:41:15

Select backup data (0-4,[Q=Quit]) : 0 (Enter)
Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Restoring backup data was completed.
Hit enter key. (Enter)
```

If you enter E at the **UBR command** menu and press **Enter**, the menu for restoring EFI configuration information is displayed.

```
(M,B,E,F,V,H,D,[Q])   : E(Enter)

-- EFI menu --
  R. Restore.
  Q. Quit.
(R,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
R.	Restore.	Restores EFI configuration information.
Q.	Quit	Returns to the previous menu.

If you enter R at the **EFI configuration** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, the history list for storing EFI configuration information appears and you are prompted to select a datum to be restored. When you enter the number to specify the history, a confirmation message appears. To restore the configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(R,[Q]) : R (Enter)
Select partition (0-7,[Q=Quit])   : 0 (Enter)

-- Backup file list --
No. Time
--- -------------------
  0 2009-03-10 15:58:30
  1 2009-03-11 19:49:39
  2 2009-03-13 15:21:04
  3 2009-03-13 17:03:26
  4 2009-03-13 17:41:15

Select backup data (0-4,[Q=Quit]) : 0 (Enter)
Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Restoring backup data was completed.
Hit enter key. (Enter)
```

If you enter F at the **UBR command** menu and press **Enter**, the menu for restoring the FRU data of the server blade is displayed.

```
(M,B,E,F,V,H,D,[Q])   : F(Enter)

-- FRU of server blade menu --
   R. Restore.
   Q. Quit.
(R,[Q]) :
```

Select a menu item from the following list to execute the function.

Menu		Description
R.	Restore.	Restores FRU data of the server blade.
Q.	Quit	Returns to the previous menu.

If you enter R at the **FRU of the server blade** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, you are prompted to select a server blade. When you enter the server blade number, the list of history to save the FRU information of the server blade appears. You are prompted to select a datum to be restored. When you enter a number to specify the history, a confirmation message appears. To restore the configuration, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(R,[Q]) : R (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)
Select server blade (0,[Q=Quit]): 0 (Enter)

-- Backup file list --
No. Time
--- -------------------
  0 2009-03-10 15:58:30
  1 2009-03-11 19:49:39
  2 2009-03-13 15:21:04
  3 2009-03-13 17:03:26
  4 2009-03-13 17:41:15

Select backup data (0-4,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Restoring backup data was completed.
Hit enter key. (Enter)
```

If you enter V at the **UBR command** menu and press **Enter**, the menu for backing up and restoring LPAR manager configuration information is displayed.

```
(M,B,E,F,V,H,D,[Q]) : V(Enter)

-- LP menu --
  B. Backup.
  R. Restore.
  Q. Quit.
(B,R,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
B.	Backup.	Backs up LPAR manager configuration information.
R.	Restore.	Restores LPAR manager configuration information.
Q.	Quit	Returns to the previous menu.

If you enter B at the **LP** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, you are prompted to enter a file name. When you enter the file name, a confirmation message appears. To create the file storing the configuration information, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,R,[Q]) : B (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)
Input backup file name ([Q=Quit]) : conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Creating backup file was completed.
- Backup file name is hvm-conf.backup.
Hit enter key. (Enter)
```

When the file finishes storing the configuration information, the file name is displayed and the prompt is ready. Press **Enter**, and the screen returns to the **management module configuration** menu. That file is stored in the user directory in the management module. You can take out the file via FTP or SFTP. The account name and password for connection via FTP or SFTP are the same as when you log in to the system console.

If you enter R at the **LP** menu and press **Enter**, the LP manager restore menu is displayed.

```
(B,R,[Q]) : R (Enter)

-- LP restore menu --
   B. Restore backup file to local backup data.
   L. Restore local backup data.
   Q. Quit.
(B,L,[Q]) :
```

Select a menu item from the following table to execute the function.

Menu		Description
B.	Restore backup file to local backup.	Restores the LPAR manager configuration stored in the user directory and saves it in the LPAR manager data management area.
L.	Restore local backup data.	Sets the configuration data stored in the LPAR manager data management area of the management module and will be restored at the next LPAR manager boot.
Q.	Quit	Returns to the previous menu.

If you enter B at the **LP restore** menu and press **Enter**, the list of LPAR manager configuration data files is displayed. You are prompted to select a file to restore. When you enter the number to specify the file, you are prompted to select a partition. When you enter the partition number and press **Enter**, a confirmation message appears. To restore the configuration in the LPAR manager configuration data management area, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,L,[Q]) : B (Enter)

-- Backup file list --
<File0>
hvm-bbbb.backup

Select backup file (0,[Q=Quit]) : 0 (Enter)
Select partition (0-7,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Restoring backup data was completed.
Hit enter key. (Enter)
```

If you enter L at the **LP restore** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, a confirmation message appears. To restore the configuration at the next LPAR manager boot, enter Y at the confirmation prompt and press **Enter**. To cancel the operation, enter N at the confirmation prompt and press **Enter**, or simply press **Enter**.



```
(B,L,[Q]) : L (Enter)

Select partition (0-7,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Restoring backup data was completed.
Hit enter key. (Enter)
```

When restoring the configuration before LPAR migration to the migrated partition with the restoring function of this command, restore the configuration before migration to both the source and destination. See Chapter 12: Logical partitioning manager for further information.

If you enter H at the **UBR command** menu and press **Enter**, the Fibre-channel HBA menu is displayed.

```
(M,B,E,F,V,H,D,[Q]) : H(Enter)

-- Fibre Channel HBA menu --
  B. Backup.
  F. Backup.(Hitachi 16Gb Fibre Channel Card)

  Q. Quit.
(B,F, [Q]) :
```

Select a menu you require from the following list, and execute it.

Menu		Description
B.	Backup.	Backs up settings for Hitachi 4 Gb or 8 Gb Fibre-channel card settings.
F	Backup.(Hitachi 16Gb Fibre Channel Card)	Backs up settings for Hitachi 16 Gb Fibre-channel card
Q.	Quit	Returns to the previous menu.

Entering B allows you to back up settings for Hitachi 4 Gb or 8 Gb fibre channel card. If you enter B at the **Fibre-channel card setting** menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, you are prompted to select a server blade. When you enter the server blade slot number and press **Enter**, you are prompted to select an expansion card or I/O adapter. If you select an expansion card, you are prompted to enter the expansion card slot number. If you select an I/O adapter, you are prompted to enter the I/O adapter slot number. If you select an I/O adapter on an I/O slot expansion unit, you are prompted to enter the slot number of the connection board to the I/O slot expansion unit and the I/O adapter slot number on the I/O slot expansion unit.

When you enter the slot number, the list of history data for the Fibre-channel card configuration, you are prompted to select a datum. When you enter the number to specify the datum, you are prompted to enter the string for a file name used for the backup of the Fibre-channel card configuration.

Enter the string for a file name, and a confirmation message appears. To create the file saving the Fibre-channel card configuration, enter `Y` at the confirmation prompt and press **Enter**. To cancel the operation, enter `N` at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,[Q]) : B

Select partition (0-7,[Q=Quit]) : 0
Select server blade (0,[Q=Quit]) : 0
Select card (0=Mezzanine card,1=I/O adapter,2=I/O adapter for expansion
unit,[Q=Quit]) : 0
Select mezzanine card (0-1,[Q=Quit]) : 0

-- Backup file list --
No. Time
--- -------------------
  0 2009-03-09 21:10:46
  1 2009-03-10 08:45:46
  2 2009-03-10 10:41:15

Select backup data (0-2,[Q=Quit]) : 0 (Enter)
Input backup file name ([Q=Quit]) : conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Creating backup file was completed.
- Backup file name is hba-conf.backup.
Hit enter key. (Enter)
```

When the file containing the Fibre-channel card configuration has been completed, the file name is displayed. Press **Enter** and the screen returns to the **Fibre-channel HBA** menu.

You can take out the file via FTP or SFTP. The account name and password for connection via FTP or SFTP are the same as when you log in to the system console.

Entering `F` allows you to back up settings for the Hitachi 16 Gb fibre channel card. If you enter `F` at the fibre channel card setting menu and press **Enter**, you are prompted to select a partition. When you enter the partition number and press **Enter**, you are prompted to select a server blade. When you enter the server blade slot number and press **Enter**, you are prompted to select one of the adapters, I/O adapter, or the one on the I/O slot expansion unit. If you select the I/O adapter, you are prompted to enter the I/O adapter slot number. If you select the I/O adapter on the I/O slot expansion unit, you are prompted to enter the slot number of the connection board to the I/O slot expansion unit and the I/O adapter slot number on the I/O slot expansion unit: prompt is ready.

When you enter the slot number, the list of history data for the fibre channel card configuration, you are prompted to select a datum to take out. When you enter the number to specify the datum, you are promoted to enter the string for a file name used for the backup of the fibre channel card configuration.

Enter the string for a file name, a message to confirm the backup: the prompt is ready. To create the file saving the fibre channel card configuration, enter `Y` at the confirmation prompt and press **Enter**. To cancel the operation, enter `N` at the confirmation prompt and press **Enter**, or simply press **Enter**.

```
(B,F,[Q]) : F

Select partition (0-7,[Q=Quit]) : 0
Select server blade (0,[Q=Quit]) : 0
Select card (1=I/O adapter,2=I/O adapter for expansion unit,[Q=Quit]) : 1
Select I/O adapter (0-1,[Q=Quit]) : 0

-- Backup file list --
No. Time
--- -------------------
  0 2009-03-09 21:10:46
  1 2009-03-10 08:45:46
  2 2009-03-10 10:41:15

Select backup data (0-2,[Q=Quit]) : 0 (Enter)
Input backup file name ([Q=Quit]) : conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Partition0> Creating backup file was completed.
- Backup file name is hba16-conf.backup.
Hit enter key. (Enter)
```

When the file containing the fibre channel card configuration has been completed, the file name is displayed: the prompt is ready for the Enter key. Press **Enter**, and the screen returns to the fibre channel HBA menu. The created file is stored in the user directory of the management module. You can take out the file via FTP or SFTP. The account name and password for connection via FTP or SFTP are the same as when you log in the system console.

Association between commands and permissions

The following table shows the association between commands and the permissions required for command execution.

	Command	Permission				
		Account	Chassis	Network	Switch module	Partition
1	BSM		Yes			
2	CER	Yes				
3	CHCO				Yes *1	Yes *1
4	CI		Yes			
5	DC		Yes			
6	DEL		Yes			
7	DF		Yes		Yes *1	
8	DH					Yes *2
9	DL		Yes			
10	ELI		Yes			
11	EX	None required				
12	FAN	None required				
13	FV		Yes			
14	FW		Yes			
15	HA		Yes			
16	HCSM		Yes			
17	HE	None required *3				
18	ILC			Yes		
19	LC			Yes		
20	LDAP		Yes			
21	LFT			Yes		
22	LM		Yes			
23	LS		Yes			
24	MAC		Yes			
25	MI		Yes			
26	MLC			Yes		
27	MMC		Yes			
28	PC					Yes *1
29	PR (configure partitions)					Yes *1
30	PR (create or delete partitions)		Yes			
31	PS		Yes			

	Command	Permission				
		Account	Chassis	Network	Switch module	Partition
32	PSM (display power supply module status)	None required				
33	PSM (other than displaying power supply module status)		Yes			
34	PSV		Yes			
35	SBC		Yes			
36	SC		Yes			
37	SCO (set inactivity timer)	None required				
38	SCO (other than setting inactivity timer)		Yes			
39	SD		Yes			
40	SDN		Yes			
41	SEC			Yes		
42	SNM		Yes			
43	SO (edit the logged-in account)	None required				
44	SO (other than edit ting logged-in account)	Yes				
45	ST		Yes			
46	SWC				Yes *1	
47	UBR		Yes			
48	UTL					Yes *1
49	WHO (display a session)	None required				
50	WHO (forcibly terminate a session)	Yes				
51	WWN		Yes			
52	XD			Yes		

Yes: Permission required to execute the command.

Yes*1: Executable only for partitions or switch modules designated as allowed.

Yes*2: Executable only when all partitions are designated as allowed.

None required: Executable without any permission.

None required*3: Executable without any permission. Only the commands executable by the user are displayed.

None required*4: Executable without any permission. Available operations are limited to changing the password, changing the console type, changing the inactivity timer setting, and changing the prompt type.

System web console

This section describes the system web console.

Functionality of the system web console

The Compute Blade 2000 Management Module's system web console provides a GUI interface for controlling a variety of Compute Blade 2000 features from a web browser on a client PC.

❑ Items to prepare

Client PC (hereafter referred to as "Client")

LAN cable (UTP-5 or better)

Table 6-1 describes the client requirements for using the system web console feature.

Table 6-1: Client Requirement

#	Item	Requirements
1	OS	Microsoft® Windows® Server 2008, Standard Edition Microsoft® Windows® Server 2008, Enterprise Edition Microsoft® Windows® Server 2003 R2, Standard Edition Microsoft® Windows® Server 2003 R2, Enterprise Edition Microsoft® Windows® Server 2003, Standard Edition Microsoft® Windows® Server 2003, Enterprise Edition Microsoft® Windows® XP Professional Microsoft® Windows® 2000 Professional Microsoft® Windows® Vista Business
2	Browser	Internet Explorer 6.0 or later versions (Tab functions of the browser, however, are not available.)
3	Display resolution	800 x 600 or later with 65536 or more colors (1280 x 1024 or later is recommended.)

❑ Client settings

Ensure that you perform the following settings.

Check the browser settings on the client before using the system web console.

The system web console may not work properly if the browser is not set up in the correct way.

Ensure that the proxy server settings allow connections to the management module.

Ensure that the browser is configured to download and run JavaScript.

Add the IP address of the management module to the list of trusted sites.

Disable any pop-up blocking features of the browser.

Ensure that the browser is set up to display images.

Ensure that cookies are enabled.

For Internet Explorer 8 or higher, enable Compatibility View.

For details about how to perform these settings, see the manual for your operating system.

❑ List of system web console features

The following table lists the settings that can be set and information that can be displayed on the system web console.

#	Screen name	Feature	Refer to the page
1	Physical Partition Management	Displays the status of physical partitions and perform associated tasks.	665
2	Server Blade Management	Displays the status of the server blade and perform associated tasks.	670
3	I/O Adapter Management	Displays the status of the I/O adapter and perform associated tasks.	674
4	Switch Module Management	Displays the status of switch modules and perform associated tasks.	676
5	Management Module Management	Displays the status of the management module and perform associated tasks.	679
6	Cooling Fan Module Management	Displays the status of fan modules.	683
7	Power Supply Module Management	Displays the status of power supply modules.	685
8	Server Chassis Management	Displays information about WWNs, FRUs, and sensors in the server chassis.	687
9	Session Management	Manages connections to the management module.	707
10	Physical Partition Settings	Changes the configuration and attributes of physical partitions.	708
11	User Account Settings	Sets up user accounts and roles.	713
12	Configuration of Network	Performs network-related settings.	715
13	Service Settings	Configures a range of network protocols.	723
14	Server Chassis Settings	Sets the power supply linkage.	729
15	Power Settings	Displays the current status of the power supply, and set up power control.	730
16	Time Settings	Sets the system time and whether daylight saving is in effect.	733
17	Language Setting	Sets a language used for displaying web console and SVP log.	735
18	Console Settings	Sets the inactivity timer for the system web console.	736
19	Backing up and Restoring the Settings	Backs up and restore settings related to the management module, server blade, FC card module, and LPAR manager.	737
20	SC/BSM Settings	Sets up linkage with SC/BSM.	740
21	HCSM Settings	Sets up linkage with HCSM.	742
22	SNMP Settings	Sets up SNMP.	744
23	E-mail Notification	Sets up remote email notification.	747

#	Screen name	Feature	Refer to the page
24	HA Monitor Settings	Configures the HA monitor.	750
25	LDAP Monitor Settings	Sets the LDAP monitor.	751
26	Firmware Management	Displays the firmware versions of the management module and server blade.	754
27	Log Management	Displays a variety of log information.	757

Login and logout

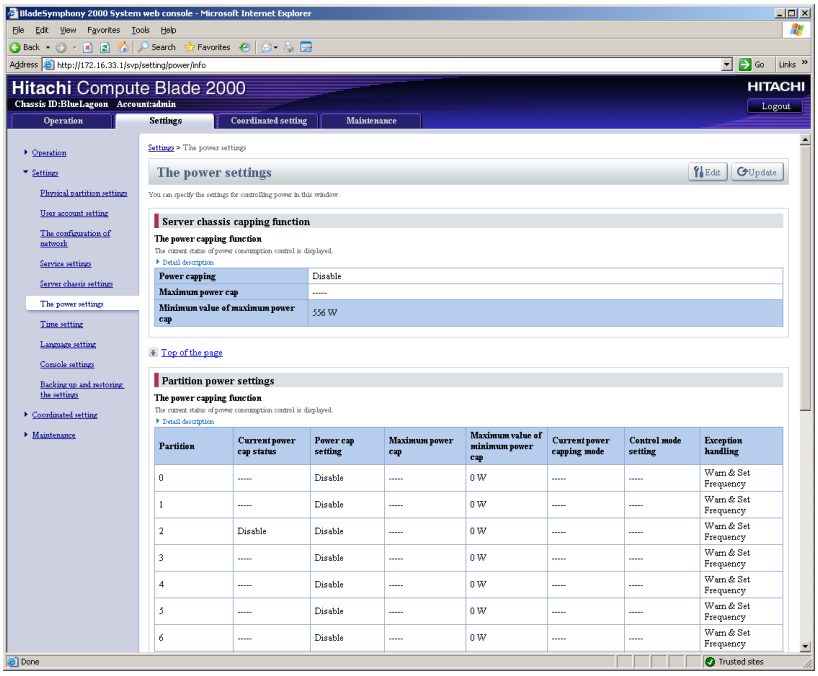
For details about how to log in and out from the system web console, see "Logging in from the System Web Console".

A maximum of 18 sessions can be established with the system web console at one time, or 19 including the session established with the system console.

Operation screen

When you are successfully logged in to the system web console, the operation screen appears.

The basic layout of the operation screen is as follows:



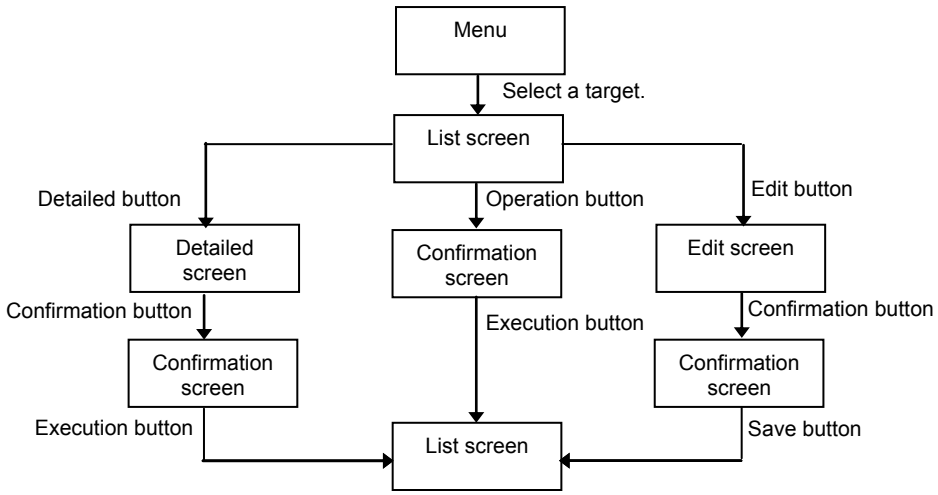
#	Item	Description
1	Chassis ID	The chassis ID of the server chassis to which you are logged in.
2	User account	The account name of the logged-in user.
3	Log out	Takes you to the logout screen. Click this button to exit system web console.
4	Menu	Click a menu item to navigate to the associated screen.
5	Refresh	Updates the information displayed in the browser window. This button does not appear with pages that do not require updating.
6	Edit	Takes you to the editing screen where you can edit the information displayed in the browser window. This button does not appear with pages that do not require editing, or if the user does not have editing permission.

To navigate to a specific page, click the page name in the menu on the left of the operation screen.



The available menu items depend on the role assigned to the logged-in user.

Operation of the system web console from the operation screen typically takes the following pattern:



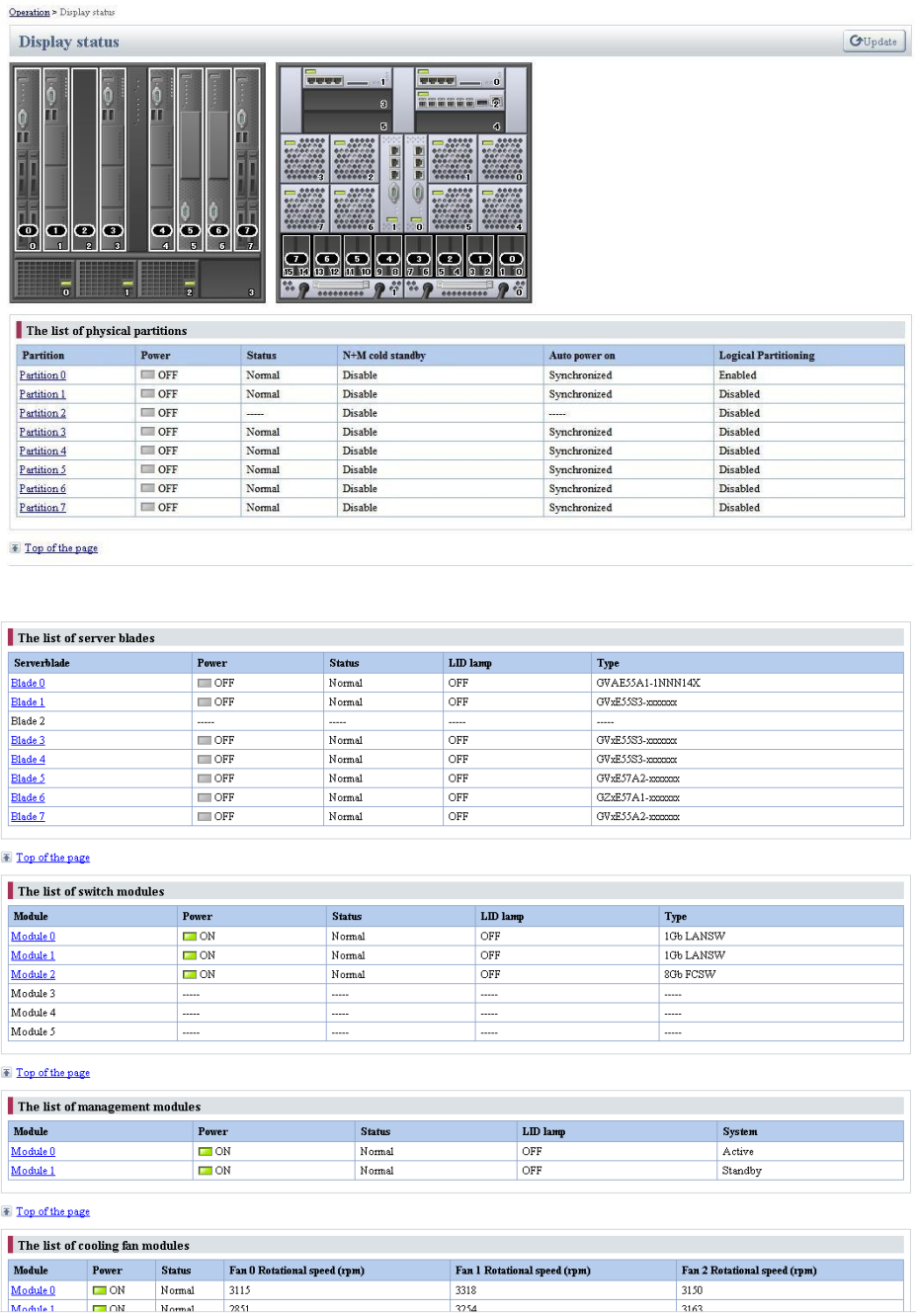
The following table describes how to interpret the information on the following pages.

#	Item	Description	Edit
	The name of the GUI item	A description of the GUI item	Indicates whether the item can be edited in the editing page. "Yes" in this column indicates that the item can be edited.

Status display

Displays the current status of the server chassis in list form.

❑ Status display view



Operation > Display status

Display status

Update

The list of physical partitions

Partition	Power	Status	N+M cold standby	Auto power on	Logical Partitioning
Partition 0	OFF	Normal	Disable	Synchronized	Enabled
Partition 1	OFF	Normal	Disable	Synchronized	Disabled
Partition 2	OFF	-----	Disable	-----	Disabled
Partition 3	OFF	Normal	Disable	Synchronized	Disabled
Partition 4	OFF	Normal	Disable	Synchronized	Disabled
Partition 5	OFF	Normal	Disable	Synchronized	Disabled
Partition 6	OFF	Normal	Disable	Synchronized	Disabled
Partition 7	OFF	Normal	Disable	Synchronized	Disabled

Top of the page

The list of server blades

Serverblade	Power	Status	LID lamp	Type
Blade 0	OFF	Normal	OFF	GVAE55A1-1NNN14X
Blade 1	OFF	Normal	OFF	GVxE55S3-xxxxxx
Blade 2	-----	-----	-----	-----
Blade 3	OFF	Normal	OFF	GVxE55S3-xxxxxx
Blade 4	OFF	Normal	OFF	GVxE55S3-xxxxxx
Blade 5	OFF	Normal	OFF	GVxE57A2-xxxxxx
Blade 6	OFF	Normal	OFF	GZxE57A1-xxxxxx
Blade 7	OFF	Normal	OFF	GVxE55A2-xxxxxx

Top of the page

The list of switch modules

Module	Power	Status	LID lamp	Type
Module 0	ON	Normal	OFF	1Gb LANSW
Module 1	ON	Normal	OFF	1Gb LANSW
Module 2	ON	Normal	OFF	8Gb FCSW
Module 3	-----	-----	-----	-----
Module 4	-----	-----	-----	-----
Module 5	-----	-----	-----	-----

Top of the page

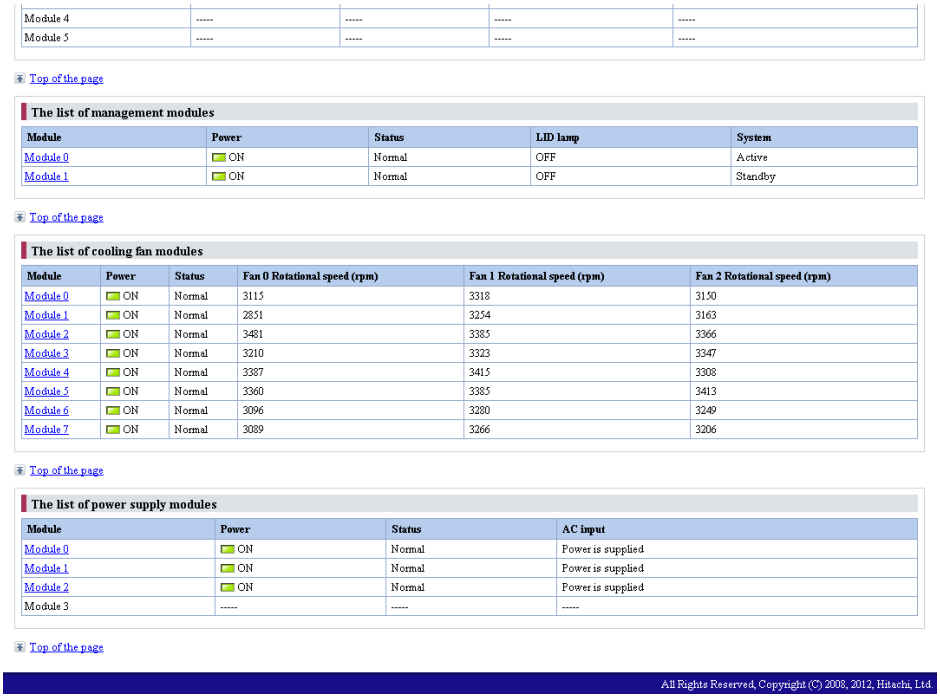
The list of management modules

Module	Power	Status	LID lamp	System
Module 0	ON	Normal	OFF	Active
Module 1	ON	Normal	OFF	Standby

Top of the page

The list of cooling fan modules

Module	Power	Status	Fan 0 Rotational speed (rpm)	Fan 1 Rotational speed (rpm)	Fan 2 Rotational speed (rpm)
Module 0	ON	Normal	3115	3318	3150
Module 1	ON	Normal	2851	3254	3163



Module 4	-----	-----	-----	-----
Module 5	-----	-----	-----	-----

Top of the page

The list of management modules

Module	Power	Status	LID lamp	System
Module 0	ON	Normal	OFF	Active
Module 1	ON	Normal	OFF	Standby

Top of the page

The list of cooling fan modules

Module	Power	Status	Fan 0 Rotational speed (rpm)	Fan 1 Rotational speed (rpm)	Fan 2 Rotational speed (rpm)
Module 0	ON	Normal	3115	3318	3150
Module 1	ON	Normal	2851	3254	3163
Module 2	ON	Normal	3481	3385	3366
Module 3	ON	Normal	3210	3323	3347
Module 4	ON	Normal	3387	3415	3308
Module 5	ON	Normal	3360	3385	3413
Module 6	ON	Normal	3096	3280	3249
Module 7	ON	Normal	3089	3266	3206

Top of the page

The list of power supply modules

Module	Power	Status	AC input
Module 0	ON	Normal	Power is supplied
Module 1	ON	Normal	Power is supplied
Module 2	ON	Normal	Power is supplied
Module 3	-----	-----	-----

Top of the page

All Rights Reserved, Copyright (C) 2008, 2012, Hitachi, Ltd.

For details about the displayed items, see the description of the management view for each module.

❑ Role-dependent variation in available operations

- To display detailed information about a partition, the user must have partition permission for that partition.
- To display detailed information about the respective modules, the user must have chassis permission.

Physical partition management

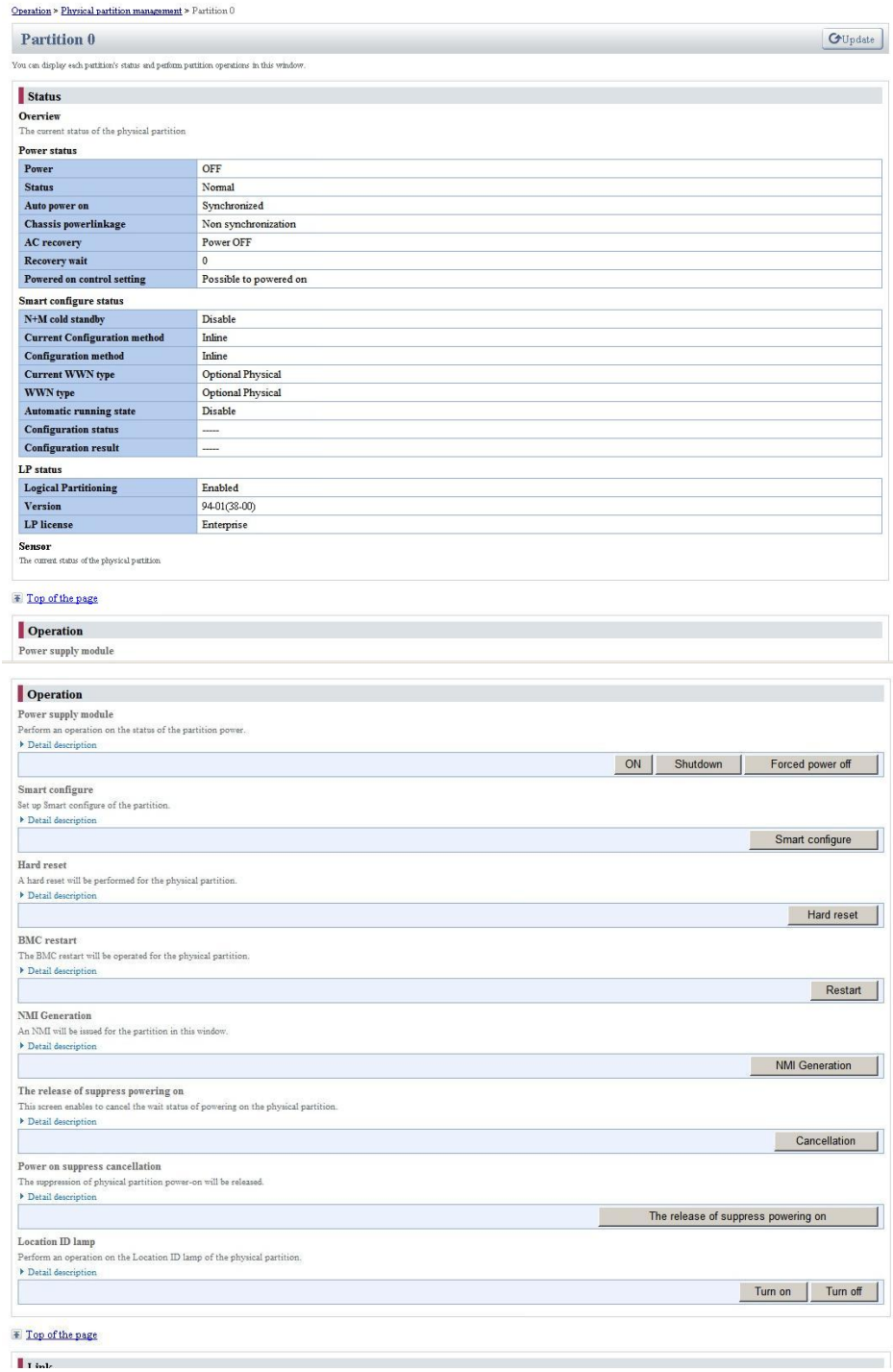
In the physical partition management view, you can display the status of physical partitions, and perform associated tasks.

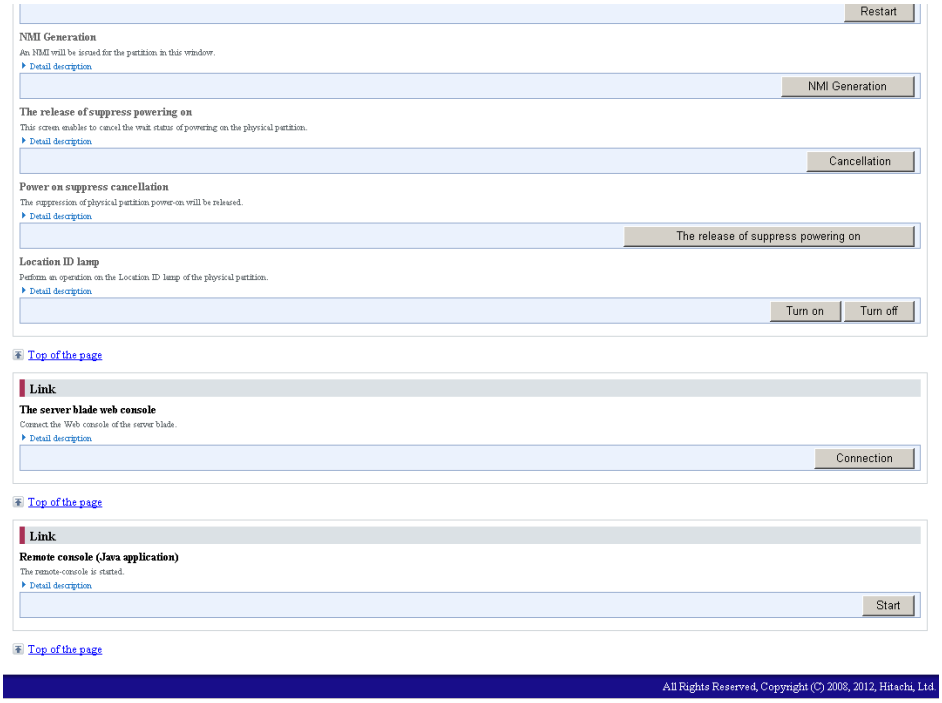
❑ List of physical partitions



#	Item	Description
1	Partition	The physical partition number. If the number appears as a hyperlink, clicking the link takes you to the Physical Partition Details view.
2	Power	The power status of the physical partition. Set as: ON or OFF
3	Status	The operating status of the physical partition. Set as: Normal, Init. Fail, Initializing, or Error.
4	N+M cold standby	Indicates N+M cold standby is Enabled or Disabled.
5	Auto power on	Setting whether or not the physical partition powers on automatically synchronized with the power-on to the server chassis: ”Synchronized” or “------“ as not synchronized.
6	Logical Partitioning	Indicates Logical Partitioning is: Disabled or Enabled
7	ON	Turns on power to the physical partitions whose check boxes are selected.
8	Shutdown	Shuts down the physical partitions whose check boxes are selected.

❑ Details of a physical partition





#	Item	Description
1	Power	The power status of the physical partition. Set as: ON or OFF
2	Status	The operating status of the physical partition. Set as: Normal, Init. Fail, Initializing, or Error
3	Auto power on	Setting whether or not the physical partition powers on automatically synchronized with the power on to the server chassis: ”Synchronized” or “------“ as not synchronized.
4	Chassis powerlinkage	Indicates whether the operation of the power supply to the physical partition is linked to activation of the power supply of the server chassis. Set as: Link or Do not link (This item is not supported. To be synchronized with the power operation for the chassis regardless of this setting value.)
5	AC recovery	Indicates what behavior the physical partition power supply adopts when power is restored to the server chassis. Set as: Remain OFF, Turn ON, or Maintain status before power failure
6	Recovery wait	Indicates how long the system waits before performing the action specified above. Set as: 0 to 60
7	Powered on control setting	Status whether or not restriction on powering on the partition is enabled: Power-on enabled or Power-on restricted.
8	N+M cold standby	Indicates whether the N+M cold standby function is enabled for the physical partition. Set as: Enabled or Disabled
9	Current Configuration	Preboot eXecution Environment (PXE) or Inline depending on settings and the type of a server blade. When no server blade is installed or the partition in

#	Item	Description
		initialization, "-------" is displayed.
10	Configuration method	Value: PXE or Inline
11	Current WWN type	The current type of WWN for Smart Configure. Value: Optional Physical WWN or Default Physical WWN depending on settings and the type of a server blade. When no server blade is installed, or the partition in initialization, "-------" is displayed.
12	WWN type	The type of WWN to be used for Smart Configure. Value: Optional Physical WWN or Default Physical WWN depending on settings and the type of a server blade.
13	Automatic running state	Displays whether or not Smart Configure is set to be automatically executed: valid or invalid.
14	Configuration status	The execution status of the Smart Configure function. Set as: No Information, Not Configured, In Progress, or Configured.
15	Configuration result	The execution result of the Smart Configure function. Set as: Do not Care, OK, or NG
16	Logical Partitioning	Indicates whether the logical partitioning is disabled or enabled. Set as: Disabled or Enabled
17	LP version	The version of LPAR manager installed on the physical partition.
18	LP license	LPAR manager license of the physical partition.
19	Sensors	The values reported by the sensors in the server blade installed in the physical partition.
20	ON	Turns on power to the physical partition.
21	Shutdown	Shuts down the physical partition.
22	Forced power off	Forcibly powers off the physical partition.
23	Smart Configure	Perform Smart Configure on the physical partition.
24	Hard reset	Performs a hard reset of the physical partition.
25	Restart	Restarts the physical partition.
26	NMI Generation	Issues a non-maskable interrupt (NMI) to the physical partition.
27	Cancellation	Cancels the power on wait of the physical partition
28	The release of suppress powering on	When the physical partition is in power ON control suppression status, cancels the suppression status for the physical partition.
29	Turn on	Turns on the Location ID LED for the physical partition.
30	Turn off	Turns off the Location ID LED for the physical partition.
31	Connection	Connects to the server blade web console running on the server blade. You can automatically log into the server blade web console with Login and Administrator privileges. This button appears only with the management module firmware version A0182 or later.
32	Start	The remote console application starts downloading. You can automatically log in to the server blade web console with Login and Administrator privileges. This button appears only with the management module firmware version A0182 or later.

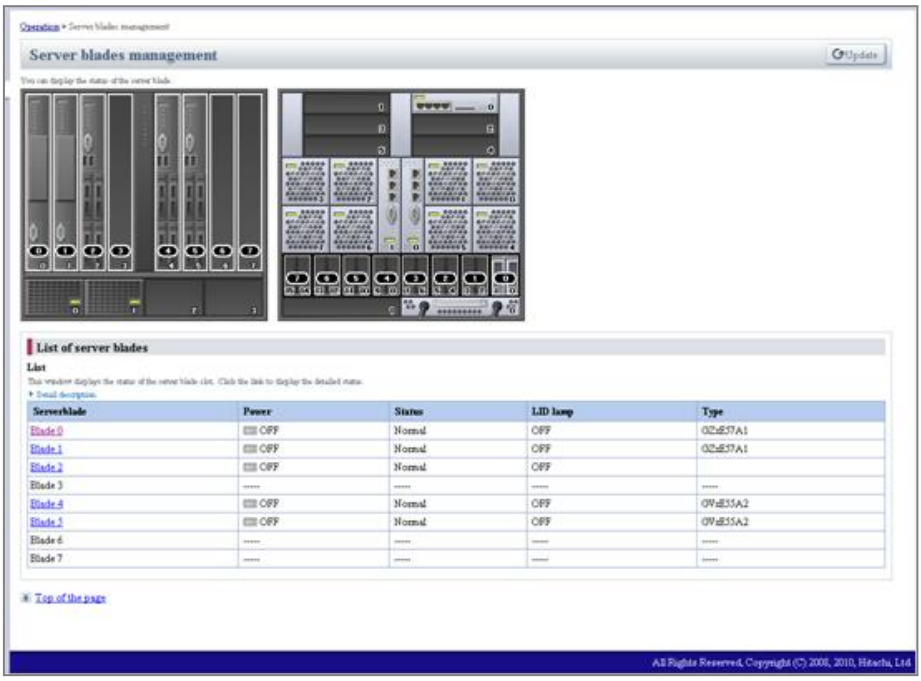
❑ Role-dependent variation in available operations

- To display detailed information about a partition, the user must have partition permission for that partition.
- To perform actions on a partition, the user must have partition permission for that partition.

Server blade management

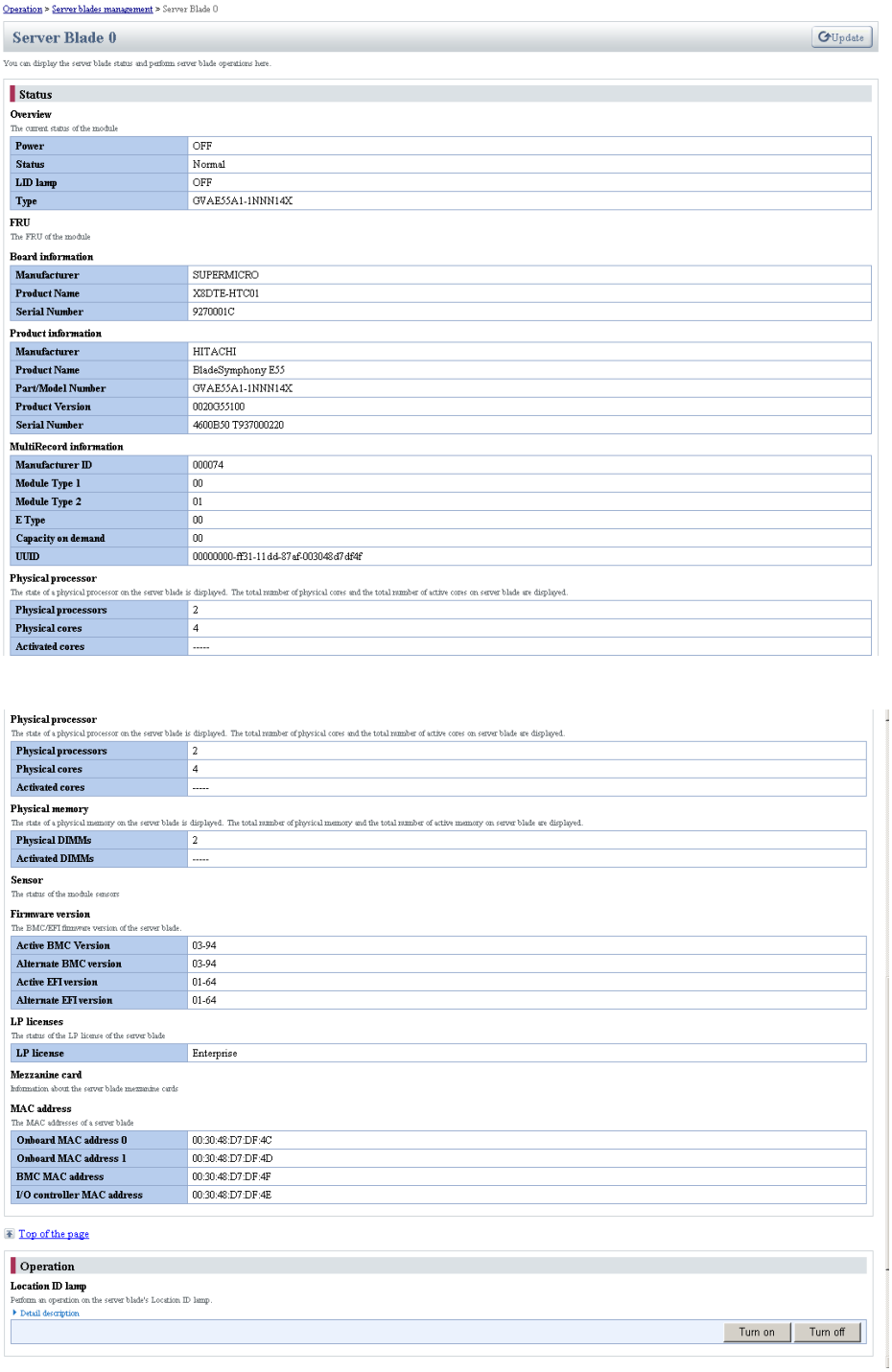
In the Server blade management view, you can display the status of server blades and perform associated tasks.

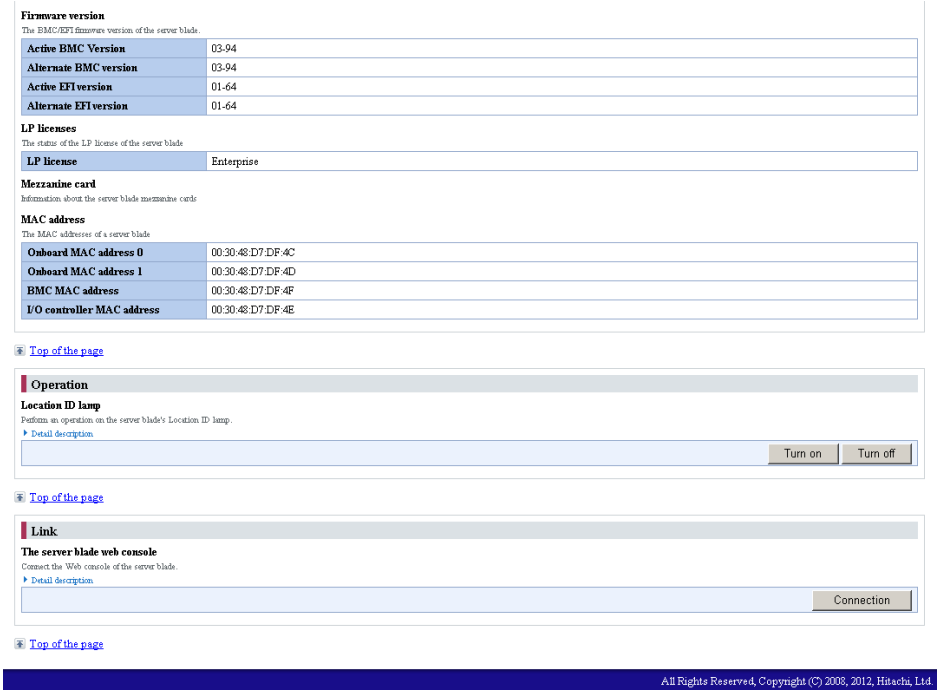
❑ Server blade list view



#	Item	Description
1	Server blade	The server blade number. If the number appears as a hyperlink, clicking the link takes you to the Server Blade Details view.
2	Power	The power status of the server blade. Set as: ON or OFF
3	Status	The operating status of the server blade. Set as: Normal, Init. Fail, Initializing, or Error
4	LID LED	The status of the Location ID LED for the server blade. Set as: Lit or Unlit
5	Type	The type of server blade.

❑ Server blade details view





Firmware version

The BMC/EFI firmware version of the server blade.

Active BMC Version	03-94
Alternate BMC version	03-94
Active EFI version	01-64
Alternate EFI version	01-64

LP licenses

The status of the LP license of the server blade

LP license	Enterprise

Mezzanine card

Information about the server blade mezzanine cards

MAC address

The MAC addresses of a server blade

Onboard MAC address 0	00:30:48:D7:DF:4C
Onboard MAC address 1	00:30:48:D7:DF:4D
BMC MAC address	00:30:48:D7:DF:4F
I/O controller MAC address	00:30:48:D7:DF:4E

Top of the page

Operation

Location ID lamp

Perform an operation on the server blade's Location ID lamp.

Detail description

Turn on | Turn off

Top of the page

Link

The server blade web console

Connect the Web console of the server blade.

Detail description

Connection

Top of the page

All Rights Reserved, Copyright (C) 2008, 2012, Hitachi, Ltd.

#	Item	Description
1	Power	The power status of the server blade. Set as: ON or OFF
2	Status	The operating status of the server blade. Set as: Normal, Init. Fail, Initializing, or Error
3	LID lamp	The status of the Location ID LED for the server blade. Set as: Lit or Unlit
4	Type	The type of server blade. Set as: Xeon A1 or Xeon EX A1
5	FRU	Information about FRUs in the server blade (under the categories Board, Product, and Multirecord) and mezzanine cards (under the category Product).
6	Physical processor	The state of a physical processor on the server blade
7	Physical memory	The state of a physical memory on the server blade.
8	Sensor	The values reported by the sensors incorporated into the server blade.
9	BMC version	The version of the BMC firmware in the server blade, including both currently active and alternative.
10	EFI version	The version of the EFI in the server blade, including both currently active and alternative.
11	LP licenses	The status of the LPAR manager license in the server blade. Set as: Install or Not Install for LPAR manager 4.0; Essential, Enterprise, or Not Install for LPAR manager 4.1 or later versions.
12	Mezzanine card	The WWNs allocated to the mezzanine cards installed in the server blade. The World Wide Port Name and World Wide Node Name are displayed for each port of each mezzanine card.
13	Inter-blade SMP connection board	Information (type and location) on the inter-blade SMP connection board installed in the server blade.
14	MAC address	The MAC addresses associated with the server blade. The on-board MAC address 0, on-board MAC address 1, BMC MAC address, and LPAR manager MAC address are all displayed.
15	Turn on	Turns on the Location ID LED for the server blade.
16	Turn off	Turns off the Location ID LED for the server blade.
17	Connection	Connects to the server blade web console running on the server blade.

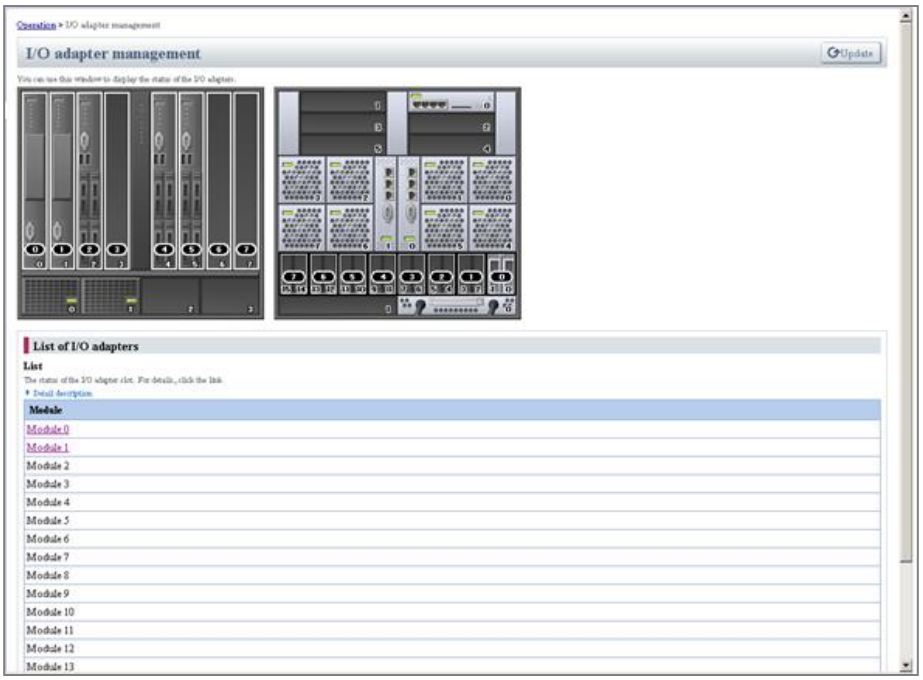
❑ Role-dependent variation in available operations

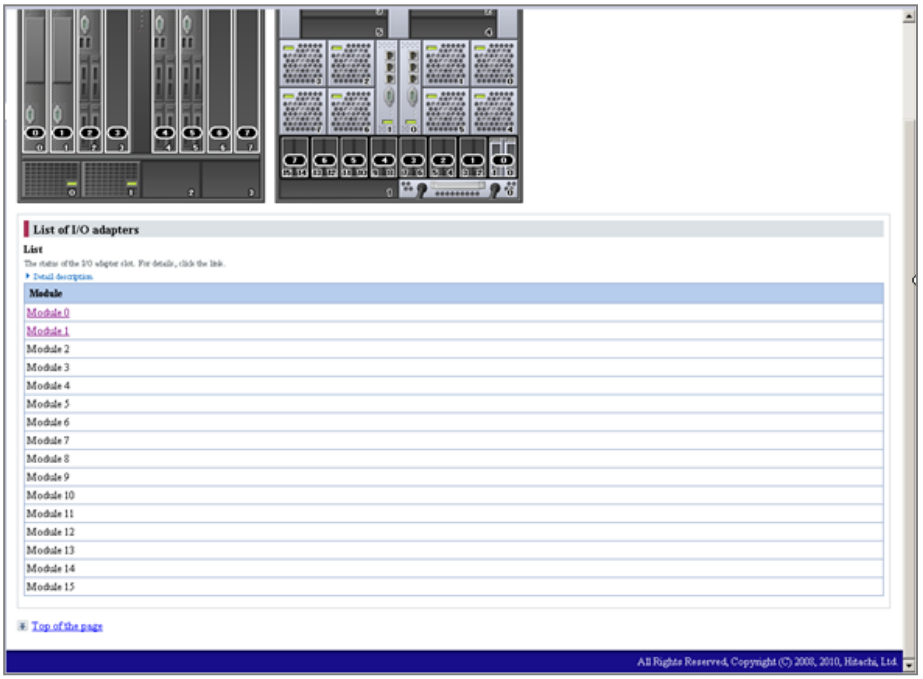
To display detailed information about a server blade, the user must have chassis permission.

I/O adapter management

In the I/O adapter management view, you can display the status of I/O adapters.

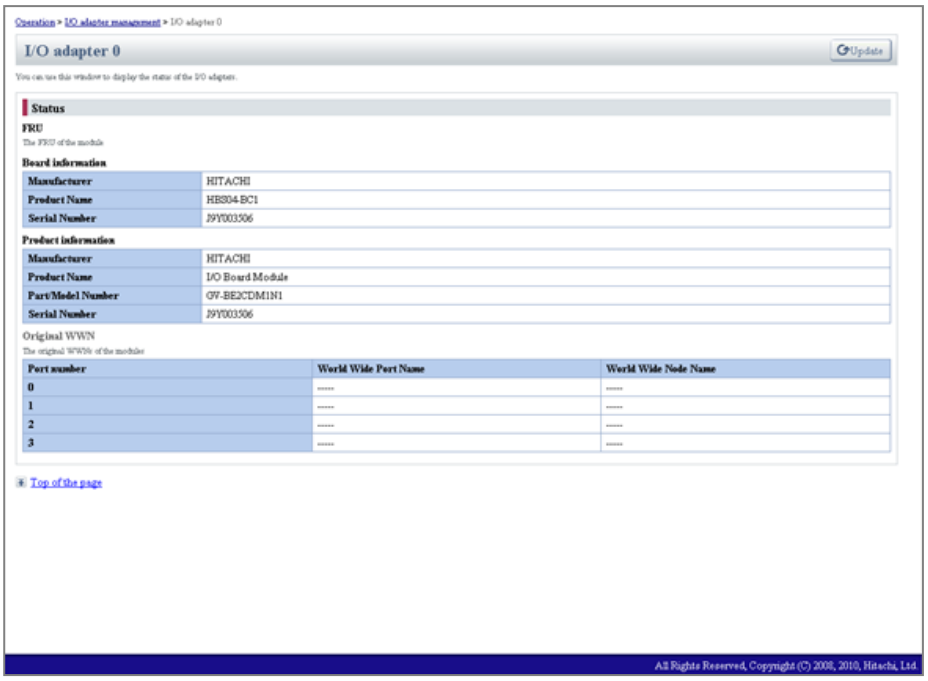
❑ I/O adapter list view





#	Item	Description
1	Module	The module number. If the number appears as a hyperlink, clicking the link takes you to the I/O Board Module Details view.

❑ I/O adapter details view



#	Item	Description
1	FRU	The FRU information (under the categories Board and Product) of the module.
2	Default Physical WWN	The WWNs allocated to the module. The World Wide Port Name and World Wide Node Name are displayed for each of the module's ports.

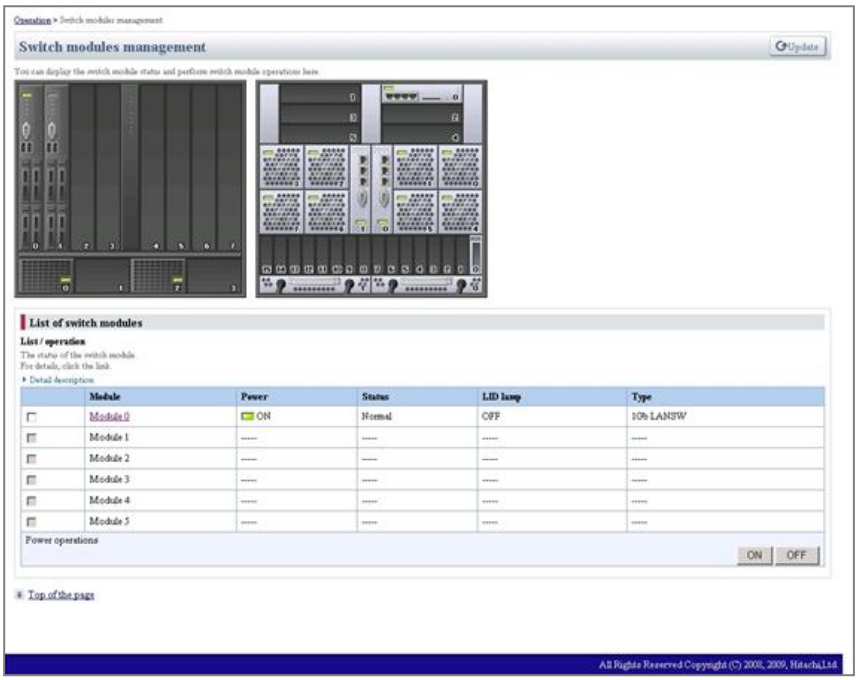
❑ Role-dependent variation in available operations

To display detailed information about a module, the user must have chassis permission.

Switch module management

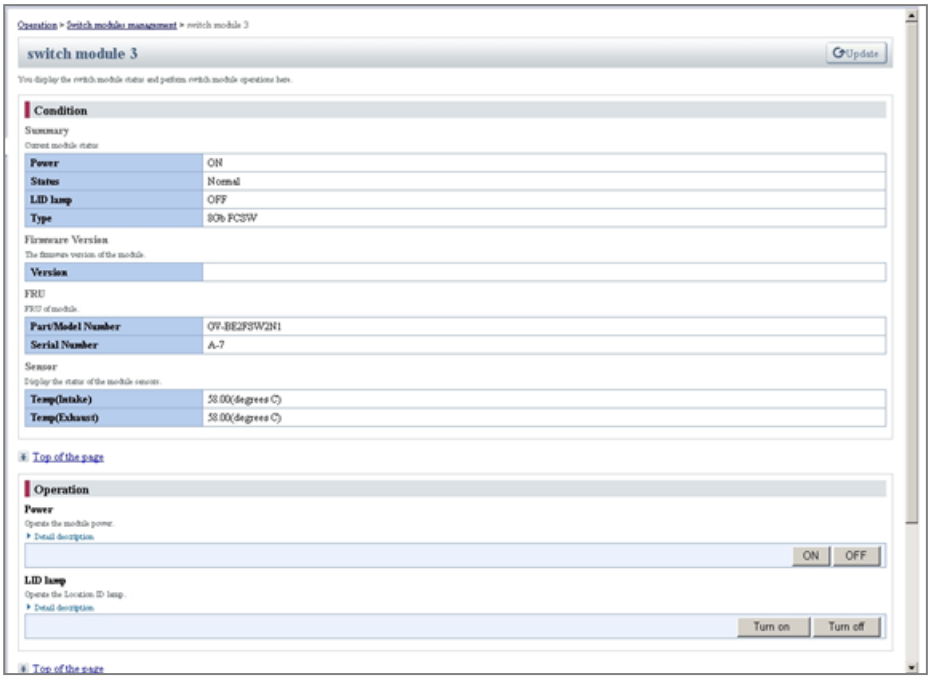
In the Switch module management view, you can display the status of switch modules, and perform associated tasks.

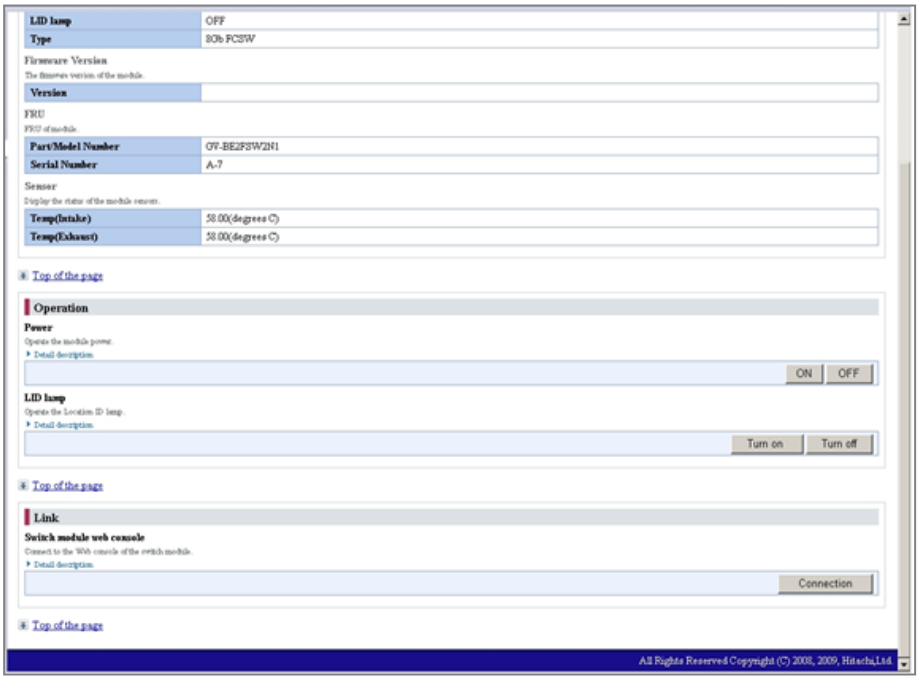
❑ Switch module list view



#	Item	Description
1	Module	The module number. If the number appears as a hyperlink, clicking the link takes you to the Switch module details view.
2	Power	The power status of the module. Set as: ON or OFF
3	Status	The operating status of the module. Set as: STARTING, NORMAL, CONFIG. ERROR, or ERROR
4	LID lamp	The status of the Location ID LED for the module. Set as: Lit or Unlit
5	Type	The type of the module. Set such as: 1Gb LANSW, 1_10 LANSW, or 8G FCSW
6	ON button	Powers on the modules whose check boxes are selected.
7	OFF button	Powers off the modules whose check boxes are selected.

❑ Switch module details view





#	Item	Description
1	Power	The power status of the module. Set as: ON or OFF
2	Status	The operating status of the module. Set as: STARTING, NORMAL, CONFIG. ERROR, or ERROR
3	LID lamp	The status of the Location ID LED for the module. Set as: Lit or Unlit

<table>
<tr><th>#</th><th>Item</th><th>Description</th></tr>
<tr><td>4</td><td>Type</td><td>The type of the module.
Set such as: 1Gb LANSW, 1_10 LANSW, or 8G FCSW</td></tr>
<tr><td>5</td><td>Version</td><td>Firmware version of the module</td></tr>
<tr><td>6</td><td>FRU</td><td>The FRU information for the module</td></tr>
<tr><td>7</td><td>Sensor</td><td>The value of a sensor installed in the switch module</td></tr>
<tr><td>8</td><td>ON</td><td>Turns on power to the module.</td></tr>
<tr><td>9</td><td>OFF</td><td>Turns off powers to the module.</td></tr>
<tr><td>10</td><td>Connection</td><td>Connects to the web console of the switch module. Web console-capable switch modules are as follows:
With the management module firmware version A0182 or later:
- 1 Gb LAN switch module
- 1/10 Gb LAN switch module
- Internal Fibre-channel switch
With the management module firmware version A0181 or earlier:
- Internal Fibre-channel switch
When you connect to the web console of a switch module using the Connection button, configure the switch module network as shown in the table below. Go to System web console > Settings > The configuration of network > Management LAN network general setting > The switch module to configure the settings to configure the settings.
<table>
<tr><th>Item</th><th>Connected to</th><th>IP address</th></tr>
<tr><td>1 Gb LAN switch module</td><td>Internal LAN network</td><td>Not required</td></tr>
<tr><td>1/10 Gb LAN switch module</td><td>Internal LAN network</td><td>Not required</td></tr>
<tr><td>Internal Fibre-channel switch</td><td>Management LAN network or an internal port of the switch module</td><td>Set an IP address for the PC to be connected to the web console.</td></tr>
</table>
If you have configured the settings shown above with the LAN switch module, check the switch module IP address referring to Chapter 13 > Network Settings > Setting the IP address.</td></tr>
<tr><td>11</td><td>Turn on</td><td>Turns on the Location ID LED for the module.</td></tr>
<tr><td>12</td><td>Turn off</td><td>Turns off the Location ID LED for the module.</td></tr>
</table>

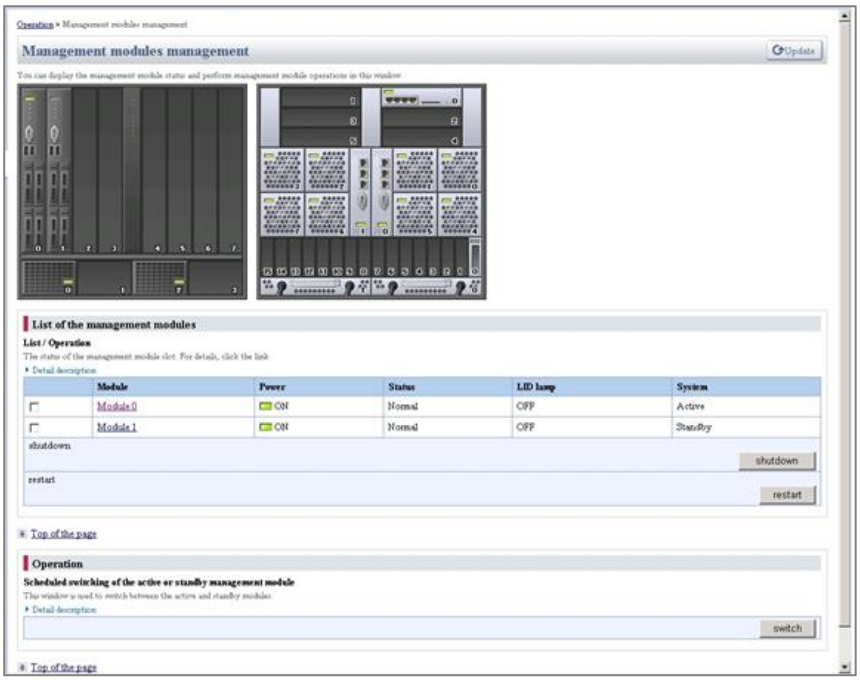
❑ Role-dependent variation in available operations

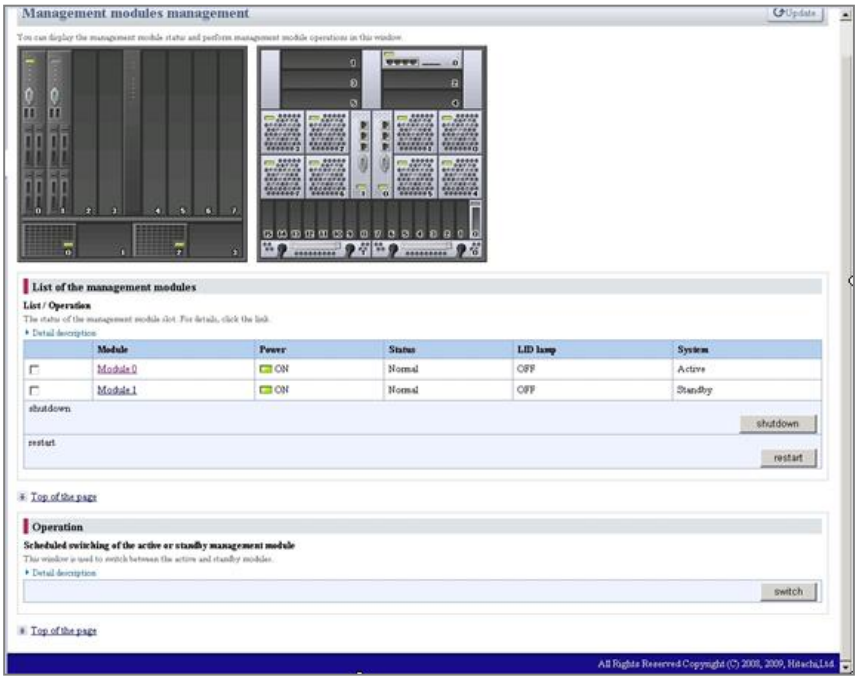
- To display detailed information about a switch module, the user must have switch module permission for that module.
- To perform actions on a switch module, the user must have switch module permission for that module.

Management module management

In the Management module management view, you can display the status of management modules, and perform associated tasks.

❑ Management module list view



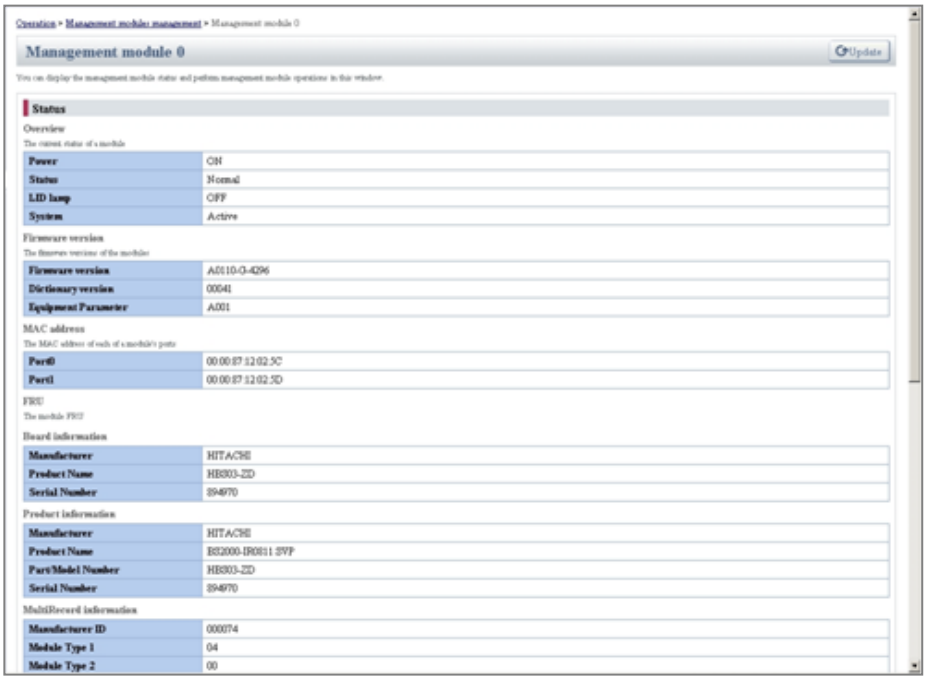


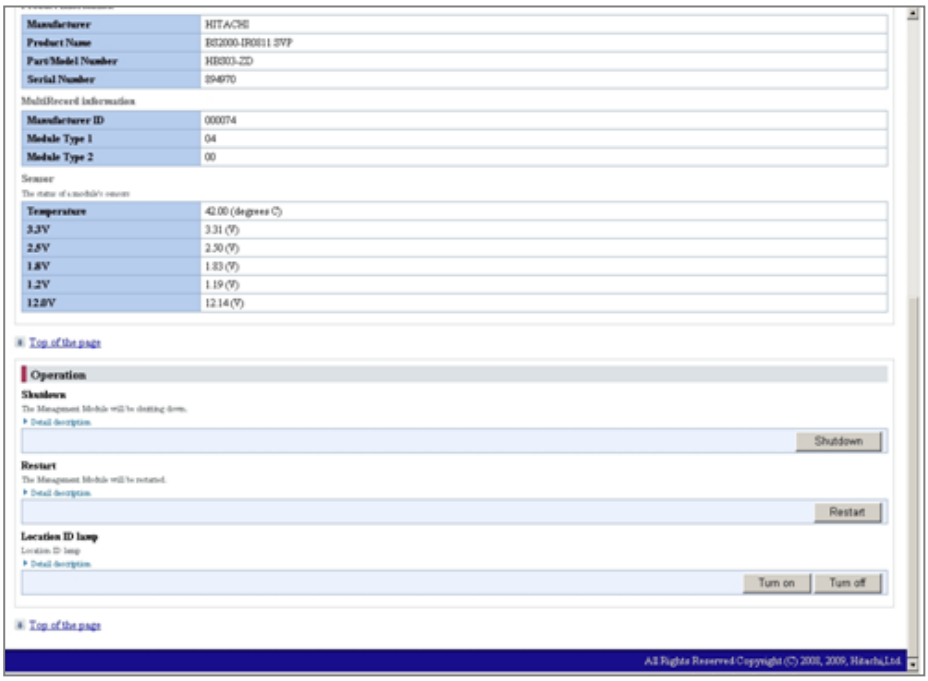
#	Item	Description
1	Module	The module number. If the number appears as a hyperlink, clicking the link takes you to the Management module details view.
2	Power	The power status of the module. Set as: ON or OFF
3	Status	The operating status of the module. Set as: Starting, Normal, BootDisable, Shutting Down, or Error
4	LID lamp	The status of the Location ID LED for the module. Set as: Lit or Unlit
5	System	Indicates whether the management module is serving as an active or standby system. Set as: Active or Standby
6	Shutdown	Shuts down the modules whose check boxes are selected.
7	Restart	Restarts the modules whose check boxes are selected.
8	Switch	Switches the roles of the active management module and the standby management module.



Do not perform Shutdown and Restart while the server blade is operating. Error events, which have occurred while the management module is restarting or shutting down, may not be detected.
When restarting and shutting down a management module while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

❑ Management module details view





#	Item	Description
1	Power	The power status of the module. Set as: ON or OFF
2	Status	The operating status of the module. Set as: Starting, Normal, BootDisable, Shutting Down, or Error
3	LID lamp	The status of the Location ID LED for the module. Set as: Lit or Unlit
4	System	Indicates whether the management module is serving as an active or standby system. Set as: Active or Standby
5	Firmware version	Displays the firmware version of the management module, dictionary version, and equipment parameter version.
6	MAC address	The MAC addresses associated with the module. The MAC addresses of Port 0 and Port 1 are displayed.
7	FRU	FRU information for the module (under categories Board, Product, and Multirecord).
8	Sensor	The values reported by the sensors in the module.
9	Shutdown	Shuts down the module.
10	Restart	Restarts the module.
11	Turning on	Turns on the Location ID LED for the module.
12	Turning off	Turns off the Location ID LED for the module.

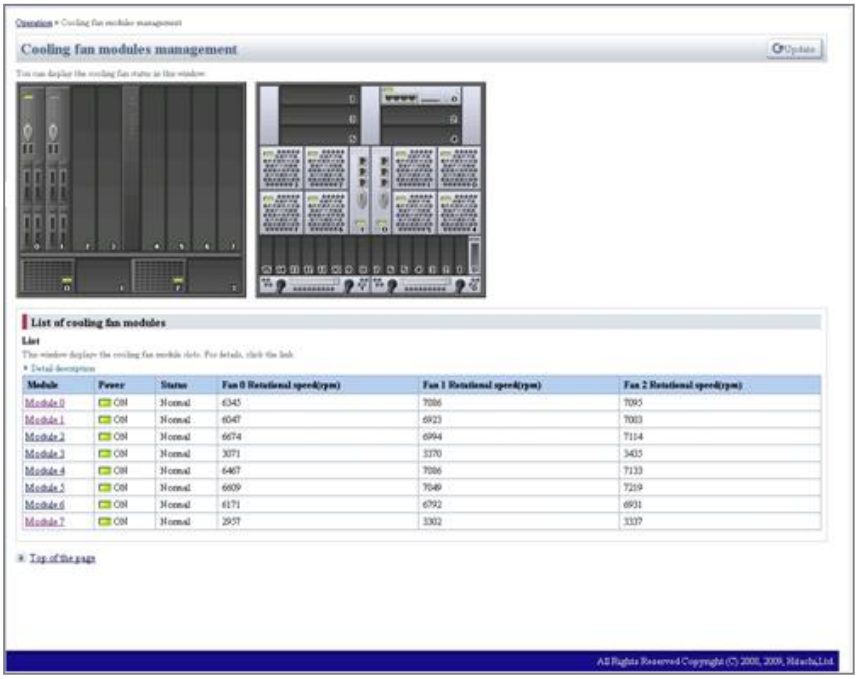
❑ Role-dependent variation in available operations

- To display detailed information about a module, the user must have chassis permission.
- To perform actions on a module, the user must have chassis permission.

Cooling fan module management

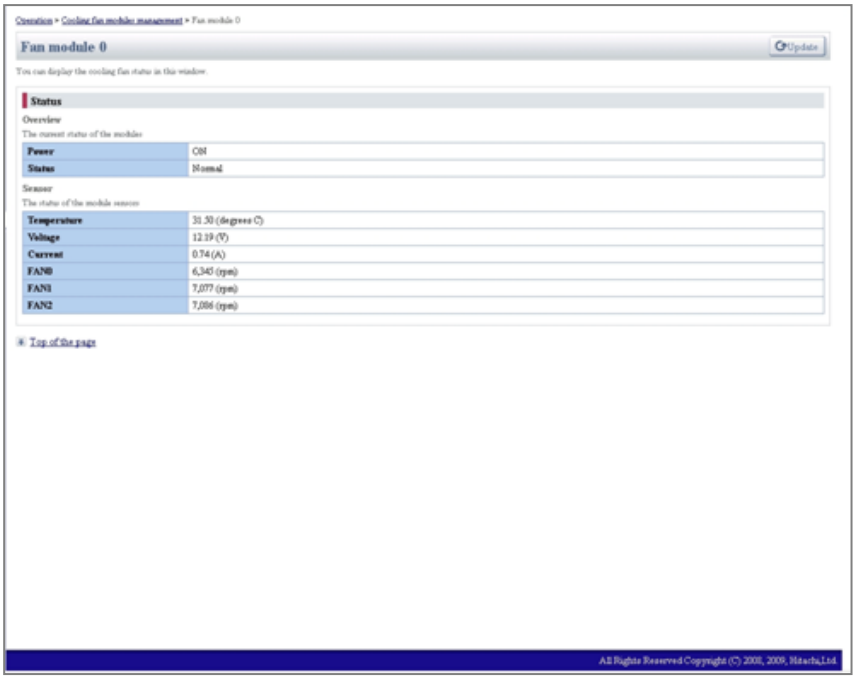
In the Cooling fan module management view, you can display the status of fan modules.

❑ Fan module list view



#	Item	Description
1	Module	The module number. If the number appears as a hyperlink, clicking the link takes you to the Fan module details view.
2	Power	The power status of the module. Set as: ON, Turning ON , OFF, or Turning OFF
3	Status	The operating status of the module. Set as: Normal or Error
4	Fan 0-2 Rotational speed (rpm)	The speed in revolutions per minute (RPM) of the fans within the fan module.

❑ Fan module details view



#	Item	Description
1	Power	The power status of the module. Set as: ON, Turning ON , OFF, or Turning OFF
2	Status	The operating status of the module. Set as: Normal or Error
3	Sensor	The values reported by the sensors in the module.

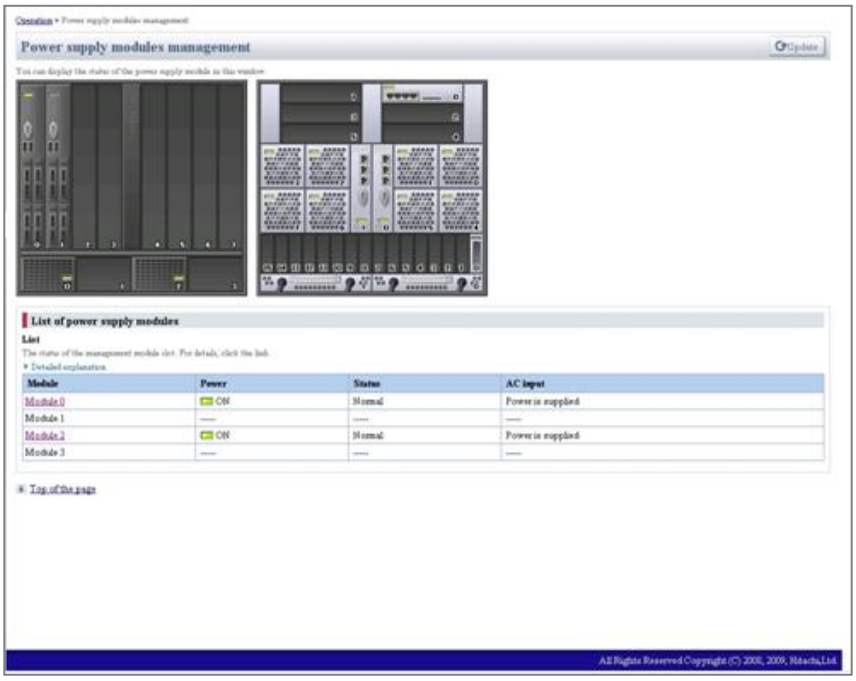
❑ Role-dependent variation in available operations

To display detailed information about a module, the user must have chassis permission.

Power supply module management

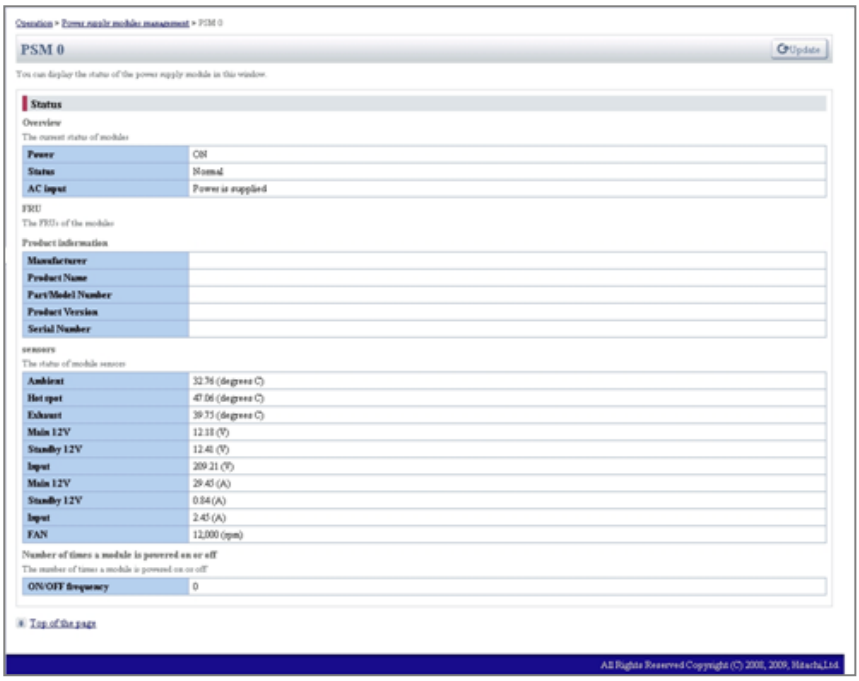
In the Power supply module management view, you can display the status of power supply modules.

❑ Power supply module list view



#	Item	Description
1	Module	The module number. If the number appears as a hyperlink, clicking the link takes you to the Power supply module details view.
2	Power	The power supply status of the module. Set as: ON, Turning ON , OFF, or Turning OFF
3	Status	The operating status of the module. Set as: Normal or Error
4	AC input	The status of the AC power supply to the module. Set as: AC input or No AC input

❑ Power supply module details view



#	Item	Description
1	Power	The power status of the module. Set as: ON, Turning ON , OFF, or Turning OFF
2	Status	The operating status of the module. Set as: Normal or Error
3	AC input	The status of the AC power supply to the module. Set as: AC input or No AC input
4	FRU	FRU information for the module (under the category Product).
5	Sensors	The values reported by the sensors in the module.
6	ON/OFF frequency	The number of times the power supply module has been switched off.

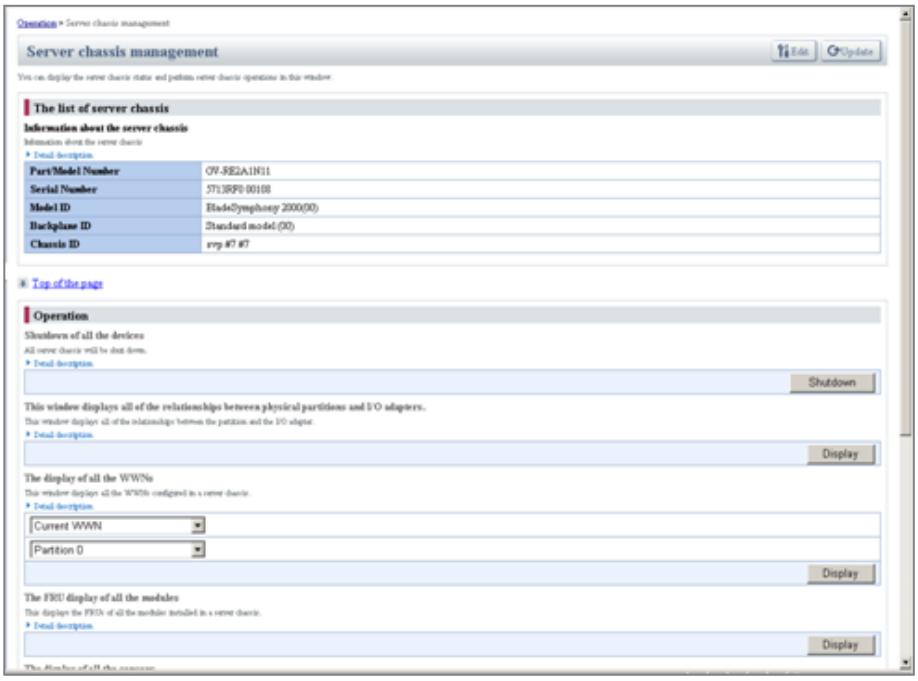
❑ Role-dependent variation in available operations

To display detailed information about a module, the user must have chassis permission.

Server chassis management

In the Server chassis management view, you can display the status of the server chassis, and perform associated tasks.

❑ Server chassis list view

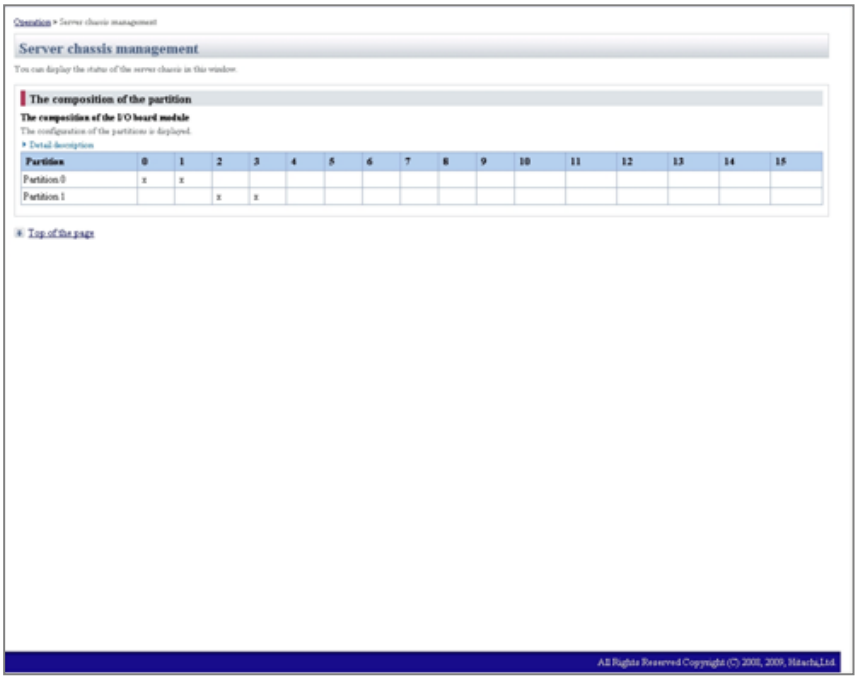




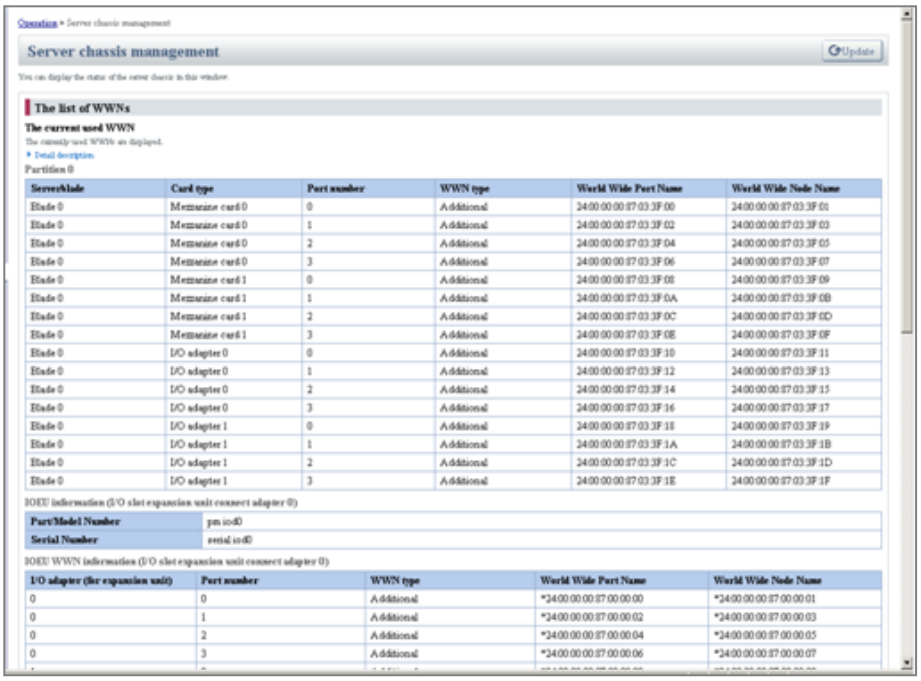
#	Item	Description	Edit
1	Part/Model Number	The model number of the server chassis.	
2	Serial Number	The serial number of the server chassis.	
3	Model ID	The product name of the server chassis.	
4	Backplane ID	The model name of the server chassis as identified from the backplane ID.	
5	Chassis ID	The chassis ID. You may enter a maximum of 20 ASCII characters.	✓
6	Shutdown	Shuts down the entire device.	
7	Display	Takes you to a view displaying the correspondence between physical partitions and I/O board modules.	
8	Display	Takes you to a page where you can view or set WWNs such as WWN currently used, Default Physical WWN, Optional Physical WWN, or also which partition information to display from the pull-down menu.	
9	Display	Takes you to a page displaying the FRU information for all modules.	
10	Display	Takes you to a page displaying the sensors for all modules.	
11	Display	Takes you to a page displaying the power consumption of the server chassis.	
12	Display	Takes you to a page displaying the weight of the server chassis and the rate of air flow supplied by the cooling fans.	
13	Display	Takes you to a page displaying the license of the server chassis.	

❑ Partition configuration list view

In this view, displays the associated I/O board module for each partition.



❑ Current WWN list view



Items of the partition information are described in the table below:

#	Item	Description	Edit
1	Serverblade	The server blade number.	
2	Card type	The type of card. May be a mezzanine card or I/O board module.	
3	Port number	The associated port number.	
4	WWN type	Default Physical or Optional Physical.	
5	World Wide Port Name	The World Wide Name (WWN) of the device. An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	
6	World Wide Node Name	The World Wide Name (WWN) associated with the port. An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	

Information about the I/O slot expansion unit connected to the I/O adapter is described in the table below (per I/O adapter connected to the I/O slot expansion unit).

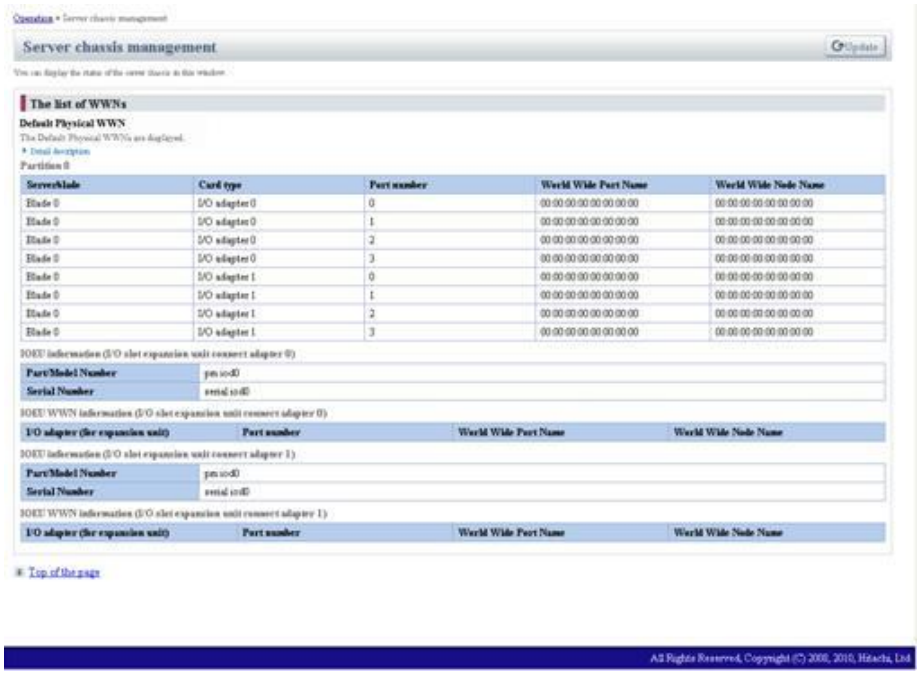
#	Item	Description	Edit
1	Part/Model Number	Part/Model number of the I/O slot expansion unit	-
2	Serial Number	Serial number of the I/O slot expansion unit	-

Items of information on the I/O slot expansion unit connected to the I/O adapter are described in the table below (per I/O adapter connected to the I/O slot expansion unit).

#	Item	Description	Edit
1	I/O adapter for I/O slot expansion units	Slot numbers of the I/O adapter on the I/O slot expansion unit.	-

#	Item	Description	Edit
2	Port number	-	-
3	WWN type	Default Physical WWN and Optional Physical WWN	
4	World Wide Port Name	The World Wide Name (WWN) An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	-
5	World Wide Node Name	WWN An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	-

❑ Default Physical WWN List view



Items of the partition information are described in the table below:

#	Item	Description	Edit
1	Serverblade	The server blade number.	
2	Card type	The type of card. Set as: Mezzanine card or I/O board module.	
3	Port number	The port number.	
4	World Wide Port Name	The World Wide Name (WWN) of the device.	
5	World Wide Node Name	The World Wide Name (WWN) of the device.	

Items of information on the I/O slot expansion unit connected to the I/O adapter are described in the table below (per I/O adapter connected to the I/O slot expansion unit).

#	Item	Description	Edit
1	Part/Model Number	Part/Model number of the I/O slot expansion unit	-
2	Serial Number	Serial number of the I/O slot expansion unit	-

Items of information on the I/O slot expansion unit connected to the I/O adapter are described in the table below (per I/O adapter connected to the I/O slot expansion unit).

#	Item	Description	Edit
1	I/O adapter for I/O slot expansion units	Slot numbers of the I/O adapter on the I/O slot expansion unit.	-
2	Port number	-	-
3	World Wide Port Name	The World Wide Name (WWN) An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	-
4	World Wide Node Name	WWN An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	-



- When a fibre channel adapter has two ports, information on four ports is displayed. In this case, WWNs unique to the fibre channel adapter are displayed in port0 and port1, and a value consisting of all 0, zero, is displayed in port2 and port3 as WWN.
- For 10 Gb CNA adapter or 10 Gb CNA board, the following values are shown.
  - WWN for port 0 is the WWN value for port 0 of the controller 0.
  - WWN for port 1 is the WWN value for port 1 of the controller 0.
  - WWN for port 2 is the WWN value for port 0 of the controller 1.
  - WWN for port 3 is the WWN value for port 1 of the controller 1.

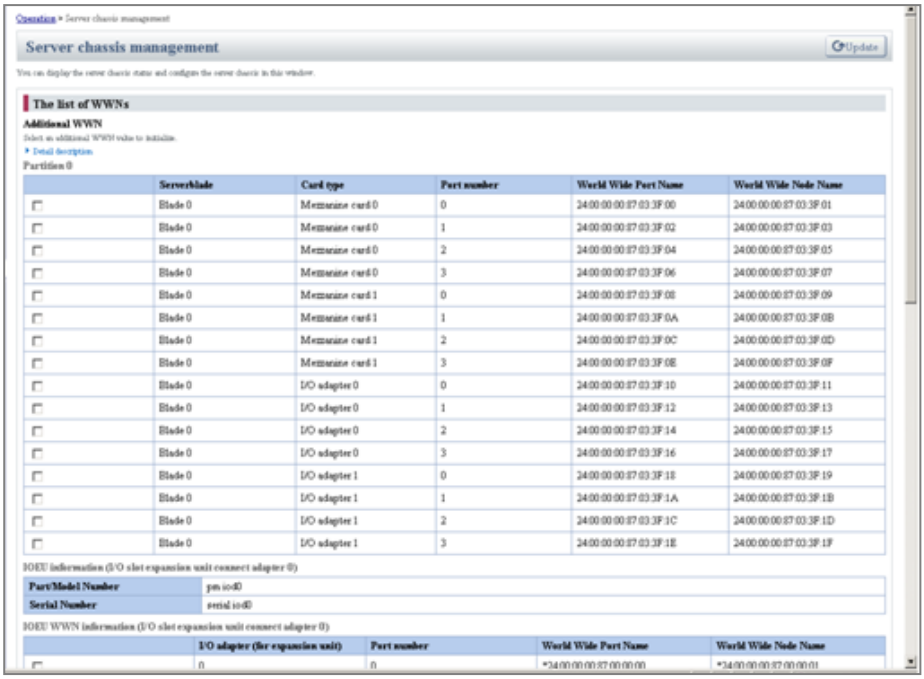
  WWN is shown only when CNA Personality setting is FCoE.
  When a single CNA controller is installed, WWN values for port 2 and port 3 are shown as all 0, zero.
- For Emulex 8 Gb 2-port fibre channel mezzanine card, current WWN may be shown in the Default Physical WWN field.
  - Applicable EFI firmware versions with each server blade model are as follows:
    - All EFI firmware versions with standard server blade X55A1 and X55A2 models
    - All EFI firmware versions with high-performance server blade X57A1 model
    - EFI version 07-29/08-29 or earlier with high-performance server blade X57A2 model
  - To find the Default Physical WWN for Emulex 8 GB 2-port fibre channel mezzanine card, perform the following steps:
    1. Shut down the OS and power off the server blade.
    2. Power on the server blade and boot the OS.
    3. Check the Default Physical WWN without rebooting the OS.

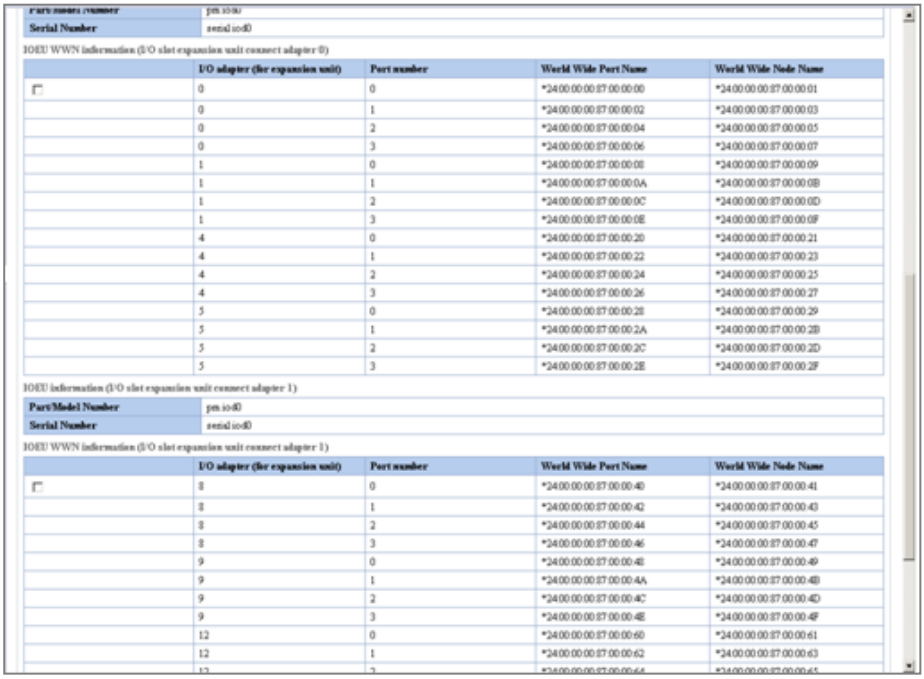


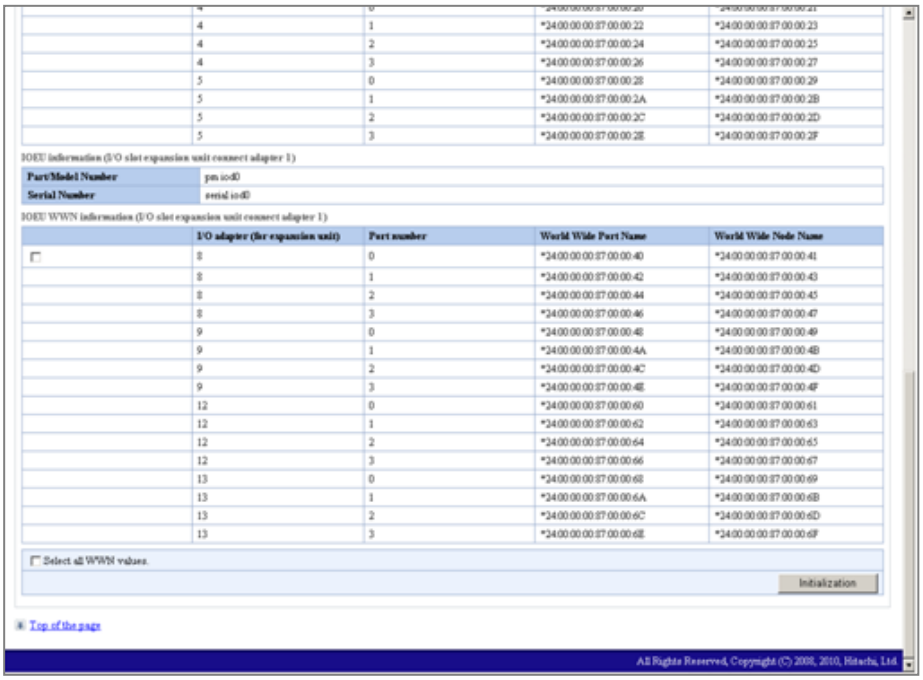
For the fibre channel mezzanine card, Default Physical WWN may be shown as a value consisting of all zeros.

- How to check Default Physical WWN
  - For Emulex fibre channel mezzanine card
    See *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI edition)* to check it on the BIOS Utility screen.
  - For Hitachi fibre channel mezzanine card
    See *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)* to check it on the SELECT HBA screen.
- Applicable EFI firmware version with each server blade model is as follows:
  - EFI firmware version 09-33/10-33 or earlier with standard server blade X55S3/X55R3 models.

❑ Optional Physical WWN list view







Items of the partition information are described in the table below:

#	Item	Description	Edit
1	Server blade	The server blade number.	
2	Card type	The type of card. Set as: Mezzanine card or I/O board module.	
3	Port number	The port number.	
4	World Wide Port Name	The World Wide Name (WWN) of the device. An asterisk (*) is appended if the Optional Physical WWN has been changed from its initial value.	✓
5	World Wide Node Name	The World Wide Name (WWN) of the device. An asterisk (*) is appended if the Optional Physical WWN has been changed from its initial value.	✓

Items of information on the I/O slot expansion unit connected to the I/O adapter are described in the table below: per I/O adapter connected to the I/O slot expansion unit.

#	Item	Description	Edit
1	Part/Model Number	Part/Model number of the I/O slot expansion unit	-
2	Serial Number	Serial number of the I/O slot expansion unit	-

Items of information on the I/O slot expansion unit connected to the I/O adapter are described in the table below (per I/O adapter connected to the I/O slot expansion unit).

#	Item	Description	Edit
1	I/O adapter for I/O slot expansion units	Slot numbers of the I/O adapter on the I/O slot expansion unit.	-
2	Port number	-	-
3	World Wide Port	The World Wide Name (WWN)	✓

#	Item	Description	Edit
	Name	An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	
4	World Wide Node Name	WWN An asterisk (*) is appended if an Optional Physical WWN has been changed from its initial value.	✓

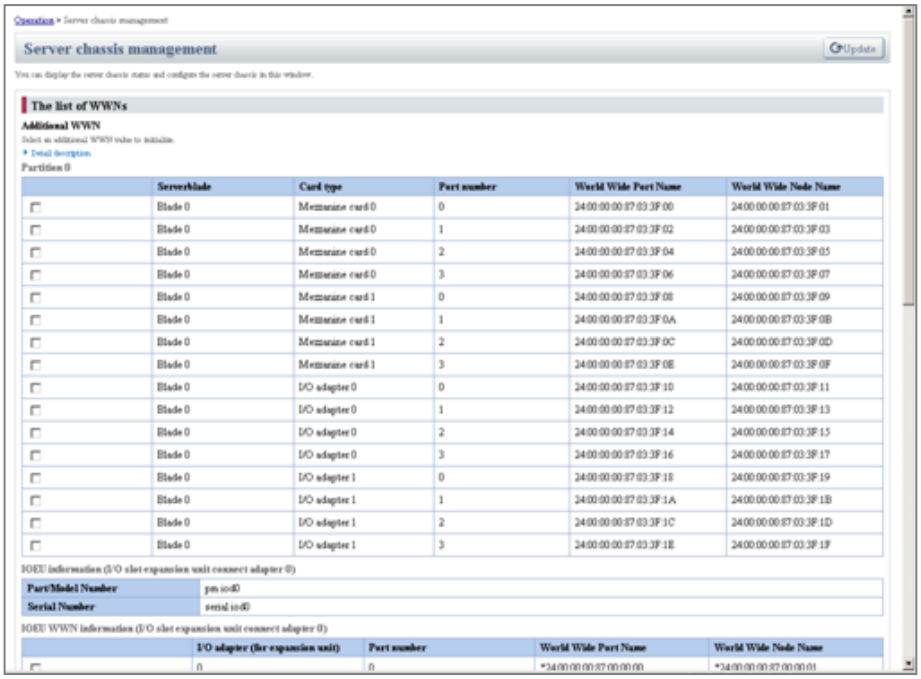
To edit Optional Physical WWNs of the I/O slot expansion unit, edit the World Wide Port name of port 0 of the I/O adapter 0 or 8 for I/O slot expansion units. This results in calculating and setting all Optional Physicals WWN of I/O adapter 0, 1, 4, 5 (or 8, 9, 12, 13) for I/O slot expansion units.

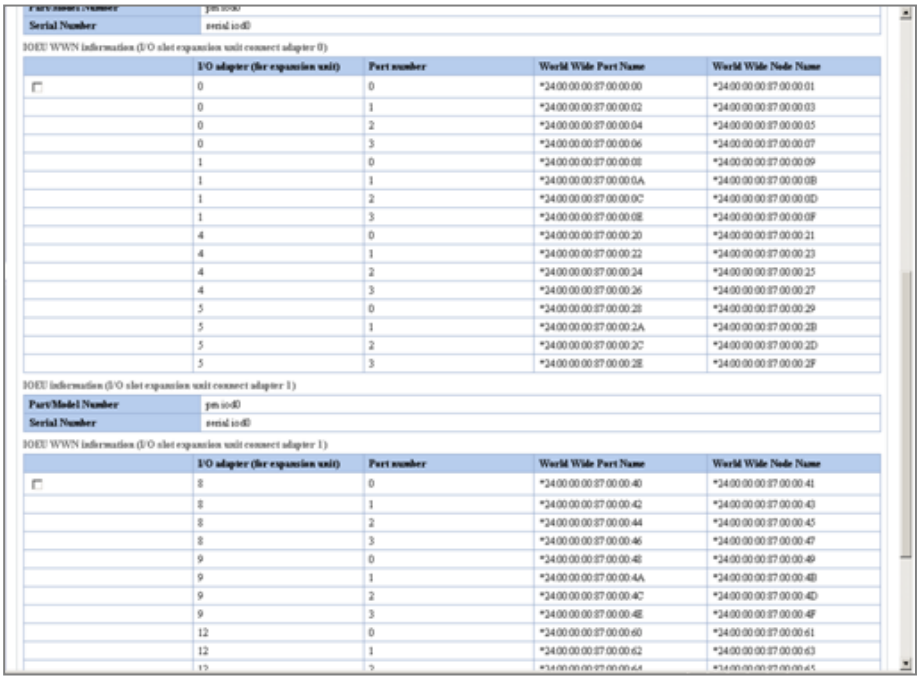
In the same way, edit the World Wide Port name of port 0 of the I/O adapter 2 or 10 for I/O slot expansion units. This results in calculating and setting all Optional Physical WWNs of I/O adapters 2, 3, 6, 7 (or 10, 11, 14, 15) for I/O slot expansion units.

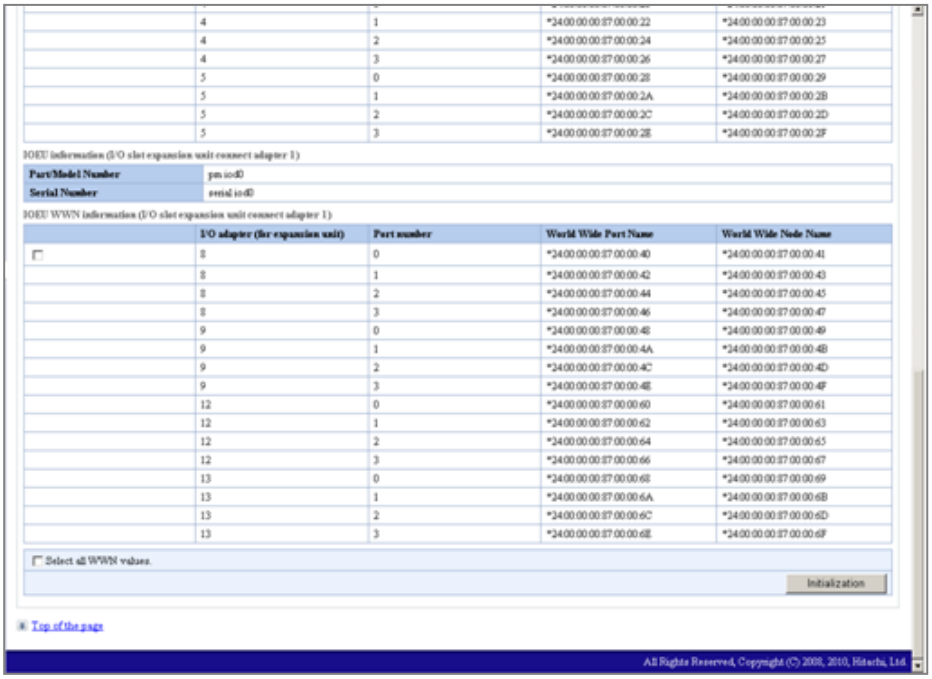
The operational button is described in the table below:

#	Item	Description	Edit
1	Initialization	Goes to the screen for initializing Optional Physical WWNs.	-

❑ Optional Physical WWN initialization view



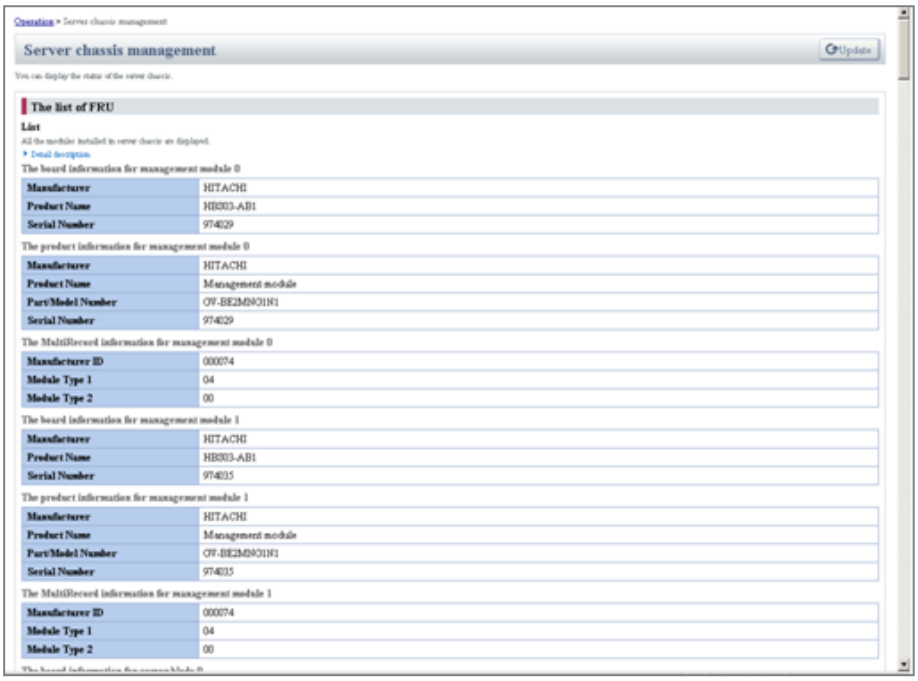


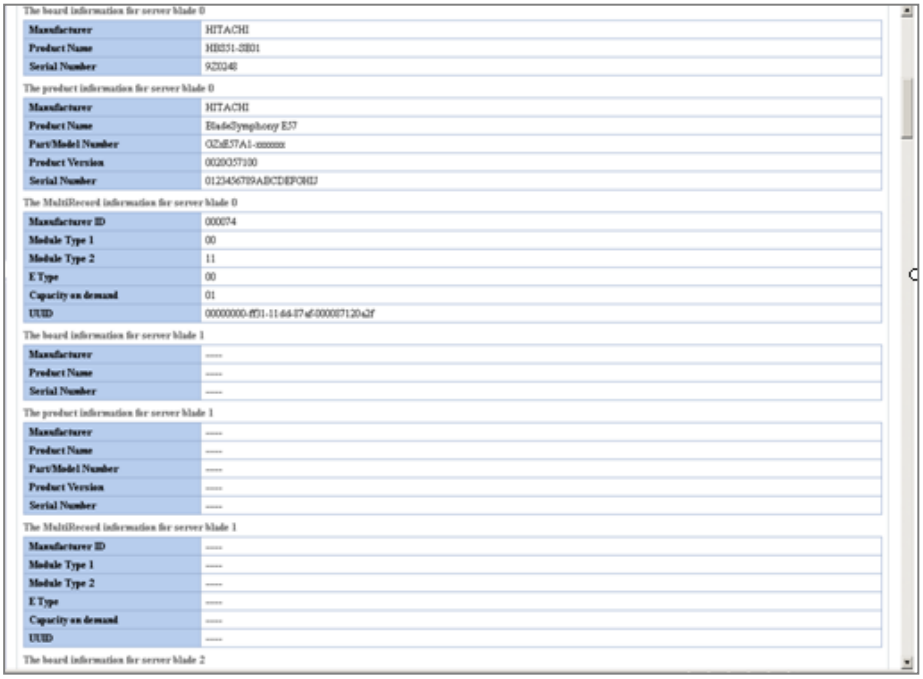


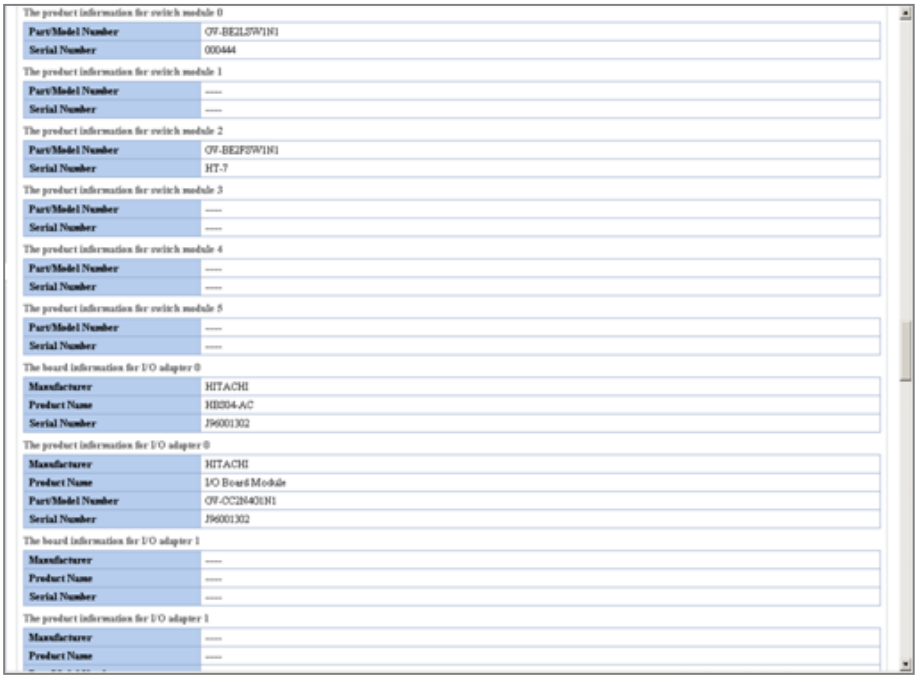
#	Item	Description
1	Initialization	Place a check mark in a check box of WWN to initialize, click **Initialization**, and then you can initialize the WWN. To edit Optional Physical WWNs of the I/O slot expansion unit, edit the World Wide Port name of port 0 of the I/O adapter 0 or 8 for I/O slot expansion units. This results in calculating and setting all Optional Physical WWN of I/O adapter 0, 1, 4, 5 (or 8, 9, 12, 13) for I/O slot expansion units. In the same way, edit the World Wide Port Name of port 0 of the I/O slot expansion units. Edit the World Wide Port name of port 0 of the I/O adapter 2 or 10 for I/O slot expansion units. This results in calculating and setting all Optional Physical WWNs of I/O adapters 2, 3, 6, 7 (or 10, 11, 14, 15) for I/O slot expansion units.

❑ FRU list view

Displays FRU information for all installed modules.







The product information for switch module 0

Part/Model Number	GW-BE2L2SW1N1
Serial Number	000444

The product information for switch module 1

Part/Model Number	----
Serial Number	----

The product information for switch module 2

Part/Model Number	GW-BE2F2SW1N1
Serial Number	HT-7

The product information for switch module 3

Part/Model Number	----
Serial Number	----

The product information for switch module 4

Part/Model Number	----
Serial Number	----

The product information for switch module 5

Part/Model Number	----
Serial Number	----

The board information for I/O adapter 0

Manufacturer	HITACHI
Product Name	HII304-AC
Serial Number	J96001302

The product information for I/O adapter 0

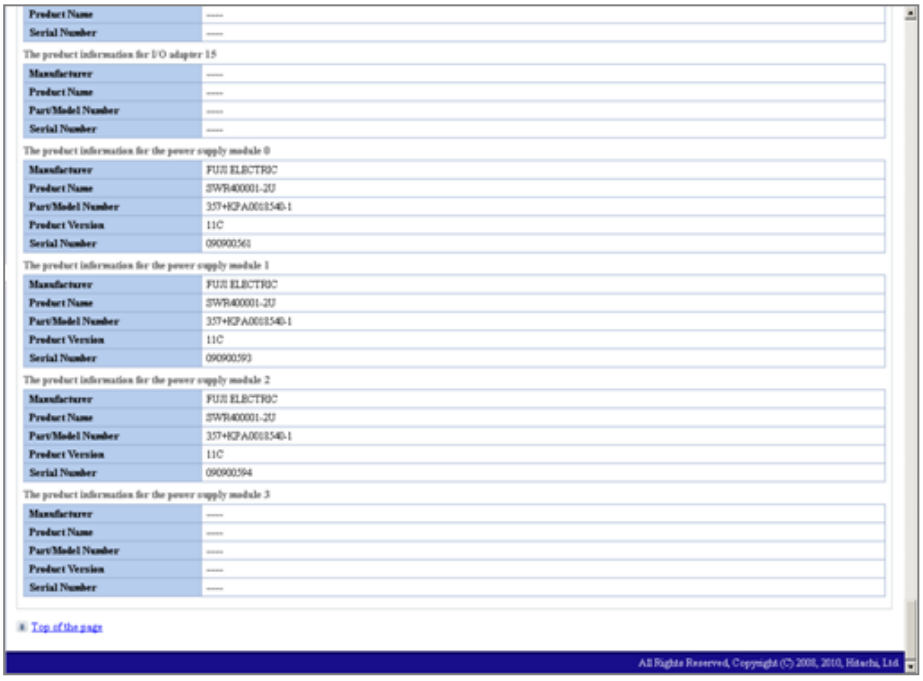
Manufacturer	HITACHI
Product Name	I/O Board Module
Part/Model Number	GW-CC2N401N1
Serial Number	J96001302

The board information for I/O adapter 1

Manufacturer	----
Product Name	----
Serial Number	----

The product information for I/O adapter 1

Manufacturer	----
Product Name	----



Product Name	----
Serial Number	----

The product information for I/O adapter 15

Manufacturer	----
Product Name	----
Part/Model Number	----
Serial Number	----

The product information for the power supply module 0

Manufacturer	FUJI ELECTRIC
Product Name	SWR400001-2U
Part/Model Number	357+KFA001854D-1
Product Version	11C
Serial Number	090900561

The product information for the power supply module 1

Manufacturer	FUJI ELECTRIC
Product Name	SWR400001-2U
Part/Model Number	357+KFA001854D-1
Product Version	11C
Serial Number	090900593

The product information for the power supply module 2

Manufacturer	FUJI ELECTRIC
Product Name	SWR400001-2U
Part/Model Number	357+KFA001854D-1
Product Version	11C
Serial Number	090900594

The product information for the power supply module 3

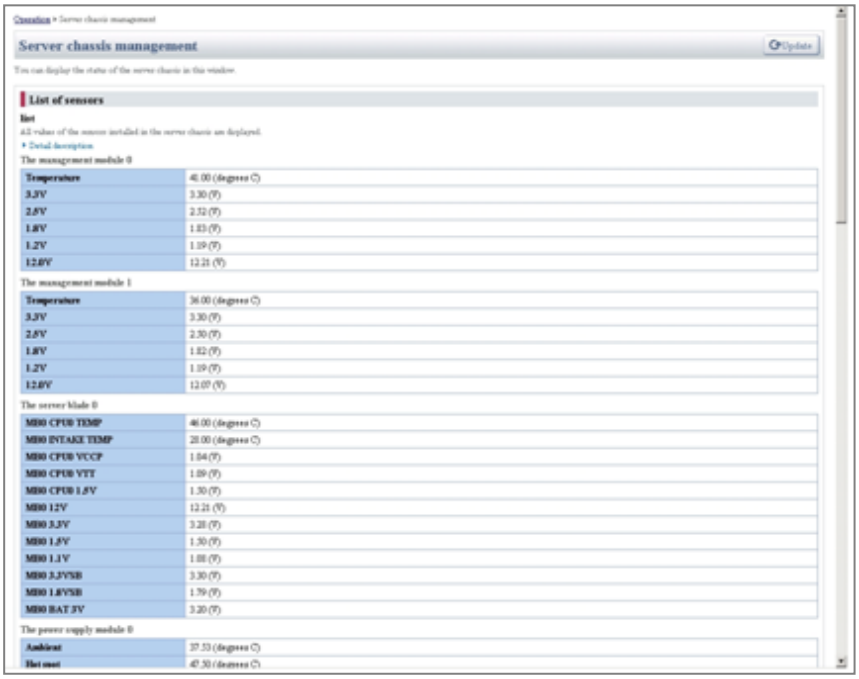
Manufacturer	----
Product Name	----
Part/Model Number	----
Product Version	----
Serial Number	----

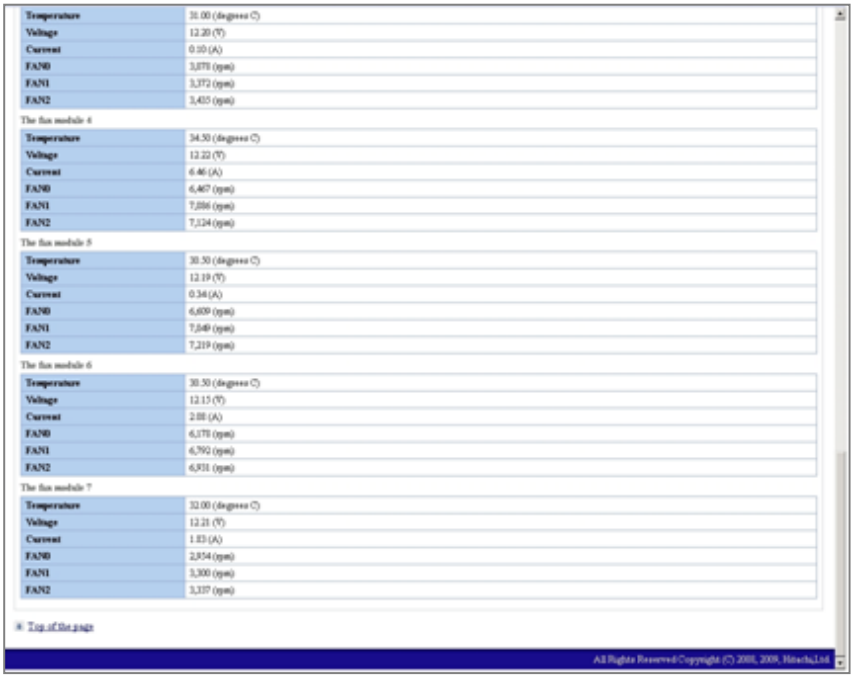
Top of the page

All Rights Reserved, Copyright (C) 2008, 2010, Hitachi, Ltd.

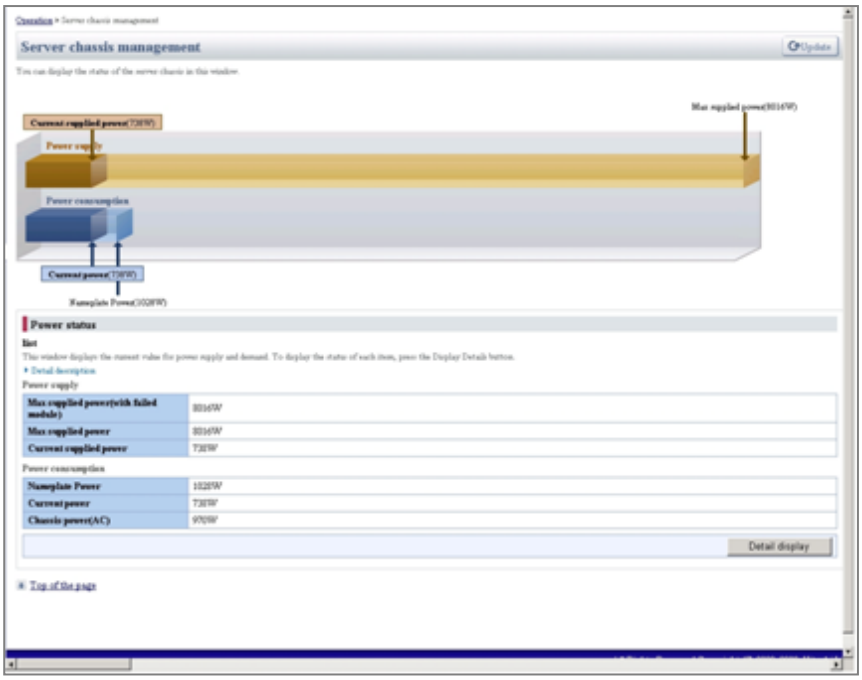
❑ Sensor list view

Displays sensor information for all installed modules.



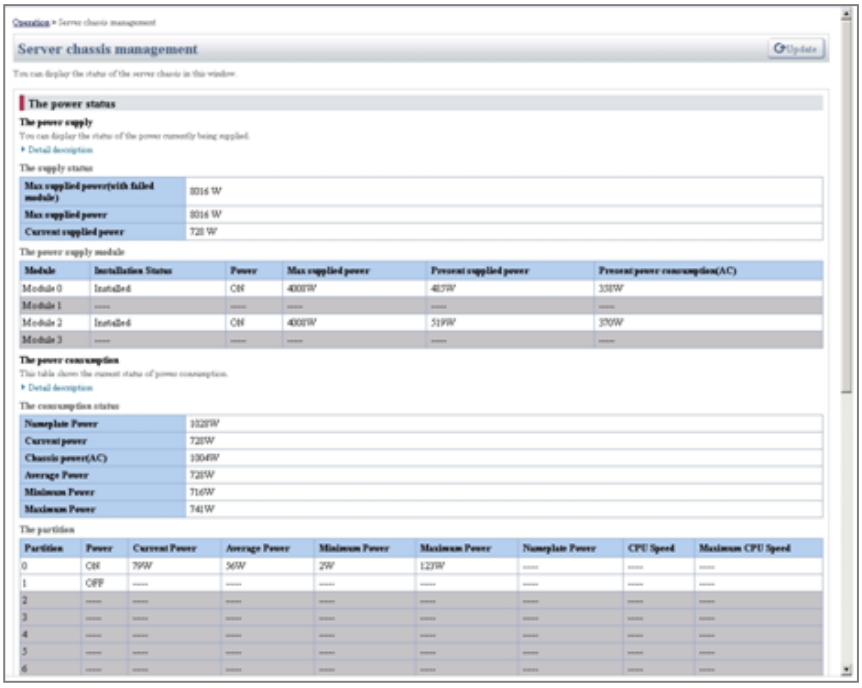


❑ Power status list view



#	Item	Description	Edit
1	Max supplied power (with failed module)	The maximum amount of power (in watts) able to be supplied by all installed power supply modules (including faulty modules). This item does not appear if no faulty modules are present.	
2	Max supplied power	The maximum amount of power (in watts) able to be supplied by all installed power supply modules (excluding faulty modules).	
3	Current power supply	The amount of power being supplied by all active power supply modules (in watts).	
4	Power consumption	The total rated power output of all installed power supply modules (in watts).	
5	Current power	The power consumption of all active modules (in watts).	
6	Chassis power (AC)	The power consumption of all active modules (in watts) converted to AC.	
7	Detail display	Takes you to the Details view.	

❑ Power status details view



Operation ▸ Server chassis management

Server chassis management

Update

You can display the status of the server chassis in this window.

The power status

The power supply

You can display the status of the power currently being supplied.

▸ Detail description

The supply status

Max supplied power(with failed module)	8016 W
Max supplied power	8016 W
Current supplied power	728 W

The power supply module

Module	Installation Status	Power	Max supplied power	Present supplied power	Present power consumption(AC)
Module 0	Installed	ON	4000W	487W	338W
Module 1	----	----	----	----	----
Module 2	Installed	ON	4000W	519W	370W
Module 3	----	----	----	----	----

The power consumption

This table shows the current status of power consumption.

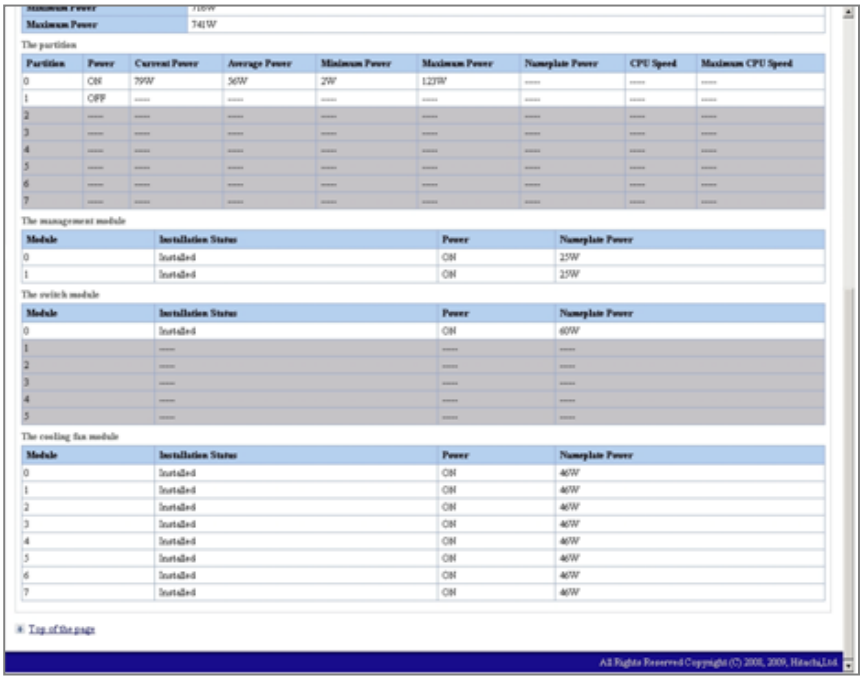
▸ Detail description

The consumption status

Nameplate Power	1028W
Current power	728W
Chassis power(AC)	1004W
Average Power	728W
Minimum Power	716W
Maximum Power	741W

The partition

Partition	Power	Current Power	Average Power	Minimum Power	Maximum Power	Nameplate Power	CPU Speed	Maximum CPU Speed
0	ON	79W	56W	29W	123W	----	----	----
1	OFF	----	----	----	----	----	----	----
2	----	----	----	----	----	----	----	----
3	----	----	----	----	----	----	----	----
4	----	----	----	----	----	----	----	----
5	----	----	----	----	----	----	----	----
6	----	----	----	----	----	----	----	----



Maximum Power 741W

The partition

Partition	Power	Current Power	Average Power	Minimum Power	Maximum Power	Nameplate Power	CPU Speed	Maximum CPU Speed
0	ON	79W	56W	29W	123W	----	----	----
1	OFF	----	----	----	----	----	----	----
2	----	----	----	----	----	----	----	----
3	----	----	----	----	----	----	----	----
4	----	----	----	----	----	----	----	----
5	----	----	----	----	----	----	----	----
6	----	----	----	----	----	----	----	----
7	----	----	----	----	----	----	----	----

The management module

Module	Installation Status	Power	Nameplate Power
0	Installed	ON	25W
1	Installed	ON	25W

The switch module

Module	Installation Status	Power	Nameplate Power
0	Installed	ON	60W
1	----	----	----
2	----	----	----
3	----	----	----
4	----	----	----
5	----	----	----

The cooling fan module

Module	Installation Status	Power	Nameplate Power
0	Installed	ON	46W
1	Installed	ON	46W
2	Installed	ON	46W
3	Installed	ON	46W
4	Installed	ON	46W
5	Installed	ON	46W
6	Installed	ON	46W
7	Installed	ON	46W

▸ Top of the page

All Rights Reserved Copyright (C) 2008, 2009, Hitachi,Ltd.

The supply status

#	Item	Description	Edit
1	Max supplied power (with failed module)	The maximum amount of power (in watts) able to be supplied by all installed power supply modules (including faulty modules). This item does not appear if no faulty modules are present.	
2	Max supplied power	The maximum amount of power (in watts) able to be supplied by all installed power supply modules (excluding faulty modules).	
3	Current power supply	The amount of power being supplied by all active power supply modules (in watts).	

The power supply modules

#	Item	Description	Edit
1	Module	The module number of the power supply module.	
2	Installation Status	The installation status of the power supply module.	
3	Power	The power status of the module. Set as: ON, Turning ON , OFF, or Turning OFF	
4	Max supplied power	The rated power output of the power supply module (in watts).	
5	Present supplied power	The current power consumption of the power supply module (in watts).	
6	Present power consumption (AC)	The current AC power consumption of the power supply module (in watts).	

The consumption status

#	Item	Description	Edit
1	Nameplate Power	The maximum rated power consumption of all installed modules (in watts).	
2	Current power	The power consumption of all active modules (in watts).	
3	Chassis power (AC)	The power consumption of all active modules (in watts) converted to AC.	
4	Average power	The mean power consumption over the past three minutes (in watts).	
5	Minimum power	The minimum power consumption over the past three minutes (in watts).	
6	Maximum power	The maximum power consumption over the past three minutes (in watts).	

The partition

#	Item	Description	Edit
1	Partition	The partition number of the physical partition.	
2	Power	The power status of the physical partition. Set as: ON or OFF	
3	Current Power	The current power consumption of the physical partition (in watts).	
4	Average Power	The mean power consumption over the past three minutes (in watts).	

#	Item	Description	Edit
5	Minimum Power	The minimum power consumption over the past three minutes (in watts).	
6	Maximum Power	The maximum power consumption over the past three minutes (in watts).	
7	Nameplate Power	The maximum rated power consumption of the server blade associated with the physical partition (in watts).	
8	CPU Speed	The current CPU frequency of the server blade associated with the physical partition (in MHz).	
9	Maximum CPU Speed	The maximum operating frequency of the CPU of the server blade associated with the physical partition (in MHz).	

Management module

#	Item	Description	Edit
1	Module	The module number of the module.	
2	Installation Status	The installation status of the management module.	
3	Power	The power status of the module. Set as: ON or OFF	
4	Nameplate Power	The power rating of the module (in watts).	

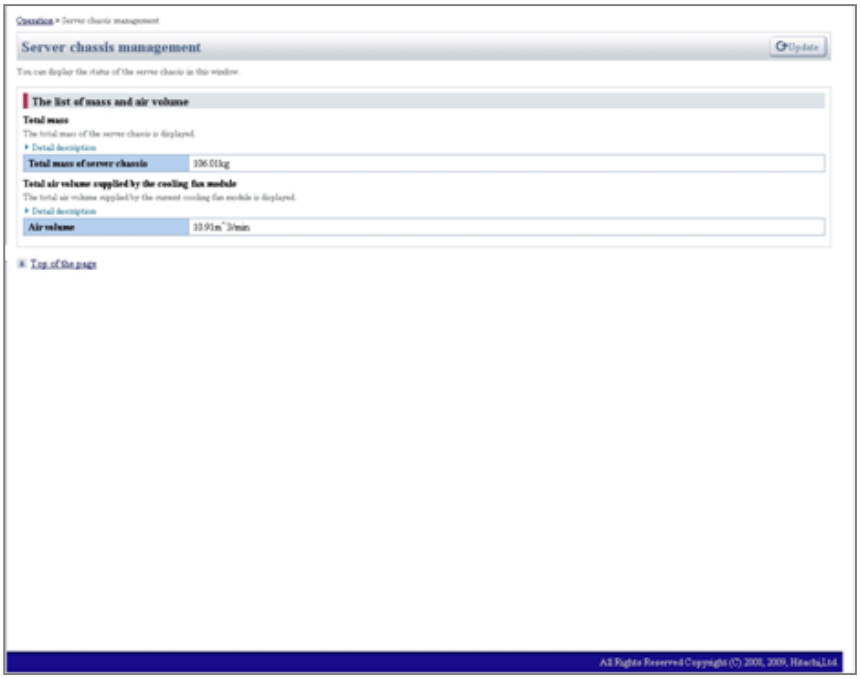
The switch module

#	Item	Description	Edit
1	Module	The module number of the module.	
2	Installation Status	The installation status of the switch module.	
3	Power	The power status of the module. Set as: ON or OFF	
4	Nameplate Power	The power rating of the module (in watts).	

The cooling fan module

#	Item	Description	Edit
1	Module	The module number of the module.	
2	Installation Status	The installation status of the fan module.	
3	Power	The power status of the module. Set as: ON or OFF	
4	Nameplate Power	The power rating of the module (in watts).	

❑ Mass and air flow list view



#	Item	Description	Edit
1	Total mass of server chassis	The total weight of the server chassis (in kg).	
2	Air volume	The total volume of air flow of all cooling fans in the server chassis (in m^3/min).	

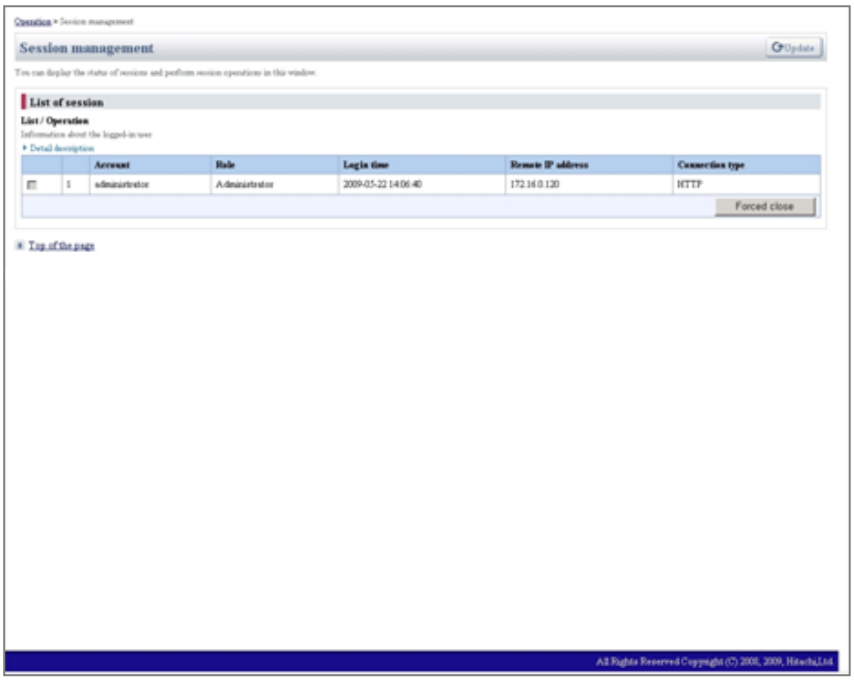
❑ Role-dependent variation in available operations

- To display and edit server chassis information, the user must have chassis permission.
- To execute a total shutdown of the chassis, the user must have chassis permission.
- To display the correspondence between physical partitions and I/O board modules, the user must have permission for all physical partitions.
- To display a full list of WWNs, the user must have chassis permission.
- To display the FRU information for all modules, the user must have chassis permission and permission for all switch modules.
- To display the sensor readings for all modules, the user must have chassis permission and permission for all switch modules.
- To display the power consumption status, the user must have chassis permission.
- To display the weight and air flow of the server chassis, the user must have chassis permission.

Session management

In the Session management view, you can display the status of active sessions, and perform associated tasks.

❑ Session list view



#	Item	Description	Edit
1	Account	The names of the user accounts currently connected to the management module.	
2	Role	The name of the role assigned to the user account.	
3	Login time	The time when the user logged in.	
4	Remote IP address	The IP address from which the user connected to the management module. No IP address is displayed for serial connections.	
5	Connection type	The protocol used to connect to the management module. Displayed as: Serial, Telnet, SSH, or HTTP	
6	Forced close	Forcibly terminates the sessions of users whose check boxes are selected.	

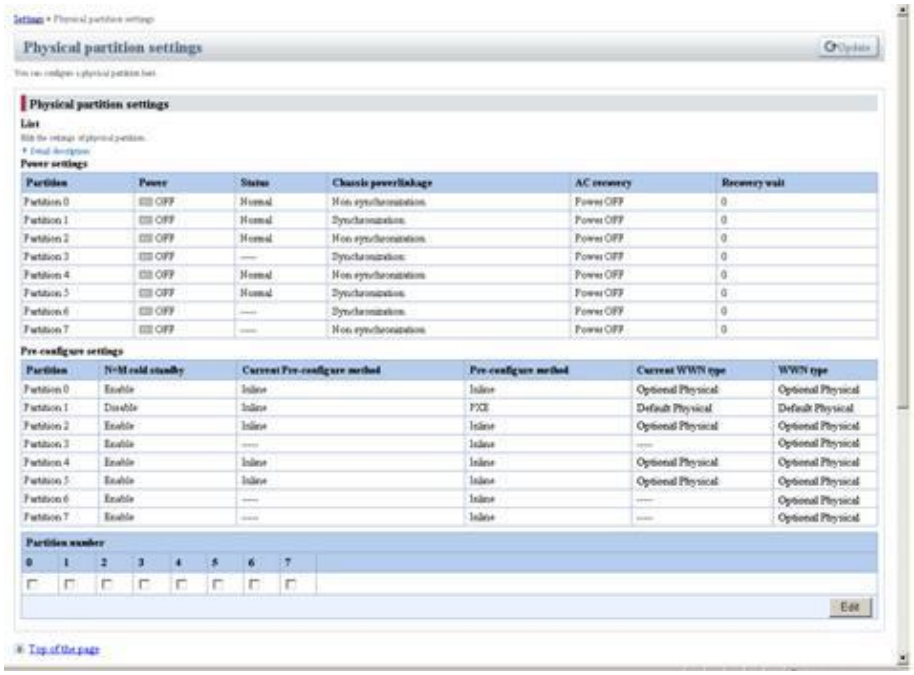
❑ Role-dependent variation in available operations

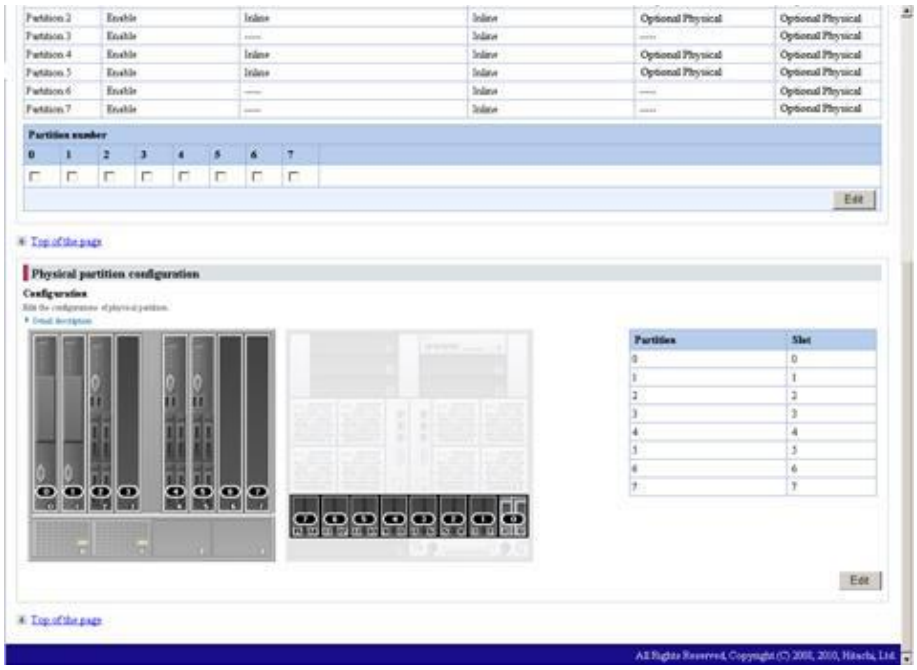
To display sessions and forcibly disconnect users, the user must have account permission.

Physical partition settings

In the Physical partition setup view, you can change the configuration and attributes of physical partitions

❑ Physical partition settings list view





Power setting items are described in the table below:

#	Item	Description	Edit
1	Partition	The physical partition number.	
2	Power	The power status of the physical partition. Set as: ON or OFF	
3	Status	The operating status of the physical partition. Set as: Normal, Init. Fail, Initializing, or Error	
4	Chassis powerlinkage	Indicates whether the operation of the power supply to the physical partition is linked to activation of the power supply of the server chassis. Set as: Link or Do not link	Yes
5	AC recovery	Indicates what behavior the physical partition power supply adopts when power is restored to the server chassis. Set as: Remain OFF, Turn ON, or Maintain status before power failure.	Yes
6	Recovery wait	Indicates how long the system waits before performing the action specified above. Set as: 0 to 60	Yes

Smart Configure setting items are described in the table below:

#	Item	Description	Edit
1	Partition	The physical partition number.	
2	N+M cold standby	Sets Enable or Disable.	Yes
3	Current Configuration method	The current Configuration method depends on the Smart Configure method settings and device configuration.	
4	Configuration method	Sets a Smart Configure method: PXE or Inline	Yes
5	Current WWN type	WWN type currently used	-
6	WWN type	Sets a WWN type to use: Original or Additional	Yes

Smart Configure setting item is described in the table below:

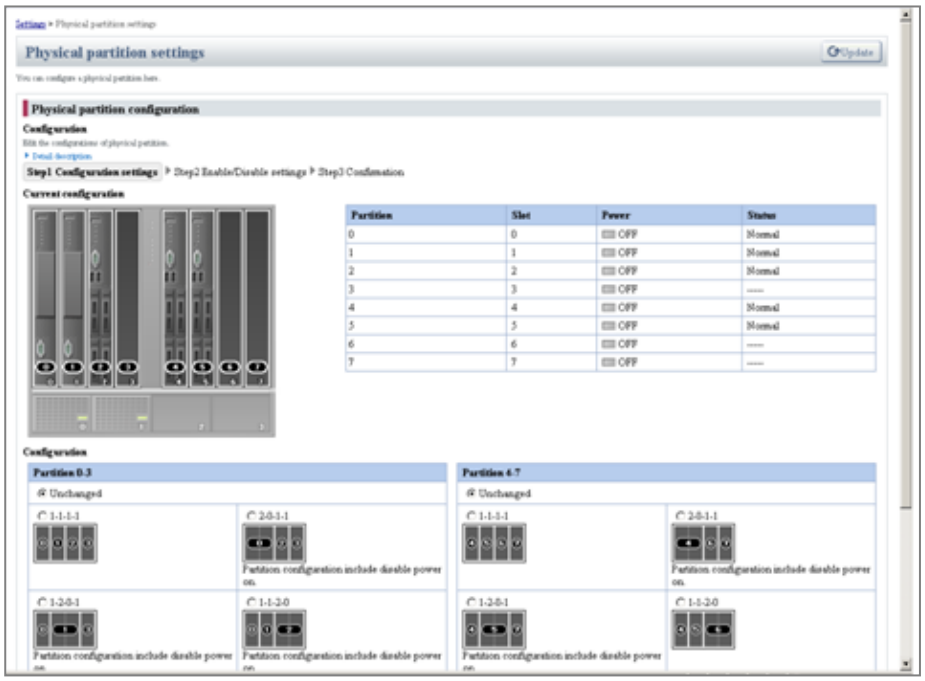
#	Item	Description	Edit
1	Edit	Goes to the editing screen of the physical partition whose check box is checked.	-

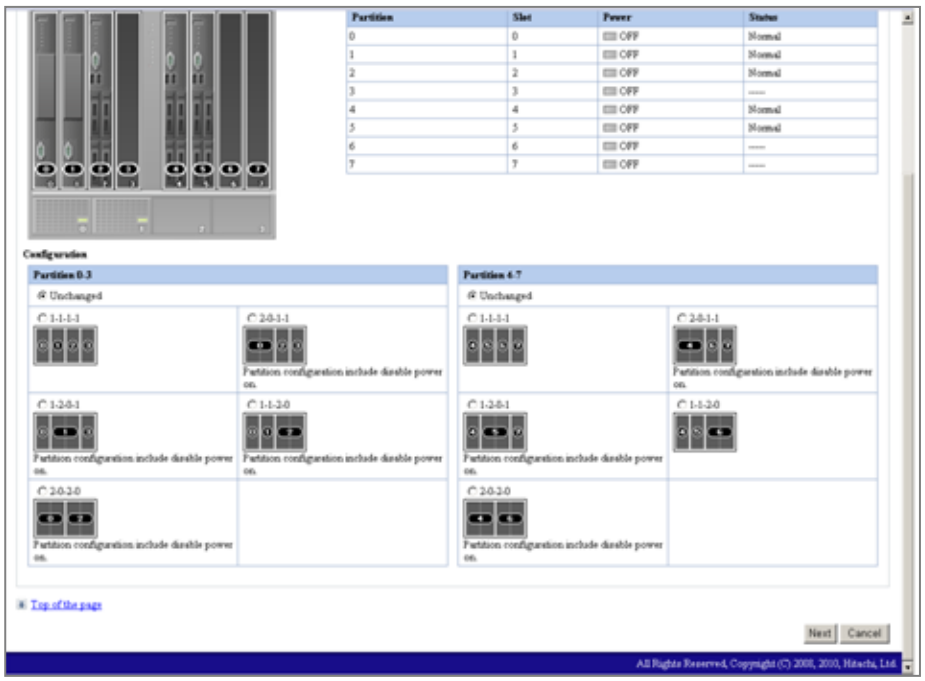
Physical partition configuration items are described in the table below:

#	Item	Description	Edit
1	Partition	The number of a physical partition	-
2	Slot number	The slot number belongs to a physical partition. “-------“ is shown to ineffective partitions.	-
3	Edit	Goes to the wizard to change physical partition configuration.	-

Change the configuration of the physical partition by following the steps below:

■ Step 1

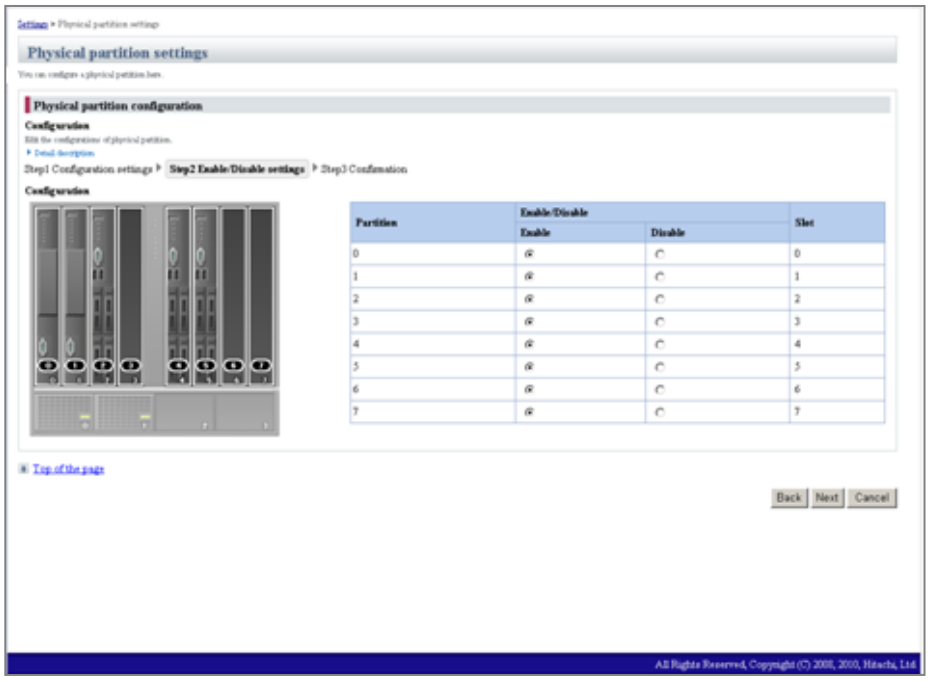




Select a new configuration for physical partition 0 to 3 and 4 to 7 using a radio button.

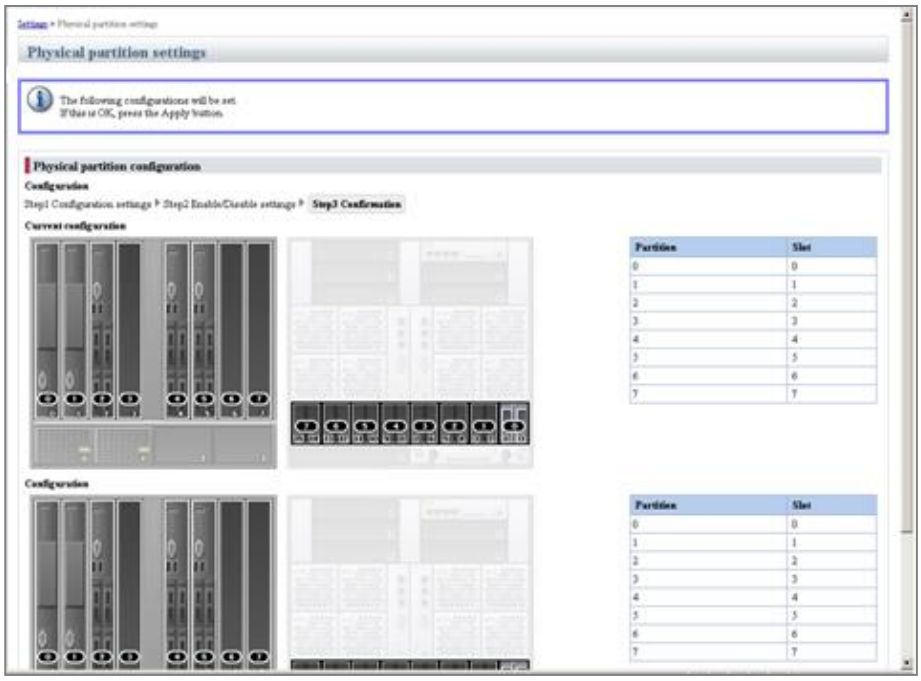
If any physical partition cannot be powered on in any configuration because no server blade or SMP connection board is installed, a message appears indicating that the partition cannot be powered on. You cannot change the configuration with partitions that have been power on.

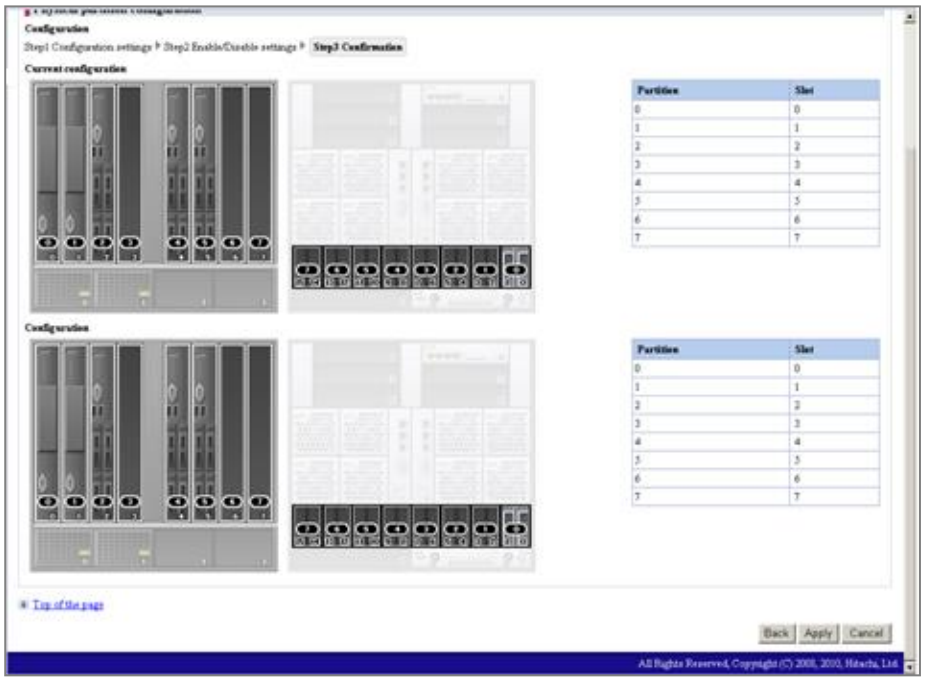
■ Step 2



In the physical partition configuration you select, enable or disable physical partitions.

■ Step 3





Check the physical partition configuration. Click **Apply** to apply the new configuration.

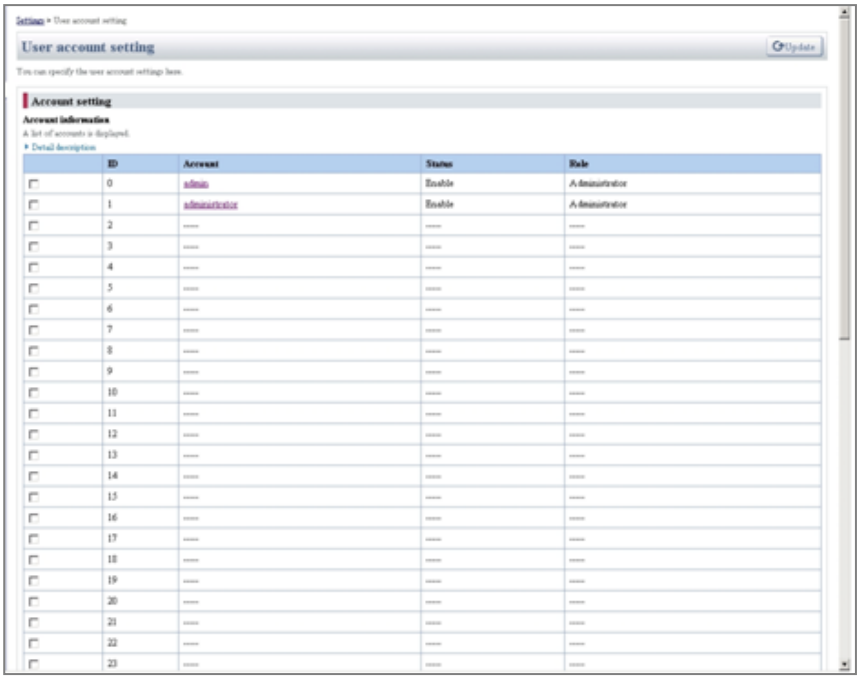
❑ Role-dependent variation in available operations

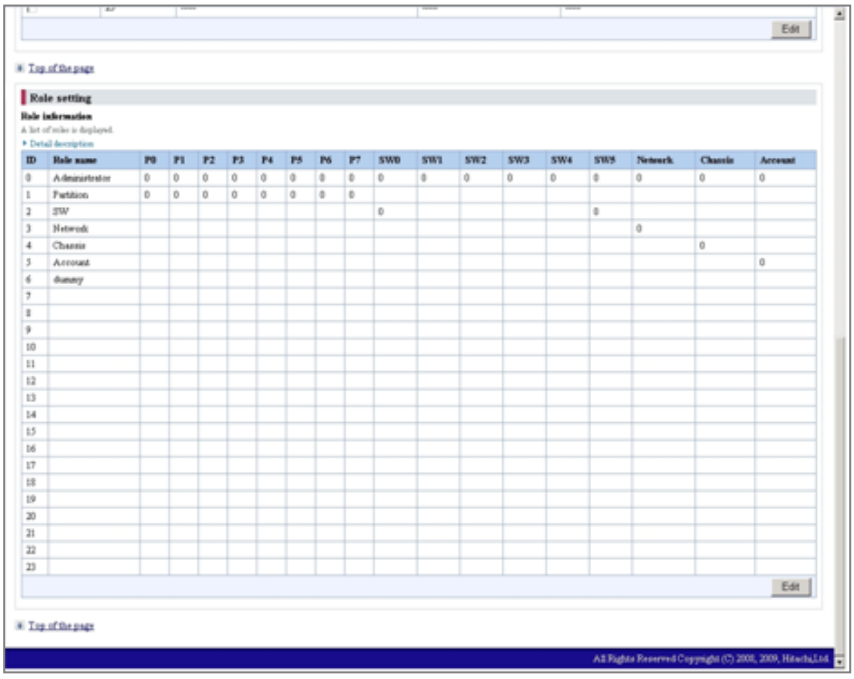
To edit a partition, the user must have partition permission for that partition.

User account settings

In the User account setup view, you can set up user accounts and roles.

❑ User account settings list view





User account

#	Item	Description	Edit
1	ID	The ID number of the account.	
2	Account name	The user account name. Account names can contain a maximum of 32 characters. The conventions for account names follows: First character: Alphabetic character Second and subsequent characters: Alphanumeric characters, hyphens (-), underscores (_), and periods (.).	
3	Status	Indicates whether the user account is enabled or disabled. Set as: Enabled or Disabled	
4	Role	The role assigned to the account.	
5	Edit	Takes you to the editing view for the user accounts whose check boxes are selected. In the editing view, you can edit the account name, status, and role, as well as the following settings: ・Text-based console type (system console or other) ・Prompt type ("SVP>" or the chassis ID) ・Inactivity timer (the period of inactivity after which a user is automatically logged out, from 1 to 1440 minutes) ・Login password In the editing view, you can also delete existing user accounts.	

Role

#	Item	Description	Edit
1	ID	The ID number of the role.	
2	Role name	The name of the role. Role names can contain a maximum of 15 characters. The conventions for role names are as follows: First character: Alphabetic character Second and subsequent characters: Alphanumeric characters, hyphens (-), underscores (_), and periods (.)	
3	P0 to P7, SW0 to SW5, Network, Chassis, Account	The permissions allocated to the role.	
4	Edit	Takes you to the editing view for the roles whose check boxes are selected. In the editing view, as well as changing the role name, you can set which permissions are assigned to a specific role ID. You can also delete an existing role by deleting the role name in the editing view.	

❑ Role-dependent variation in available operations

- To display and edit information for an account that is not the user's account, the user must have account permission.
- To display and edit roles, the user must have account permission.

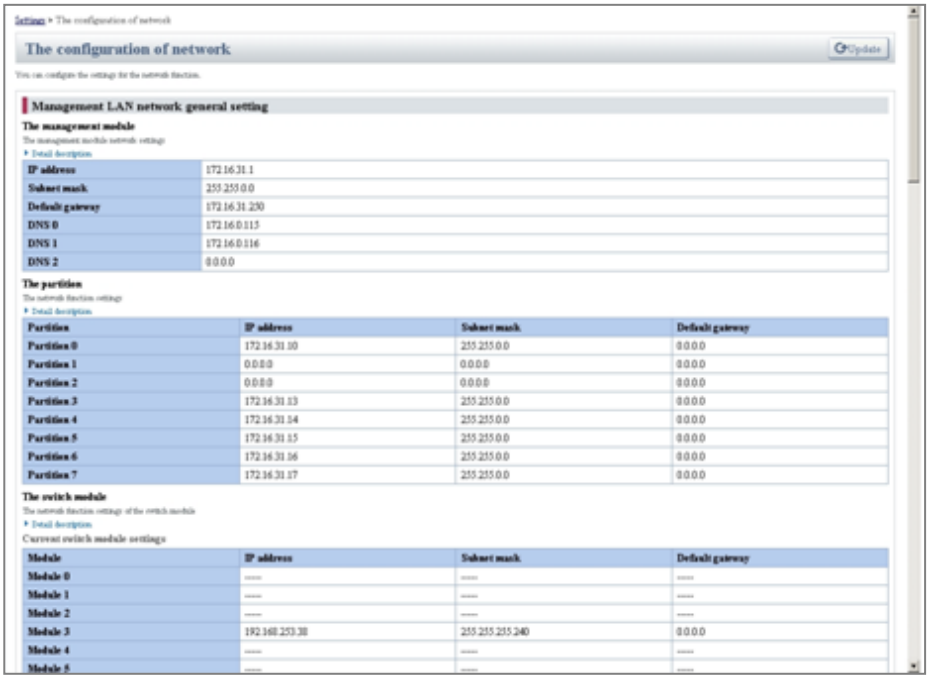
Configuration of network

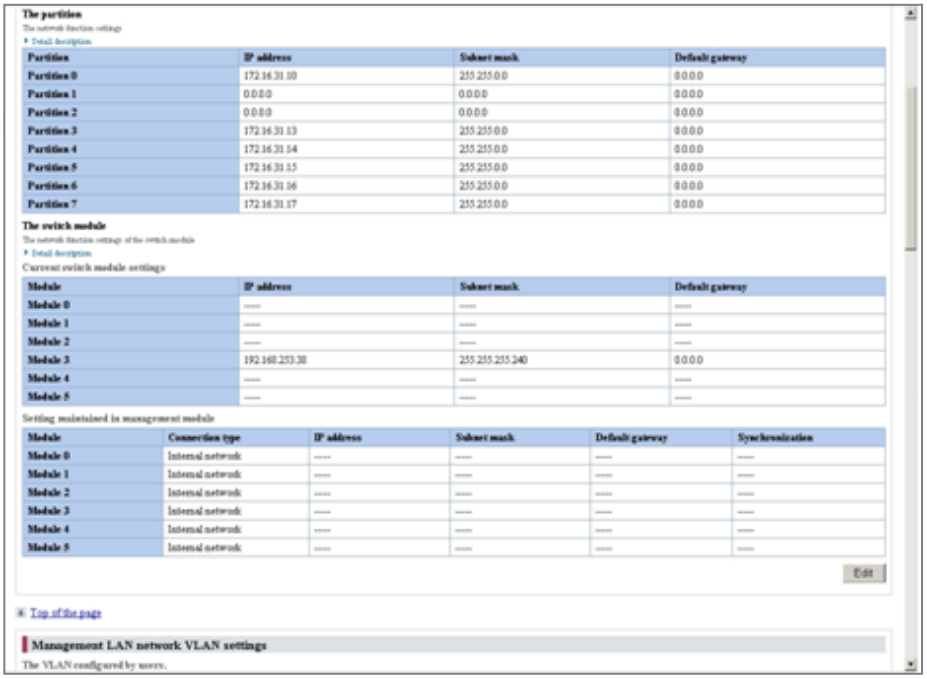
In the Network Setup view, you can view the status of the network and perform related settings.

Tip

- A VLAN ID can be deleted only under a condition that no module or physical partition belongs to the VLAN ID.
- Adding or deleting a VLAN ID and changing any module or physical partition cannot be executed at the same time.
- When changing a VLAN ID that has been set, delete all modules and physical partitions from the VLAN ID first, and then delete the VLAN ID. After confirming the deletion of the old VLAN ID, add a new VLAN ID in the VLAN setting screen.

❑ Network settings list view





The partition

The network function settings

▸ Detail description

Partition	IP address	Subnet mask	Default gateway
Partition 0	172.16.31.10	255.255.0.0	0.0.0.0
Partition 1	0.0.0.0	0.0.0.0	0.0.0.0
Partition 2	0.0.0.0	0.0.0.0	0.0.0.0
Partition 3	172.16.31.13	255.255.0.0	0.0.0.0
Partition 4	172.16.31.14	255.255.0.0	0.0.0.0
Partition 5	172.16.31.15	255.255.0.0	0.0.0.0
Partition 6	172.16.31.16	255.255.0.0	0.0.0.0
Partition 7	172.16.31.17	255.255.0.0	0.0.0.0

The switch module

The network function settings of the switch module

▸ Detail description

Current switch module settings

Module	IP address	Subnet mask	Default gateway
Module 0	----	----	----
Module 1	----	----	----
Module 2	----	----	----
Module 3	192.168.253.38	255.255.255.240	0.0.0.0
Module 4	----	----	----
Module 5	----	----	----

Setting maintained in management module

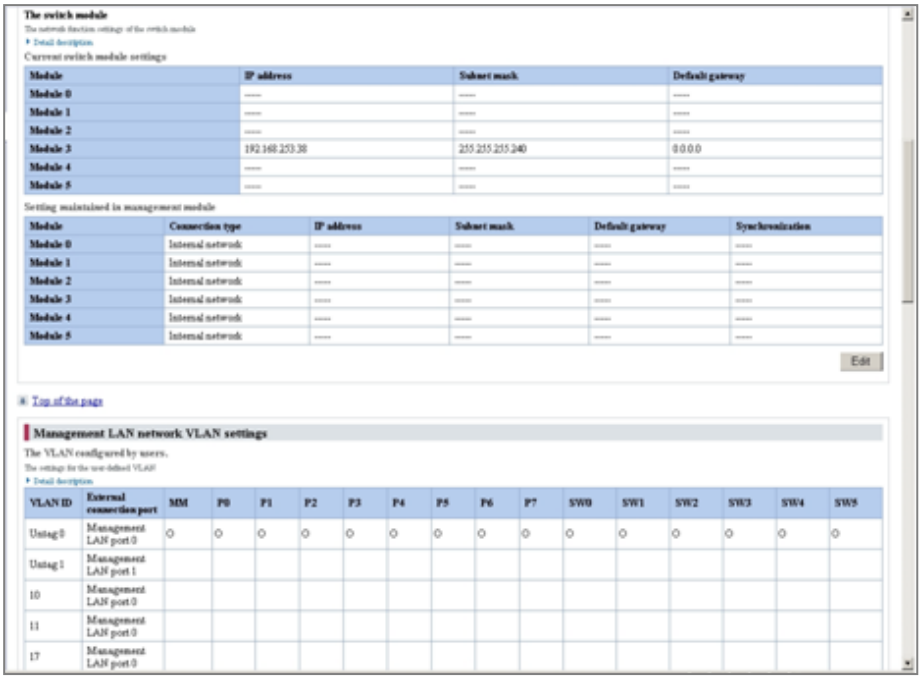
Module	Connection type	IP address	Subnet mask	Default gateway	Synchronization
Module 0	Internal network	----	----	----	----
Module 1	Internal network	----	----	----	----
Module 2	Internal network	----	----	----	----
Module 3	Internal network	----	----	----	----
Module 4	Internal network	----	----	----	----
Module 5	Internal network	----	----	----	----

Edit

Top of the page

Management LAN network VLAN settings

The VLAN configured by users.



The switch module

The network function settings of the switch module

▸ Detail description

Current switch module settings

Module	IP address	Subnet mask	Default gateway
Module 0	----	----	----
Module 1	----	----	----
Module 2	----	----	----
Module 3	192.168.253.38	255.255.255.240	0.0.0.0
Module 4	----	----	----
Module 5	----	----	----

Setting maintained in management module

Module	Connection type	IP address	Subnet mask	Default gateway	Synchronization
Module 0	Internal network	----	----	----	----
Module 1	Internal network	----	----	----	----
Module 2	Internal network	----	----	----	----
Module 3	Internal network	----	----	----	----
Module 4	Internal network	----	----	----	----
Module 5	Internal network	----	----	----	----

Edit

Top of the page

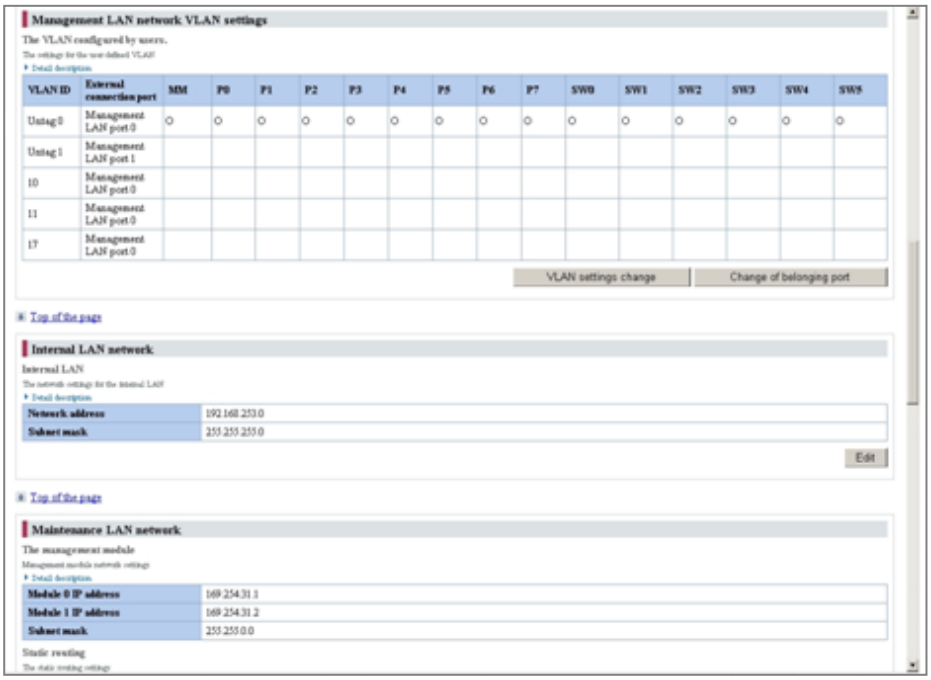
Management LAN network VLAN settings

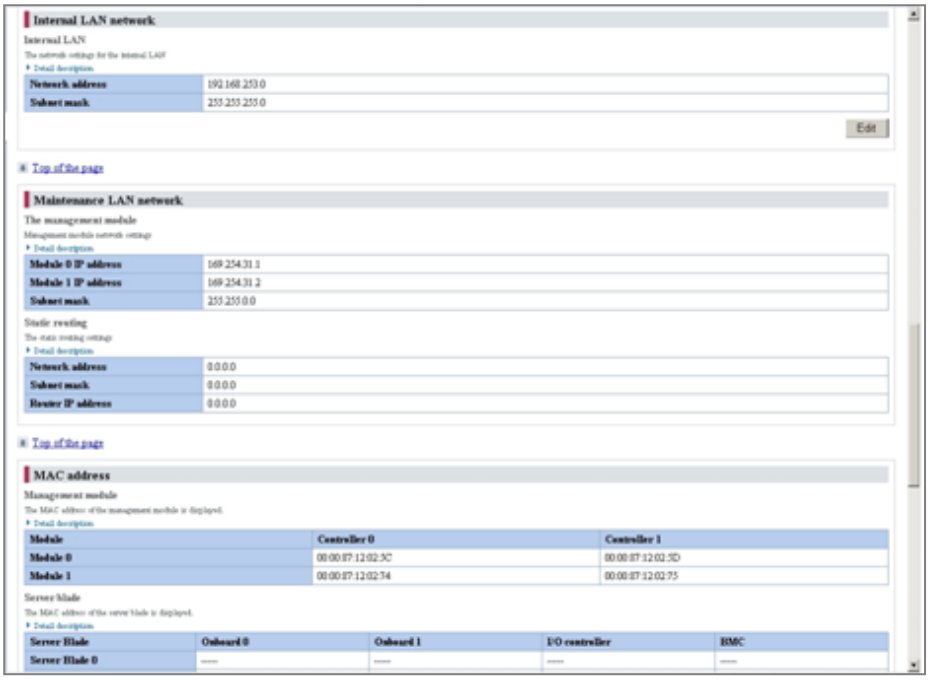
The VLAN configured by users.

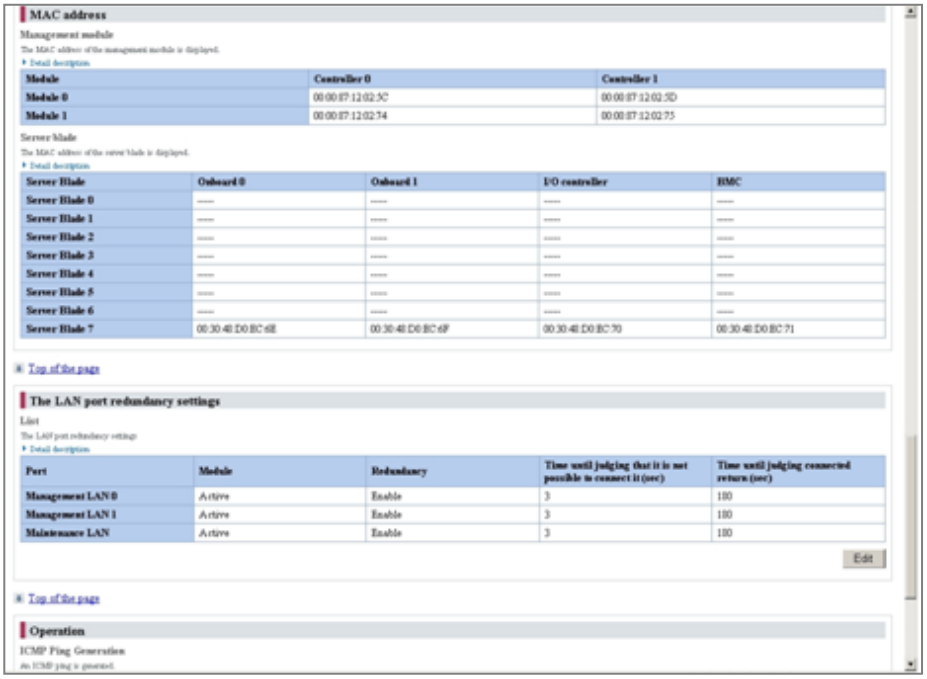
The settings for the user-defined VLAN

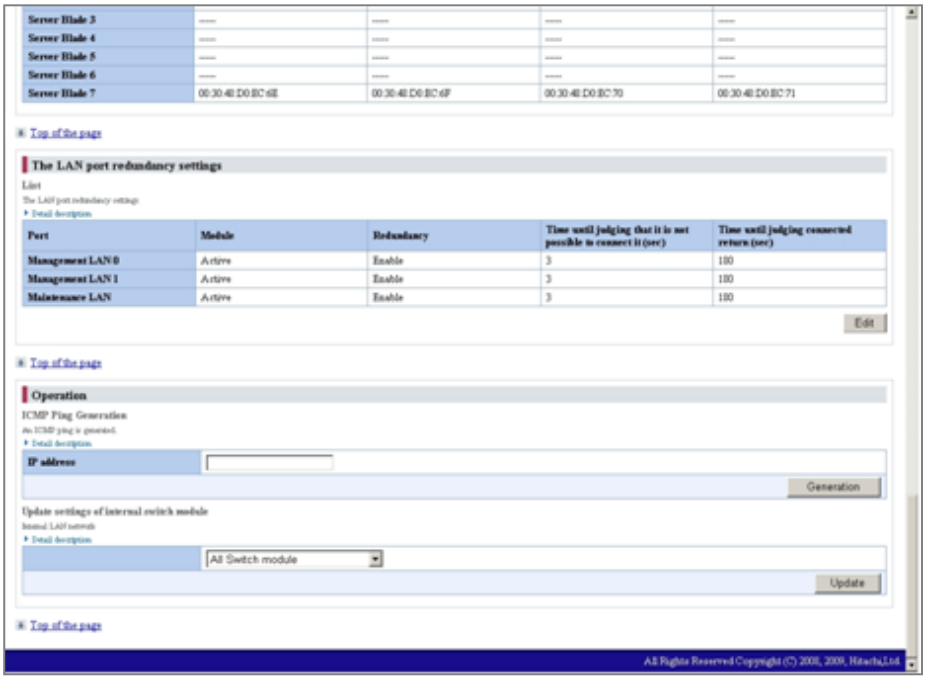
▸ Detail description

VLAN ID	External connection port	MM	P0	P1	P2	P3	P4	P5	P6	P7	SW0	SW1	SW2	SW3	SW4	SW5
Untag 0	Management LAN port 0	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untag 1	Management LAN port 1															
10	Management LAN port 0															
11	Management LAN port 0															
17	Management LAN port 0															


Management LAN network VLAN settings
The VLAN configured by users.
Detail description
VLAN ID
External connection port
MM
P0
P1
P2
P3
P4
P5
P6
P7
SW0
SW1
SW2
SW3
SW4
SW5
Untag 0
Management LAN port 0
Untag 1
Management LAN port 1
10
11
17
VLAN settings change
Change of belonging port
Top of the page
Internal LAN network
Internal LAN
Detail description
Network address
192.168.253.0
Subnet mask
255.255.255.0
Edit
Top of the page
Maintenance LAN network
The management module
Detail description
Module 0 IP address
169.254.31.1
Module 1 IP address
169.254.31.2
Subnet mask
255.255.0.0
Static routing


Internal LAN network
Internal LAN
Detail description
Network address
192.168.253.0
Subnet mask
255.255.255.0
Edit
Top of the page
Maintenance LAN network
The management module
Detail description
Module 0 IP address
169.254.31.1
Module 1 IP address
169.254.31.2
Subnet mask
255.255.0.0
Static routing
Detail description
Network address
0.0.0.0
Subnet mask
0.0.0.0
Router IP address
0.0.0.0
Top of the page
MAC address
Management module
Detail description
Module
Controller 0
Controller 1
Module 0
00:00:87:12:02:5C
00:00:87:12:02:5D
Module 1
00:00:87:12:02:74
00:00:87:12:02:75
Server blade
Detail description
Server Blade
Onboard 0
Onboard 1
I/O controller
BMC
Server Blade 0


MAC address
Management module
Module
Controller 0
Controller 1
Module 0
00:00:87:12:02:5C
00:00:87:12:02:5D
Module 1
00:00:87:12:02:74
00:00:87:12:02:75
Server blade
Server Blade
Onboard 0
Onboard 1
I/O controller
BMC
Server Blade 0
Server Blade 1
Server Blade 2
Server Blade 3
Server Blade 4
Server Blade 5
Server Blade 6
Server Blade 7
00:30:48:D0:EC:6E
00:30:48:D0:EC:6F
00:30:48:D0:EC:70
00:30:48:D0:EC:71
Top of the page
The LAN port redundancy settings
List
Port
Module
Redundancy
Time until judging that it is not possible to connect it (sec)
Time until judging connected return (sec)
Management LAN 0
Management LAN 1
Maintenance LAN
Active
Enable
3
180
Edit
Top of the page
Operation
ICMP Ping Generation


Server Blade 3
Server Blade 4
Server Blade 5
Server Blade 6
Server Blade 7
00:30:48:D0:EC:6E
00:30:48:D0:EC:6F
00:30:48:D0:EC:70
00:30:48:D0:EC:71
Top of the page
The LAN port redundancy settings
List
Port
Module
Redundancy
Time until judging that it is not possible to connect it (sec)
Time until judging connected return (sec)
Management LAN 0
Management LAN 1
Maintenance LAN
Active
Enable
3
180
Edit
Top of the page
Operation
ICMP Ping Generation
IP address
Generation
Update settings of internal switch module
All Switch module
Update
Top of the page
All Rights Reserved Copyright (C) 2008, 2009, Hitachi,Ltd.

The management module

#	Item	Description	Edit
1	IP address	The IP address of the management module.	Yes
2	Subnet mask	The subnet mask of the management module.	Yes
3	Default gateway	The default gateway of the management module.	Yes
4	DNS0 to DNS2	The DNS settings of the management module. These settings appear as IP addresses.	Yes

The partition

#	Item	Description	Edit
1	Partition	The partition number of the physical partition.	
2	IP address	The IP address of the physical partition.	Yes
3	Subnet mask	The subnet mask of the physical partition.	Yes
4	Default gateway	The default gateway of the physical partition.	Yes

The current switch module settings

#	Item	Description	Edit
1	Module	The module number.	-
2	IP address	IP address of the management interface in the switch module	-
3	Subnet mask	Subnet mask of the management interface in the switch module	-
4	Default gateway	Default gateway of the management interface in the switch module	-

The settings held by the management module

#	Item	Description	Edit
1	Module	The module number.	-
2	Connection type	Destination to which the switch module connected to. Can connect to the management LAN network, internal LAN network, or a port in the switch module.	Yes
3	IP address	IP address of the management interface in the switch module. Asterisk (*) is displayed when the switch module does not support the interface to view/update “Management interface LAN setting”.	Yes
4	Subnet mask	Subnet mask of the management interface in the switch module.	Yes
5	Default gateway	Default gateway of the management interface in the switch module.	Yes
6	Synchronization	Displays whether or not to apply the management module setting to the switch module. Yes: Currently the management module and switch module have the same setting. When synchronization is executed, the management module setting will be applied to the switch module. Yes!: Currently the management module and switch module have the different settings. When synchronization	Yes

#	Item	Description	Edit
		is executed, the management module setting will be applied to the switch module. No: Synchronization cannot be executed.	



When Network OS version 3.0.0 is on a Brocade 10 Gb DCB switch module, the default gateway setting from the management module does not take effect on the switch module. Log in to the switch module and configure it using the ip route command. See the *Network OS Administrator's Guide* for details. If Network OS version 2.0.1 is on the switch module, you cannot configure the gateway.

The VLAN configured by users

#	Item	Description	Edit
1	VLAN ID	The LAN ID. Set as: 2 to 4000 You can delete a VLAN by deleting its VLAN ID.	Yes
2	External connection port	The external connection port used by the VLAN. You can select Management LAN port 0 or Management LAN port 1.	Yes
3	MM, P0 to P7, SW0 to SW5	Indicates which user-defined VLAN is associated with each module and physical partition.	Yes

Internal LAN network

#	Item	Description	Edit
1	Network address	The network address of the internal LAN network: Changing internal LAN network addresses makes the management module restart. Do not set the internal network address to 192.168.0.0 or 192.168.254.0.	Yes
2	Subnet mask	The subnet mask of the internal LAN network. Fixed at 255.255.255.0.	



Do not change the internal network address while the server blade works. If you do, failure error events, which have occurred while the management module is restarting, may not be detected.
When changing the address while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

MAC address

#	Item	Description	Edit
1	Module	The module number.	
2	Controller 0	The MAC address of controller 0.	

#	Item	Description	Edit
3	Controller 1	The MAC address of controller 1.	
4	Server blade	The server blade number.	
5	On-board 0	The MAC address of the on-board NIC 0.	
6	On-board 1	The MAC address of the on-board NIC 1.	
7	I/O controller	The MAC address of the I/O controller.	
8	BMC	The MAC address of the BMC.	

Maintenance LAN network

#	Item	Description	Edit
1	Module 0 IP address	The IP address of management module 0 in the maintenance LAN network.	
2	Module 1 IP address	The IP address of management module 1 in the maintenance LAN network.	
3	Subnet mask	The subnet mask in the maintenance LAN network.	
4	Network address	The destination network address for static routing.	
5	Subnet mask	The subnet mask associated with the above network address.	
6	Router IP address	The IP address of the router responsible for static routing.	

The LAN port redundancy settings

#	Item	Description	Edit
1	Port	The LAN port of the management module.	
2	Module	Indicates whether the active or standby module is connecting to the network. Set as: Active or Standby	
3	Redundancy	Indicates whether LAN redundancy is enabled. Set as: Enabled or Disabled	Yes
4	Time until judging that is not possible to connect (sec)	The length of time that must elapse before a LAN link is considered to be down. A value from 1 to 3600 (in seconds)	Yes
5	Time until judging connected return (sec)	The length of time that must elapse before a LAN link is considered to be up. A value from 1 to 3600 (in seconds).	Yes

ICMP Ping Generation

#	Item	Description	Edit
1	Generation	Issues an ICMP Ping request to the specified IP address.	

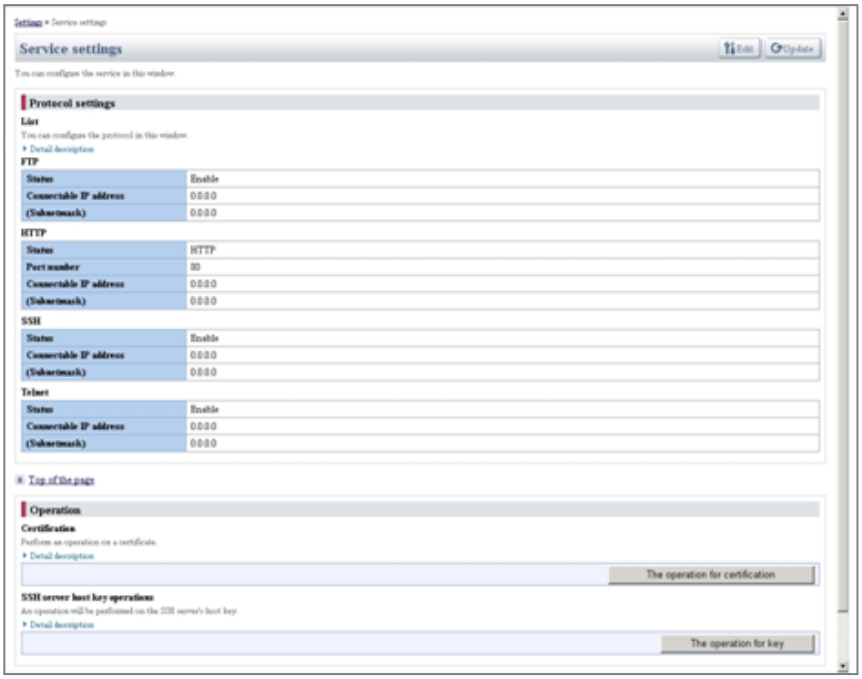
❑ Role-dependent variation in available operations

To display network settings, the user must have network permission.

Service settings

In the Service setup view, you can configure a range of network protocols and perform tasks related to public keys.

❑ Service settings list view



FTP

#	Item	Description	Edit
1	Status	Indicates whether connections that use the FTP protocol are permitted. Set as: Enabled or Disabled	Yes
2	Connectable IP address	When FTP connections are permitted, the network address from which to allow connections.	Yes
3	(Subnet mask)	The subnet mask of the network address.	Yes

HTTP

#	Item	Description	Edit
1	Status	Indicates whether connections that use the HTTP protocol are permitted. Set as: HTTP, HTTPS, or Disabled	Yes
2	Port number	The port number used for the HTTP protocol. Set as: 1 to 65535	Yes
3	Connectable IP address	When HTTP connections are permitted, the network address from which to allow connections.	Yes
4	(Subnet mask)	The subnet mask of the network address.	Yes

SSH settings

#	Item	Description	Edit
1	Status	Indicates whether connections that use the SSH protocol are permitted. Set as: Enabled or Disabled	Yes
2	Permitted network address	When SSH connections are permitted, the network address from which to allow connections.	Yes
3	(Subnet mask)	The subnet mask of the network address.	Yes

Telnet

#	Item	Description	Edit
1	Status	Indicates whether connections that use the Telnet protocol are permitted. Set as: Enabled or Disabled	Yes
2	Connectable IP address	When Telnet connections are permitted, the network address from which to allow connections.	Yes
3	(Subnet mask)	The subnet mask of the network address.	Yes

Certification

#	Item	Description	Edit
1	The operation for certification	Takes you to the Certificate Operations page.	

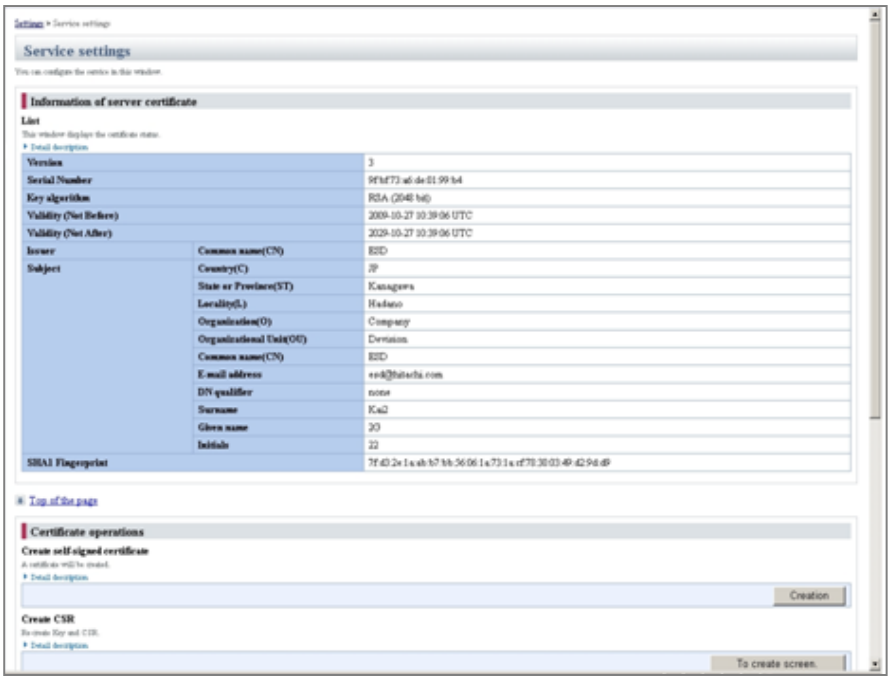
SSH server host key operations

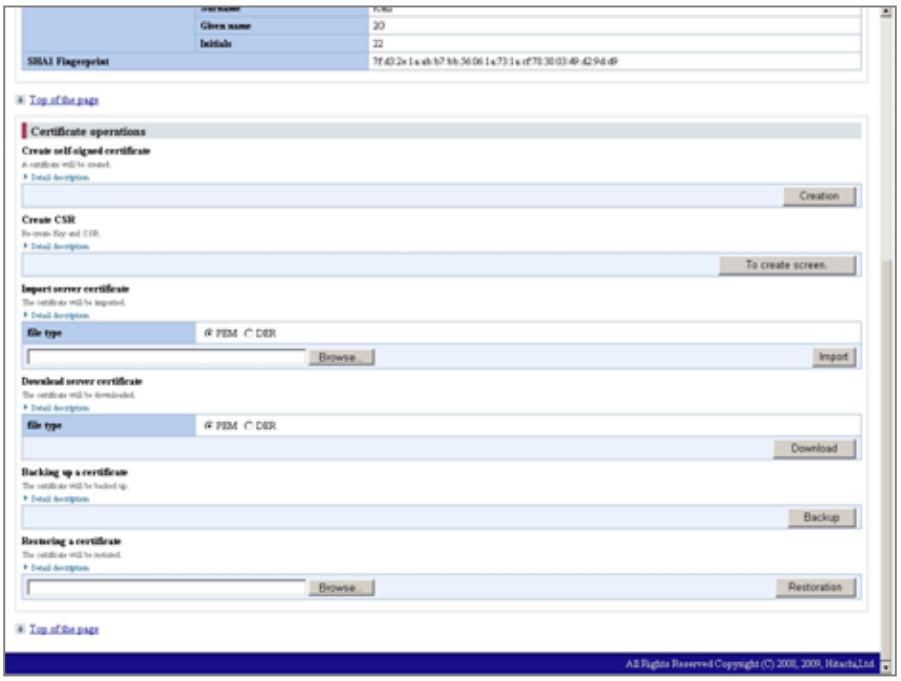
#	Item	Description	Edit
1	The operation for key	Takes you to the SSH Server Host Key Operations page.	



Communication via HTTPS is available in Microsoft® Internet Explorer 7.0.

❑ Certificate operations view





Information

#	Item		Description	Edit
1	Version		Version of the server certificate	-
2	Serial number		Serial number of the server certificate	-
3	Key algorithm/length		Key algorithm and length of the server certificate	-
4	Validity (Not Before)		Starting date of validity for the server certificate	-
5	Validity (Not After)		Ending date of the validity for the server certificate	-
6	Issuer	Common	Common name that has issued the server	

#	Item		Description	Edit
		name (CN)	certificate	
7	Subject	Country (C)	Country name the server certificate is issued for	-
		State or Provinces (ST)	State or province name the server certificate is issued for	-
		Locality (L)	City or area name the server certificate is issued for	-
		Organization (O)	Organization name the server certificate is issued for	-
		Organizational Unit (OU)	Department or section name of the organization the server certificate is issued for	-
		Common name (CN)	Common name the server certificate is issued for	-
		E-mail address	E-mail address the server certificate is issued for	-
		DN qualifier	DN qualifier the server certificate is issued for	-
		Surname	Surname the server certificate is issued for	-
		Given name	Given name the server certificate is issued for	-
		Initials	Initial the server certificate is issued for	-
8	SHA1 Fingerprint		Fingerprint the server certificate is issued for	-

Creating a self-signed certificate

#	Item	Description	Edit
1	Creation	Goes to the screen to create a self-signed certificate. For how to create it, see “Digital Certificate for the System Web console” in Chapter 13.	-

Creating a CSR

#	Item	Description	Edit
1	Creation	Goes to the screen to create a CSR certificate. For how to create it, see “Digital Certificate for the System Web console” in Chapter 13.	-

Importing a server certificate

#	Item	Description	Edit
1	Import	Imports a signed server certificate issued for the CSR. Specify the file type and file name. When you import a server certificate, consistency check with the key at the CSR creation is executed. Importing is available when both are the same.	-

Downloading a server certificate

#	Item	Description	Edit
1	Download	Downloads the server certificate currently used on the system web console. Specify a file type.	-

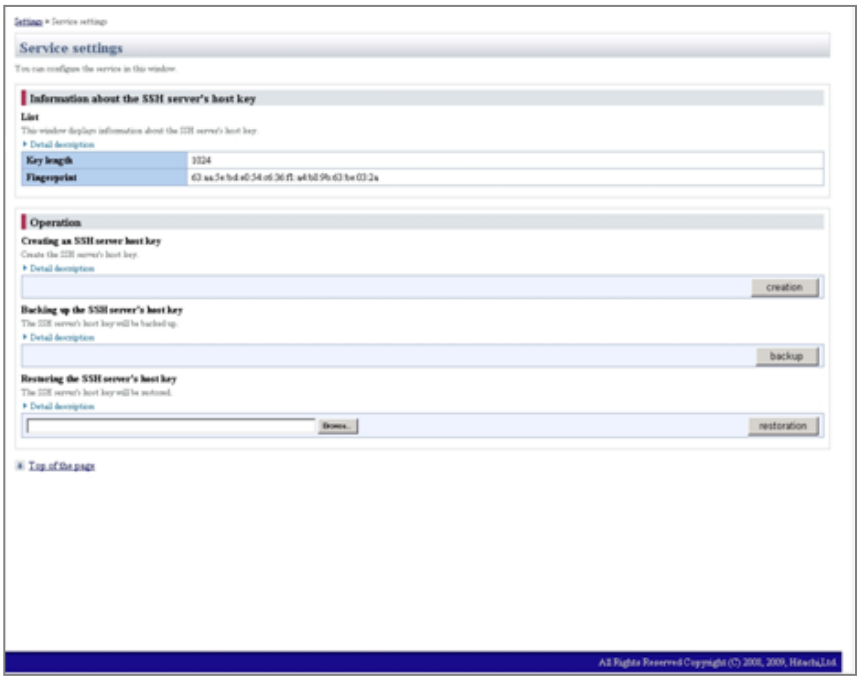
Backing up keys and certificates

#	Item	Description	Edit
1	Backup	Backs up the keys and server certificates currently used on the system web console.	

Restoring keys and certificates

#	Item	Description	Edit
1	Restoration	Restores the backed up keys and certificates in the system web console. Specify a file name.	

❑ SSH key operations view



Information

#	Item	Description	Edit
1	Key length	The key length of the SSH server's host key.	
2	Fingerprint	The fingerprint of the SSH server's host key.	

Creating an SSH server host key

#	Item	Description	Edit
1	creation button	Generates a host key pair for the SSH server. Click this button to create a new key pair.	

Backing up the SSH server's host key

#	Item	Description	Edit
1	backup	Generates a host key pair for the SSH server. Click this button to create a new key pair.	

Restoring the SSH server's host key

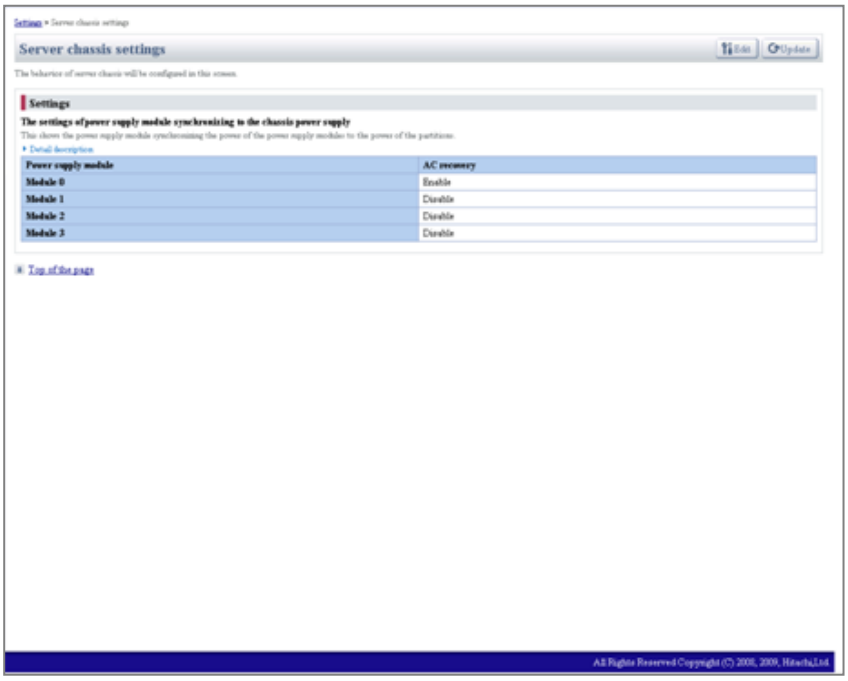
#	Item	Description	Edit
1	restoration	Restores the host key pair of the SSH server. To restore the host key pair, specify the file name and then click this button. Do not specify a file name that includes any of the following characters: /, \, double quotation mark (“), single quotation mark (‘), colon (:), semicolon (;), asterisk (*), question mark (?), <, >, or |.	

❑ Role-dependent variation in available operations

To display the Service setup view and use the features therein, the user must have network permission.

Server chassis settings

❑ Server chassis setting view



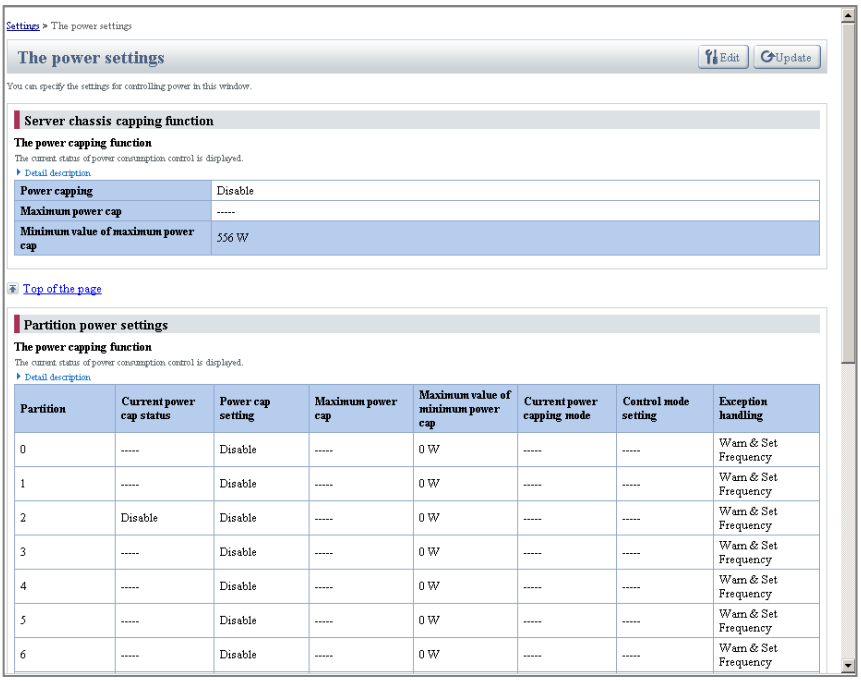
Power supply module settings to be linked to the AC input recovery

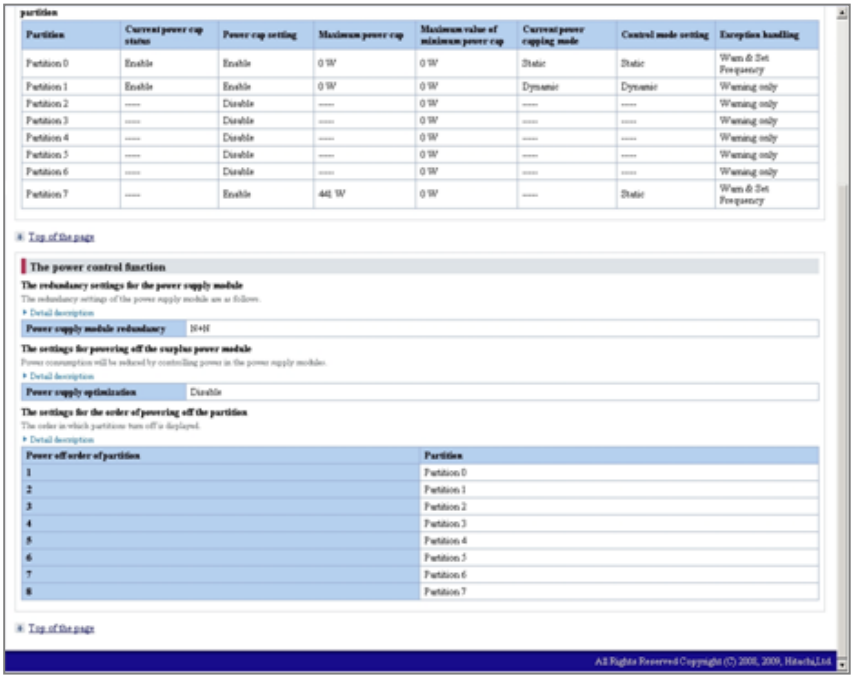
#	Item	Description	Edit
1	Power supply module	The number of a power supply.	-
2	AC recovery	Power synchronization setting: Enable or Disable. When AC power turns off from all power supply modules, which is set to Enable in this setting, and then AC power supply recovers to one of modules with Enable, power supply synchronization between the chassis and partition will start. The delay time depends on the partition settings.	

Power settings

In the Power control setup view, you can set up power control for various components.

❑ Power control settings list view





Server chassis

#	Item	Description	Edit
1	Power capping	Indicates that a limit is imposed on the power consumption of the server chassis. Set as: Enabled or Disabled	Yes
2	Maximum power cap	The maximum power consumption when chassis power consumption control is enabled. Set as: 0 to 65535 (in watts) If you specify a value lower than the minimum specifiable value, the minimum specifiable value is used instead.	Yes
3	Minimum value of maximum power cap	The minimum value that can be specified as the limit value. Set as: 0 to 65535 (in watts)	

Partition

#	Item	Description	Edit
1	Partition	The partition number of a partition.	
2	Current power cap status	The current status of the power capping feature. Set as: Enabled or Disabled	
3	Power cap setting	The power capping setting. Set as: Enabled or Disabled	Yes
4	Maximum power cap	The level at which power capping is implemented. Set as: 0 to 65535 (in watts). If you specify a value lower than the minimum power cap, the minimum power cap is used instead.	Yes
5	Minimum value of maximum power cap	The minimum value specifiable as the power cap. Set as: 0 to 65535 (in watts).	
6	Current power capping mode	The current control mode status. Set as: Static or Dynamic	
7	Control mode setting	The control mode setting. Set as: Static or Dynamic Static may not be enabled depending on a type of the server blade.	Yes
8	Exception handling	The processing performed when an exception occurs during dynamic control. Set as: Warning only or Warn & Set Frequency.	Yes

The power control function.

#	Item	Description	Edit
1	Power supply module redundancy	The redundancy setting of the power supply module. Set as: None, N+1, or N+N	Yes
2	Power supply optimization	The optimized power control setting. Set as: Enabled or Disabled	Yes
3	Power off order of partition	The order in which partitions are turned off in the event that power supply module redundancy can no longer be maintained.	Yes

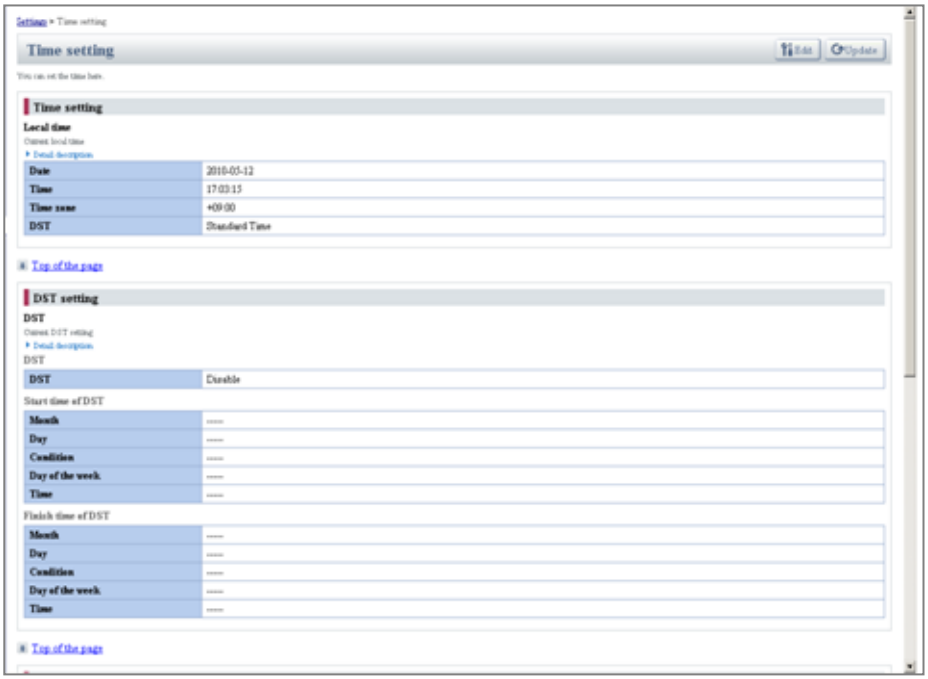
❑ Role-dependent variation in available operations

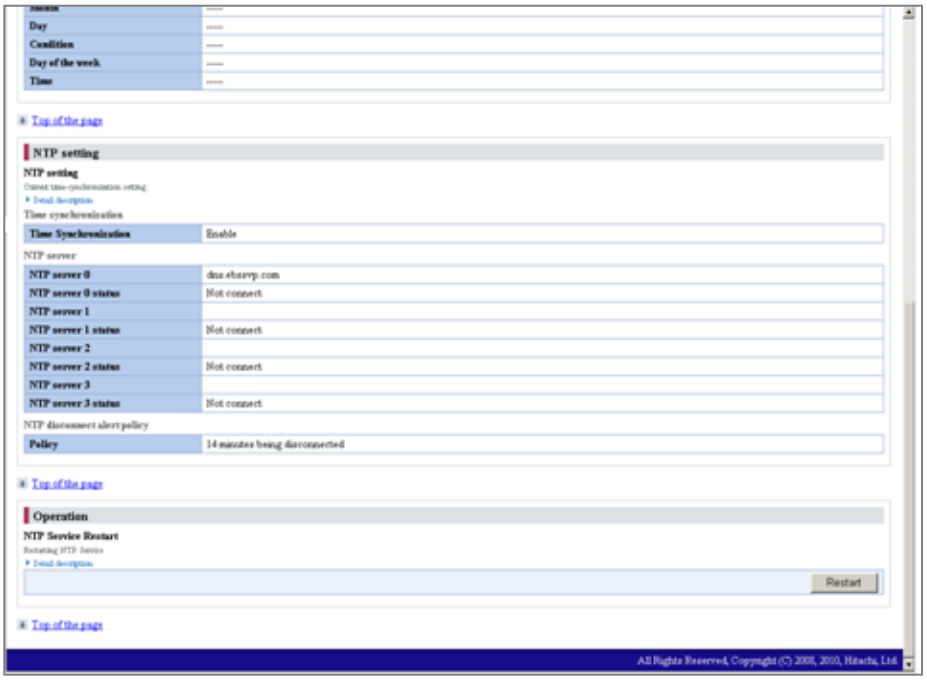
To display the Power control setup view and use the features therein, the user must have chassis permission.

Time setting

In the Time settings view, you can set how the system handles time.

❑ Time settings list view





Time settings

#	Item	Description	Edit
1	Date	The current date in local time.	Yes
2	Time	The current local time.	Yes
3	Time zone	The local time zone. Displayed in one minute increments from -1 2:00 to +14:00.	Yes
4	DST (daylight saving time)	Indicates whether the system is running under standard time or daylight saving time. Set as: Standard Time or Daylight Saving Time	

DST (Daylight Saving Time) Settings

#	Item	Description	Edit
1	DST (daylight saving time)	Indicates whether the system is to use daylight saving time. Set as: Enabled or Disabled	Yes
2	Month	The month in which daylight saving time is to start or finish. Set as: 0 to 12	Yes
3	Day	Used when the time at which daylight saving is to start or finish is specified by date. Set as: 0 to 31	Yes
4	Condition	Indicates the condition used to determine when daylight saving time starts and finishes. Day: The date specified in Day. First after (First prior): The first occurrence of the specified day of the week after (or before) the date specified in “Day”. If you specify this condition, you must specify the "Day of week" setting. Last: If you specify this condition, there is no need to specify the "Day" setting. However, the "Day of week" must be specified.	Yes
5	Day of the week	Used when the time at which daylight saving is to start or finish is specified by day of the week. Set as: Day of the week from Sunday to Saturday	Yes
6	Time	The time when daylight saving time is to start or finish.	Yes

NTP Settings

#	Item	Description	Edit
1	Time synchronization	Indicates whether the clock is synchronized automatically. Set as: Enabled or Disabled	Yes
2	NTP server 0 to 3	The NTP server to use for synchronization, as an IP address or host name. The NTP server can be specified as a fully qualified domain name (FQDN) containing up to 127 characters.	Yes
3	NTP server status 0 to 3	The status of the connection with the NTP server. Set as: Unavailable, Available, or Synchronizing	
4	NTP disconnect alert policy	Policy to alert disconnection from the NTP server. Value: - Immediately	Yes

#	Item	Description	Edit
		- n minutes being disconnected: alerts in 1 to 1440 minutes after disconnected. - Disable	

NTP Service Restart

#	Item	Description	Edit
1	Restart	Restarts the NTP service.	

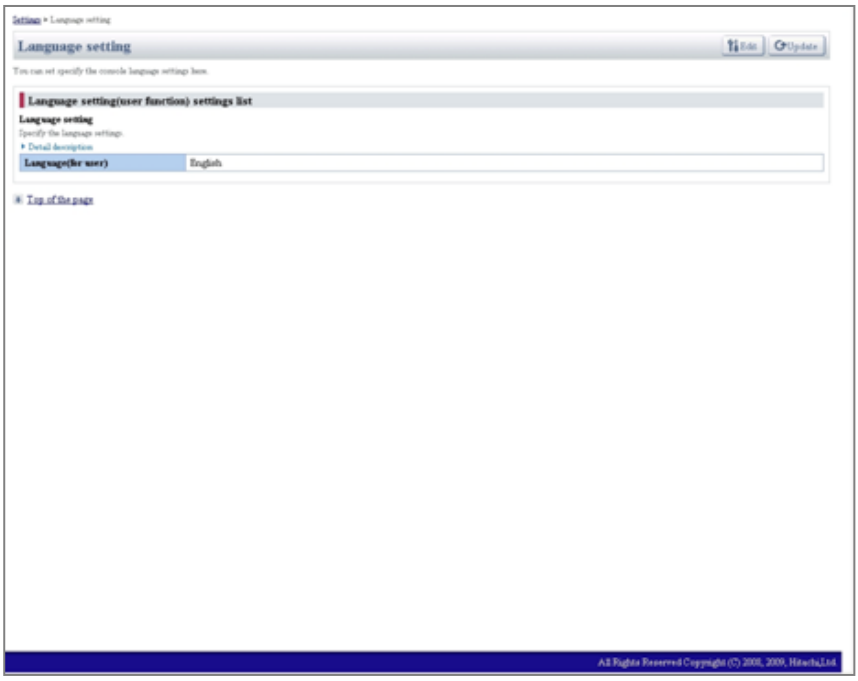
❑ Role-dependent variation in available operations

To display the Time setup view and use the features therein, the user must have chassis permission.

Language setting

In the Language setting view, you can set which language to use.

❑ Language setting list view



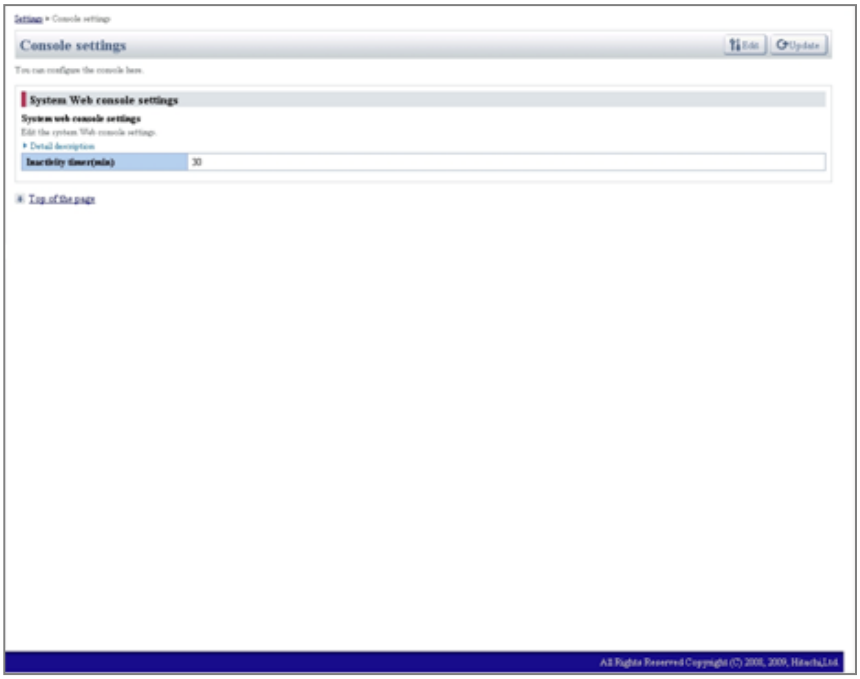
Language setting

#	Item	Description	Edit
1	Language (for user)	You can specify a language you use.	

Console settings

In the Console setup view, you can perform settings related to the system web console.

❑ Console settings list view



#	Item	Description	Edit
1	Inactivity timer (min)	The period of inactivity after which a user is automatically logged out from the system web console. Set as: 1 to 1440 (in minutes) The default is 30.	

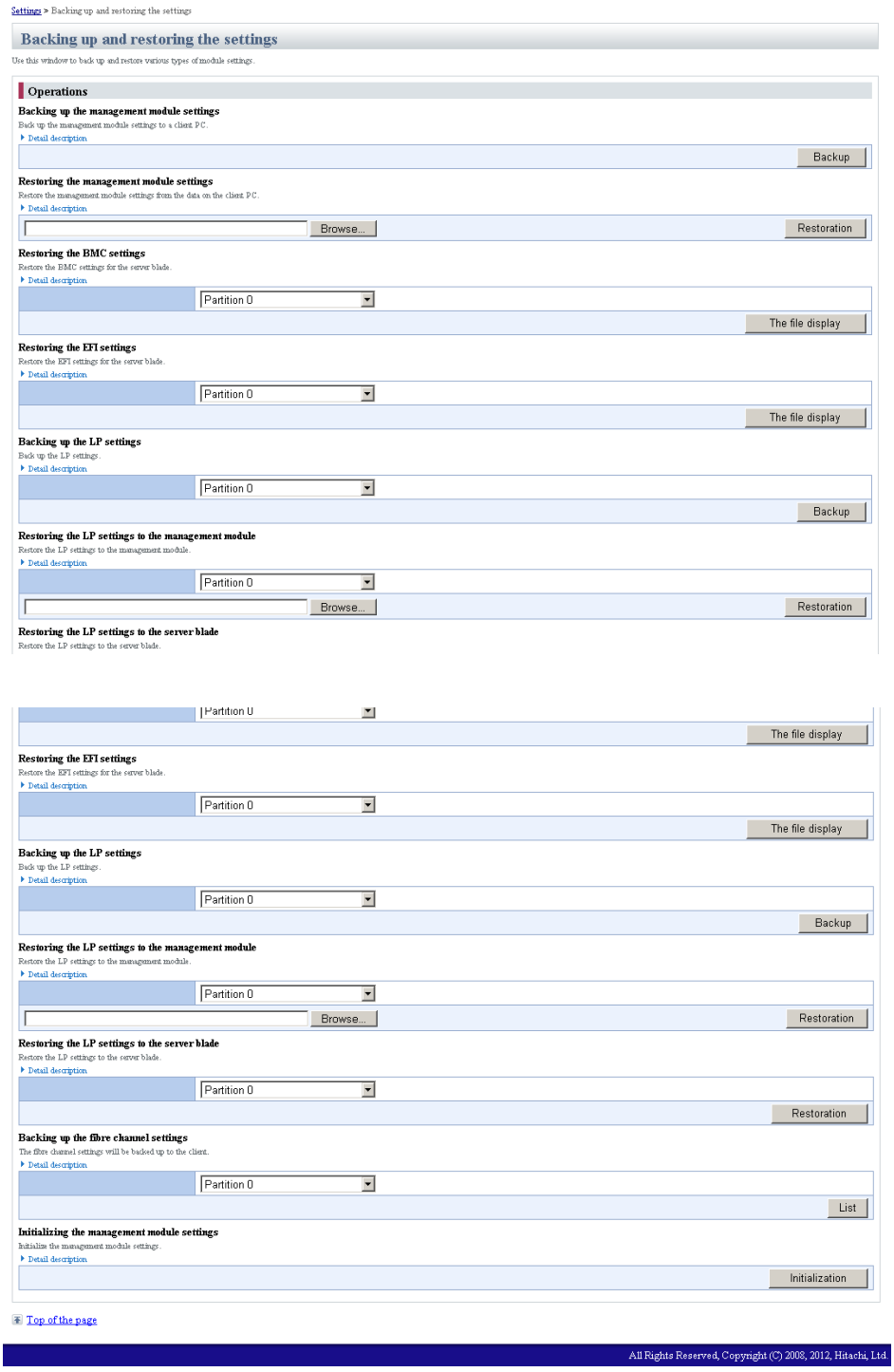
❑ Role-dependent variation in available operations

This information can be displayed and edited by all roles.

Backing up and restoring the settings

In the Console setup view, you can perform settings related to the system web console.

❑ Backing up and restoring the settings



#	Item	Description	Edit
1	Back up	Backs up the settings of the management module. When you click **Back up**, a Save As dialog box appears. Specify a file name and click **Save** to download the file.	
2	Restoration	Restores the settings of the management module. To restore the management module settings, specify the file name and then click this button.	
3	The file display	Restores the BMC settings backed up to the management module. By selecting a partition and clicking this button, you are taken to a page where you can select a backup. To restore backed-up settings, select the backup that you want to restore, and click **Restore**.	
4	The file display	Restores the EFI settings backed up to the management module. By selecting a partition and clicking this button, you are taken to a page where you can select a backup. To restore backed-up settings, select the backup that you want to restore, and then click **Restore**.	
5	Back up	Backs up LPAR manager settings kept on the management module. When you select a partition and click this button, a Save As dialog box appears. Specify a file name and click **Save** to download the file.	
6	Restoration	Restores LPAR manager settings from backed-up settings on the management module. To restore the settings, specify a file and partition and then click this button.	
7	Restoration	Restores the LPAR manager settings on the server blade from a backup file kept on the management module. To restore the settings, specify a partition and then click this button.	
8	List	Backs up Fibre-channel settings. Selecting a card type and a partition and clicking this button takes you to a page where you can select the Fibre-channel whose settings you want to back up. After selecting the Fibre-channel settings, click **Back up** to back up the settings.	
9	Initialization	Initializes the management module settings. Clicking this button restores the management module settings to the factory defaults.	



Do not restore or initialize the management module backup file while the server blade works. If you do, proper operation may not be available due to the discrepancy between the restored or initialized configuration and the configuration when the server blade operates.
When restoring or initializing the backup file while the server blade with N+M cold standby enabled is not in operation, make sure to perform Smart Configure afterwards.

❑ Role-dependent variation in available operations

To back up and restore settings, the user must have chassis permission.

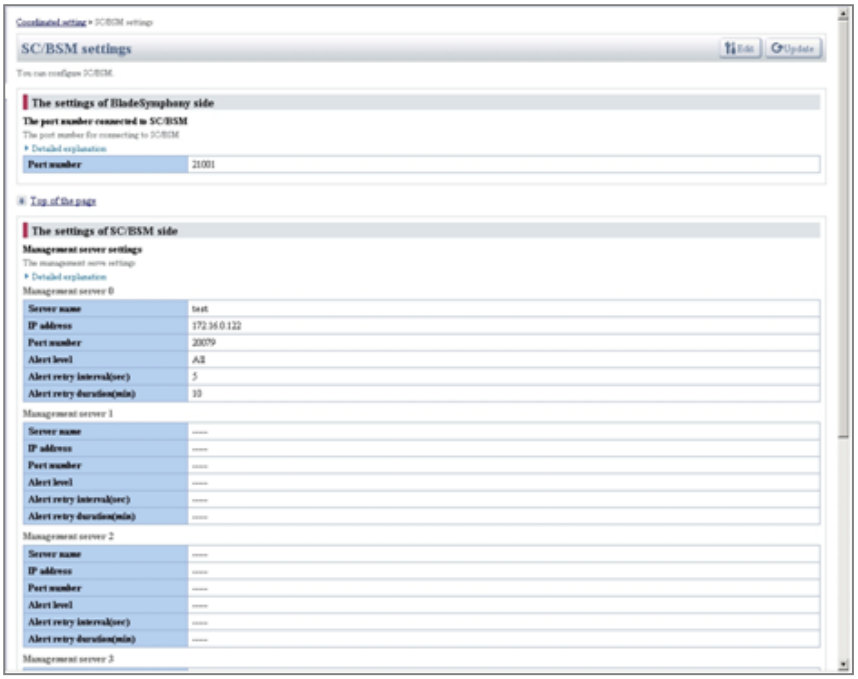


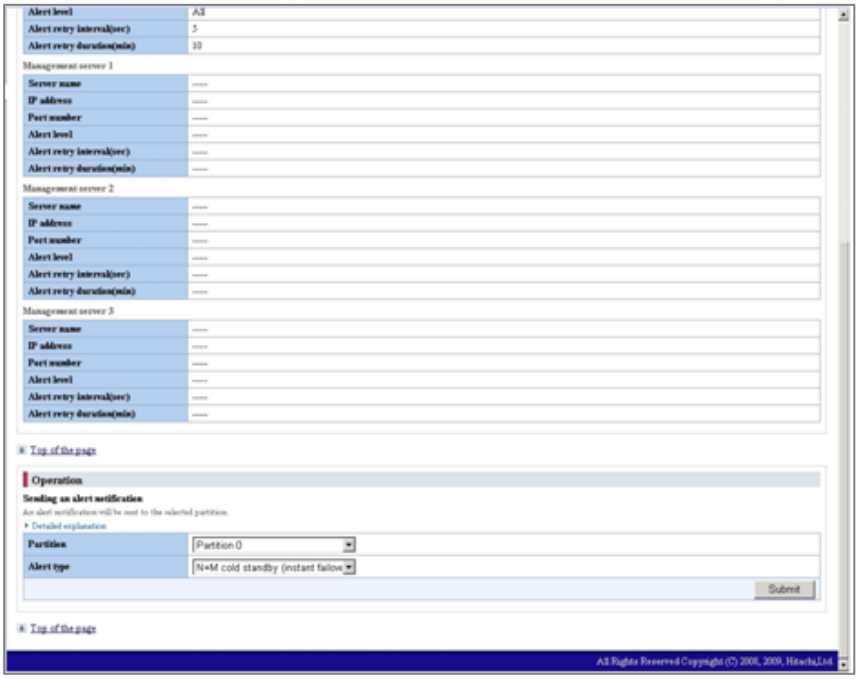
When restoring the configuration before LPAR migration to the migrated partition with the restoring function of this command, restore the configuration before migration to both the source and destination. Refer to Chapter 12: Logical partitioning manager for further information.

SC/BSM settings

In the SC/BSM Linkage setup view, you can display and configure the settings for linkage with SC/BSM.

❑ SC/BSM linkage setup view





The settings of Compute Blade side

#	Item	Description	Edit
1	Port number	The port number used to connect to SC/BSM. Set as: 0 to 65535 If “0” is set, the port to connect SC/BSM is closed	

The setting of SC/BSM side

#	Item	Description	Edit
1	Server name	The management server name. A management server name can contain a maximum of 15 alphanumeric characters or symbols.	Yes
2	IP address	The IP address of the management server.	Yes
3	Port number	The port number used to send alerts. Set as: 1 to 65535	Yes
4	Alert level	The alert notification level. You can select disable, alert, information, or all.	Yes
5	Alert retry interval (sec)	The interval between attempts by SC/BSM to send an alert notification (in seconds). Set as: 5 to 50	Yes
6	Alert retry duration (min)	The length of time SC/BSM continues to retry sending the alert notification (in minutes). Set as: 4 to 20	Yes



When configuring a management server, check **Deletion of the settings** for unused management servers.

Sending an alert information

#	Item	Description	Edit
1	Submit	Sends an alert. You can send one of two alert types, N+M cold standby (immediate switchover) and N+M cold standby (delayed switchover). To send an alert, select the destination partition and the alert type, and then click **Send**.	Yes

❑ Role-dependent variation in available operations

To display and edit information in the SC/BSM linkage letup view, the user must have chassis permission.

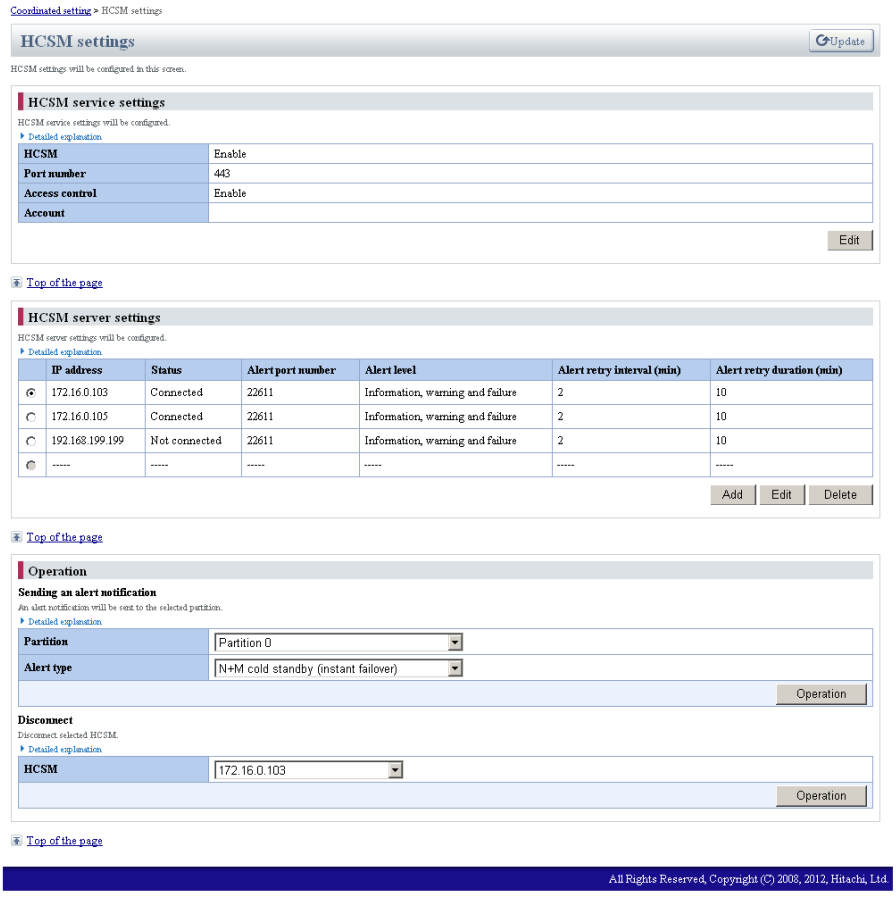


Do not perform an N+M cold standby switching test by issuing an alert in this screen together with LPAR migration targeted to that partition. Refer to Chapter 12: Logical partitioning manager in this User’s Guide for the further information.

SNMP setup view HCSM settings

In the HCSM setup view, you can display and configure settings related to the Hitachi Compute Systems Management (HCSM).

❑ HCSM setup view



HCSM service settings

#	Item	Description	Edit
1	HCSM	Shows whether HCSM is enabled or disabled. Set as: Enable or Disable.	Yes
2	Port number	Port number used for HCSM. Can be changed in the Service settings list view > HTTP > Status: Select HTTPS > Port number.	-
3	Access control	Control of access to the management module from HCSM depending on the IP address. Set as: Enable or Disable. Enable: Only access from HCSM with the address shown in HCSM server settings is available.	Yes
4	Account	Account used by HCSM to connect to the management module. No account is set by default.	Yes
5	Edit	Edits HCSM service settings.	-

HCSM server settings

#	Item	Description	Edit
1	IP address	Shows HCSM IP addresses registered in the management module.	Yes
2	Status	Shows whether or not this HCSM is connected to the management module.	-
3	Alert port number	Shows the destination HCSM port number. Default value: 22611	Yes
4	Alert level	Shows an alert level to notify one of the following values. Only failure: Notifies only failure-level alerts, no warning- and information level alerts. Warning and failure: Notifies failure- and warning-level alerts, no information-level alert. Do not notify: Notifies no alerts.	Yes
5	Alert retry interval (min)	Shows the alert retry interval from 1 to 4 minutes.	Yes
6	Alert retry duration (min)	Shows the alert retry duration from 4 to 15 minutes in case that an alert cannot be notified to HCSM due to temporary failure in the network.	Yes
7	Add	Adds HCSM to connect.	-
8	Edit	Edits settings for connection to the selected HCSM	-
9	Delete	Deletes connection of the selected HCSM.	-

Sending an alert notification

#	Item	Description	Edit
1	Partition	Selects a partition to issue a test alert.	-
2	Alert type	Selects a test alert type from the following two. - N+M cold standby (instant failover) - N+M cold standby (delayed failover)	-
3	Operation	Sends a test alert.	

Disconnect

#	Item	Description	Edit
1	HCSM	Selects HCSM to disconnect	-
2	Operation	Disconnects the selected HCSM.	-

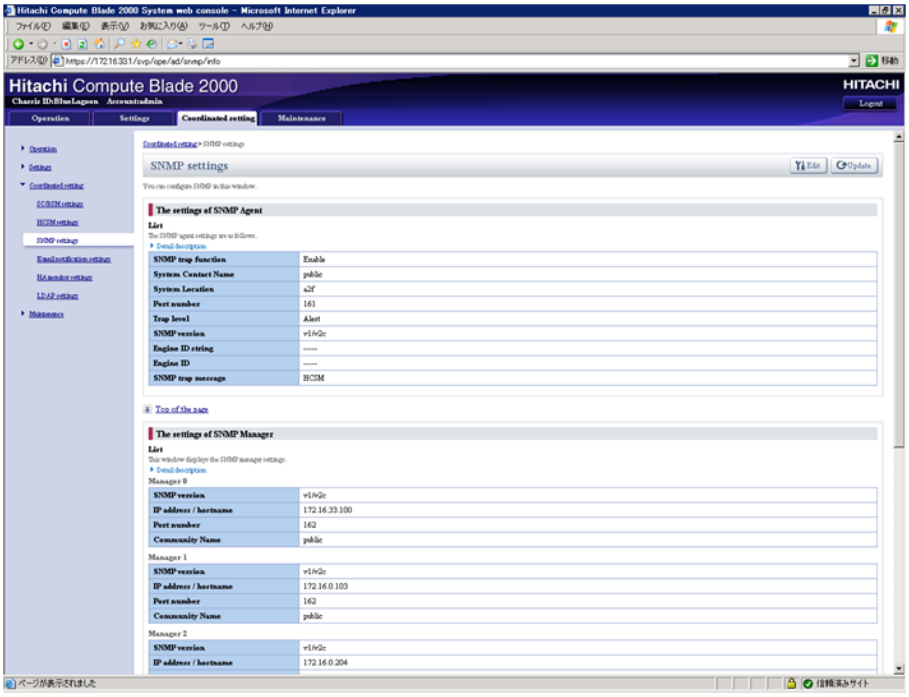
❑ Role-dependent variation in available operations

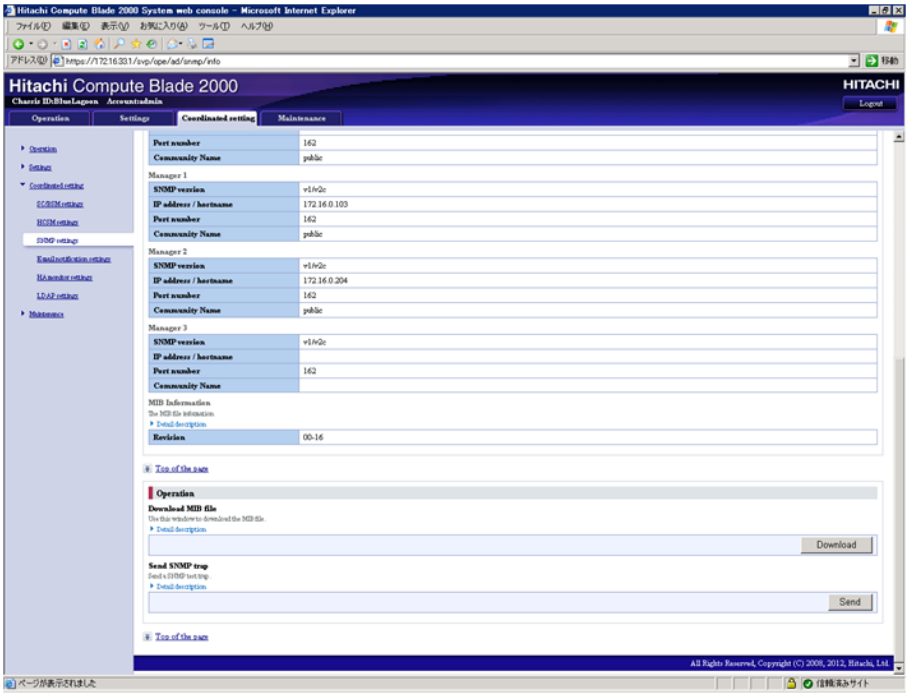
To display and configure information in the HCSM setup view, the user must have chassis permission.

SNMP settings

In the SNMP setup view, you can display and configure settings related to the Simple Network Management Protocol (SNMP).

❑ SNMP setup view





SNMP Agent settings

#	Item	Description	Edit
1	SNMP trap function	Indicates whether the SNMP trap function is enabled or disabled. Set as: Enabled or Disabled	
2	System Contact Name	The contact information for the system administrator. This field can contain a maximum of 60 alphanumeric characters and symbols.	Yes
3	System Location	The location of the system. This field can contain a maximum of 60 alphanumeric characters and symbols.	Yes
4	Port number	The port number used for SNMP transmission. Set as: 1 to 65535	Yes
5	Trap level	The trap notification level. You can select disable, alert, information, or all.	Yes
6	SNMP version	SNMP version used by the agent. Value: v1/v2c or v1/v2c\v3	Yes
7	Engine ID string	Enabled only when the SNMP version is v1/v2c/v3. Character string that the agent uses to create an engine ID: 1 to 27 character(s), 1-byte printable alphanumeric characters and signs, can be used.	Yes
8	Engine ID	Enabled only when the SNMP version is v1/v2c/v3. Engine ID used by the agent which is automatically created from the engine ID string.	-
9	SNMP trap message	Indicates SNMP trap failure messages. One of the following values. BSM: Indicates alerts in the same way as BSM alerts. HCSM: Indicates alerts in the same way as HCSM alerts.	Yes

The Manager settings

#	Item	Description	Edit
1	SNMP version	SNMP version used by the SNMP manager Set as: v1/v2c or v3.	Yes
2	IP address	IP address of the SNMP manager. Setting for the manager is disabled by specifying 0.0.0.0.	Yes
3	Port number	Destination port number for traps issued by the SNMP manager. Set as: 1 to 65535	Yes
4	Community Name	Enabled only when the SNMP version is v1/v2c. Community name of the SNMP manager This field can contain a maximum of sixty 1-byte printable alphanumeric characters and signs.	Yes
5	User Name	Enabled only when the SNMP version is v3. User name of the SNMP manager. 1 to 32 characters, 1-byte printable alphanumeric characters and signs, can be used.	Yes
6	Access Type	Enabled only when the SNMP version is v3. Access type for the SNMP manager Set as: noAuthnoPriv, AuthnoPriv, or AuthPriv	Yes
7	Authentication type	Enabled only when the SNMP version is v3 and the access type is AuthnoPriv/or AuthPriv.	Yes

#	Item	Description	Edit
		Authentication type for the SNMP manager Set as: MD5 or SHA	
8	Authentication password	Enabled only when the SNMP version is v3 and the access type is AuthnoPriv or AuthPriv. Password for the SNMP manager authentication 8 to 64 characters, 1-byte printable alphanumeric characters and signs, can be used. When nothing is entered, no change happens.	Yes
9	Encryption type	Enabled only when the SNMP version is v3 and the access type is AuthPriv. Encryption type for the SNMP manager Set as: DES or AES.	Yes
10	Encryption password	Enabled only when the SNMP version is v3 and the access type is AuthPriv. Password for the SNMP manager encryption 8 to 64 characters, 1-byte printable alphanumeric characters and signs, can be used. When nothing is entered, no change happens.	Yes

MIB Information

#	Item	Description	Edit
1	Revision	The revision number of the MIB file.	

Download MIB file

#	Item	Description	Edit
1	Download	Downloads the MIB file. When you click **Download**, a Save As dialog box appears. Specify a file name and click **Save** to download the file.	

Send SNMP trap

#	Item	Description	Edit
1	Send	Sends an SNMP trap. Click this button to send a test SNMP trap notification.	

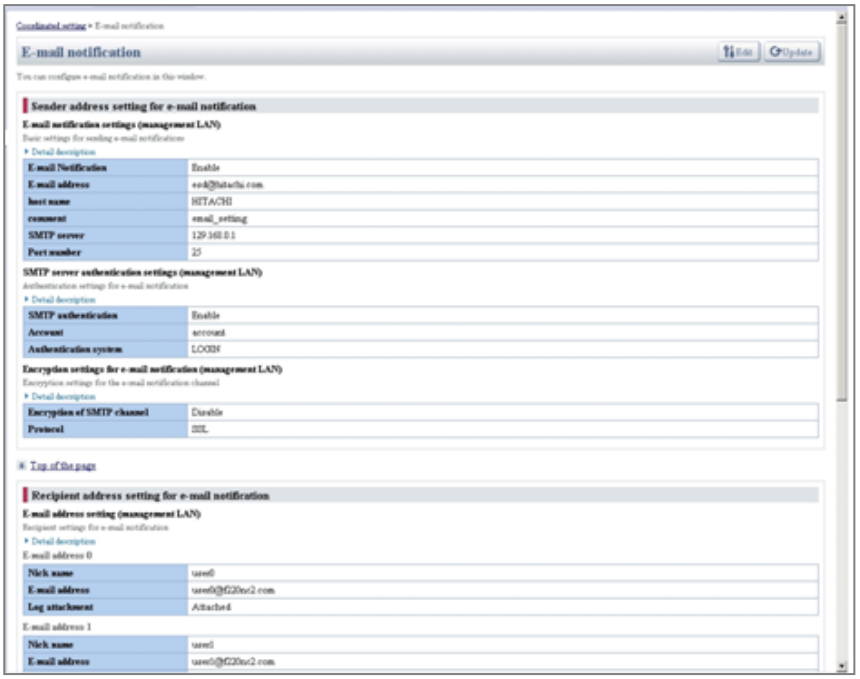
❑ Role-dependent variation in available operations

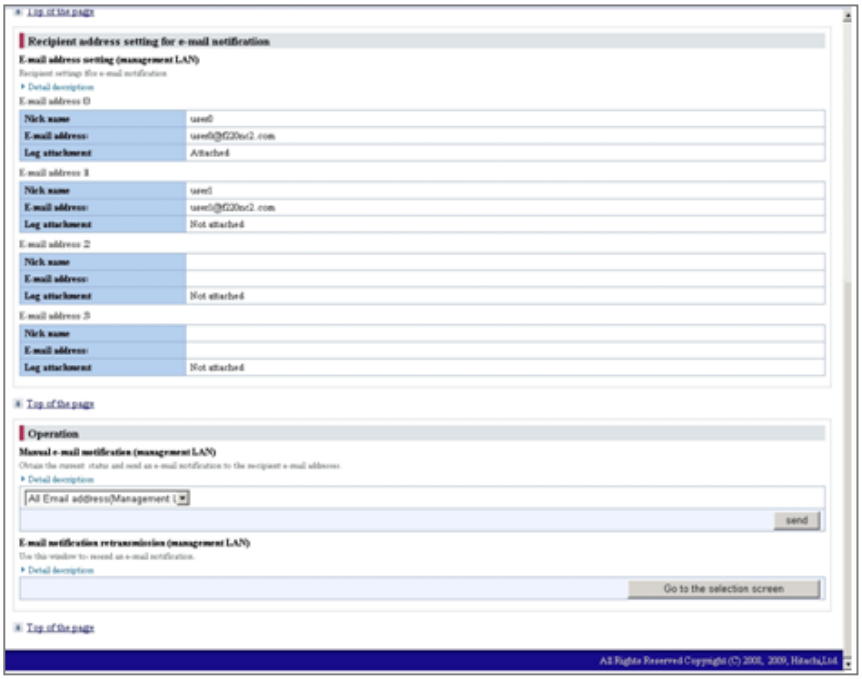
To display and edit information in the SNMP setup view, the user must have chassis permission.

E-mail notification

In the Remote E-mail notification setup view, you can display and configure settings related to remote email notification.

❑ Remote E-mail notification setup view





Sender address setting

#	Item	Description	Edit
1	E-mail Notification	Indicates whether the remote email notification function is enabled or disabled. Set as: Enabled or Disabled	
2	E-mail address	The e-mail address from which the notification is sent. This field can contain a maximum of 64 characters. You can use alphanumeric characters and the following symbols: tilde (~), @, #, $, %, ^, hyphen (-), +, =, underscore (_), period (.), [,]	Yes
3	host name	The host name of the machine. The host name can be specified as a fully qualified domain name (FQDN) containing no more than 64 characters.	Yes
4	comment	A comment. This field can contain a maximum of 32 alphanumeric characters or symbols.	Yes
5	SMTP server	The SMTP server used by the remote email notification function. Specify an IP address or host name. The host name can be specified as a fully qualified domain name (FQDN) containing no more than 64 characters.	Yes
6	Port number	The port number of the SMTP server. Set as: 1 to 65535	Yes

SMTP server authentication settings

#	Item	Description	Edit
1	SMTP authentication	Setting whether or not to execute the SMTP authentication: Set as: Enabled or Disabled	
2	Account	Account for SMTP authentication This field can contain a maximum of 64 ASCII characters. You can use alphanumeric characters and the following symbols: tilde (~), @, #, $, %, ^, hyphen (-), +, =, underscore (_), period (.), [,] You can also specify a password using up to 64 ASCII characters. Alphanumeric characters, blank " ", and other symbols that can be displayed. Make sure to specify the account and password when enabling the SMTP authentication.	Yes
3	Authentication system	Set as: PLAIN: binary data LOGIN: binary data; interactive CRAM-MD5: challenge and response	Yes

Encryption settings

#	Item	Description	Edit
1	Encryption of SMTP channel	Whether or not to encrypt SMTP paths Set as: Enabled or Disabled	
2	Protocol	Protocol for SMTP path encryption Set as: SSL or TLS.	Yes

Recipient address setting

#	Item	Description	Edit
1	Nick name	The nickname associated with the e-mail address. This field can contain a maximum of 15 alphanumeric characters or symbols.	Yes
2	E-mail address	The destination email address. This field can contain a maximum of 64 characters. You can use alphanumeric characters and the following symbols: tilde (~), @, #, $, %, ^, hyphen (-), +, =, underscore (_), period (.), [,]	Yes
3	Log attachment	Indicates whether to attach log information to the e-mail notification. Set as: Yes or No	Yes

Manual e-mail notification

#	Item	Description	Edit
1	Send	Manually sends a notification of the latest log data. Select the destination e-mail address and then click **Notify**.	

E-mail notification retransmission

#	Item	Description	Edit
1	Go to the selection screen	Use this button to resend a remote e-mail notification from the e-mail notification log. Clicking this button takes you to a page where you can select which email notification to resend. To send the information, select the desired E-mail Notification record logged in the E-mail Notification log, select the destination email address, and then click **Notify**. The notification results displayed in the selection page will be updated according to the result of the resending.	

❑ Role-dependent variation in available operations

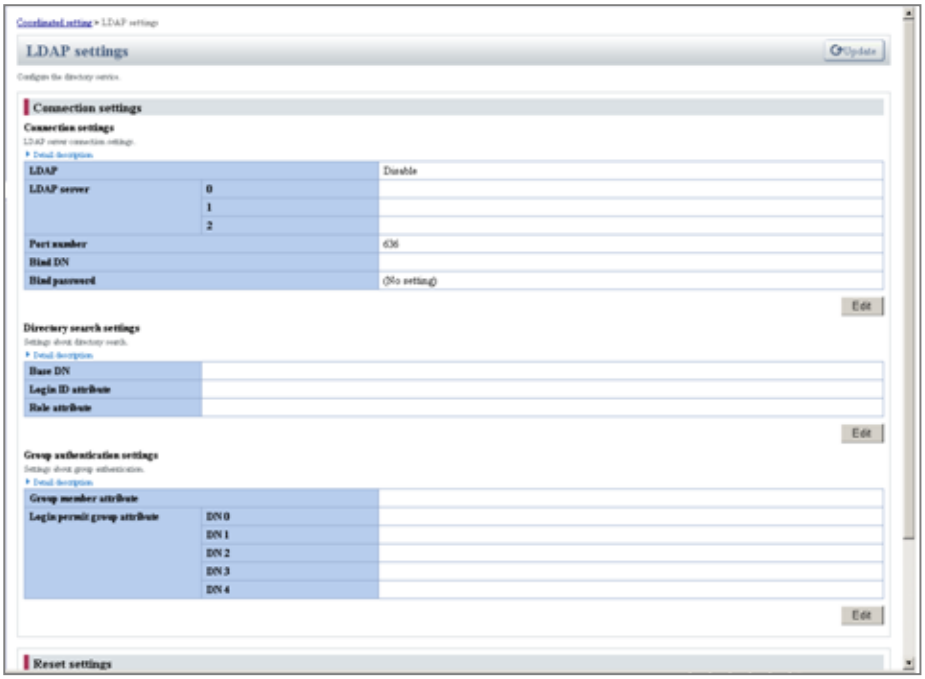
To display and edit information in the Remote E-mail notification setup view, the user must have chassis permission.

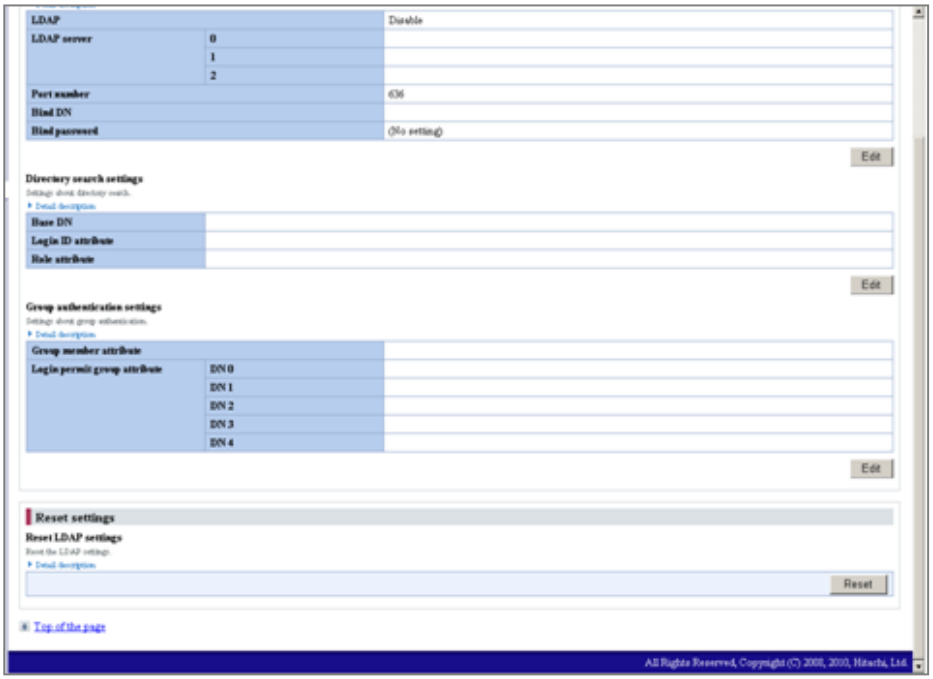
HA monitor settings

HA monitor does not function with this equipment. Thus, this setting is not available.

LDAP settings

In the LDAP settings, you can display and set connection to the directory service.





Connection settings

#	Item	Description	Edit
1	LDAP	Sets Enable or Disable LDAP.	Yes
2	LDAP server	LDAP server host name in FQDN or IPv4 up to 127 characters A blank space is not available for the head and end character. Available characters: English alphabets [A-Z][a-z]; number [0-9]; hyphen “-“; period “.”	Yes
3	Port number	Value: 1 to 65535	Yes
4	Bind DN	1 to 256 characters in ASCII A blank space is not available for the head and end character.	Yes
5	Bind password	1 to 32 characters including a blank space in ASCII	Yes
6	Bind password (retype)	Retype the Bind password.	Yes

Directory search settings

#	Item	Description	Edit
1	Base DN	1 to 256 characters in ASCII A blank space is not available for the head and end character.	Yes
2	Login ID attribute	1 to 64 characters in ASCII A blank space is not available for the head and end character Available for the first character : English alphabet [A-Z][a-z]; for the other characters: alphanumeric [A-Z][a-z] [0-9]	Yes
3	Role attribute	1 to 64 characters in ASCII A blank space is not available for the head and end character Available for the first character : English alphabet [A-Z][a-z]; for the other characters: alphanumeric [A-Z][a-z] [0-9]	Yes

Group authentication settings

#	Item	Description	Edit
1	Group member attribute	1 to 64 characters in ASCII A blank space is not available for the head and end character Available for the first character : English alphabet [A-Z][a-z]; for the other characters: alphanumeric [A-Z][a-z] [0-9]	Yes
2	Login permit group attribute	Group with permission to login: DN0 to 4 1 to 256 characters in ASCII A blank space is not available for the head and end character.	Yes

Reset LDAP settings

#	Item	Description	Edit
1	Reset	Resets all LDAP setting. Click **Reset** to jump to the confirmation screen. Then to confirm the reset, click **Confirm**.	-

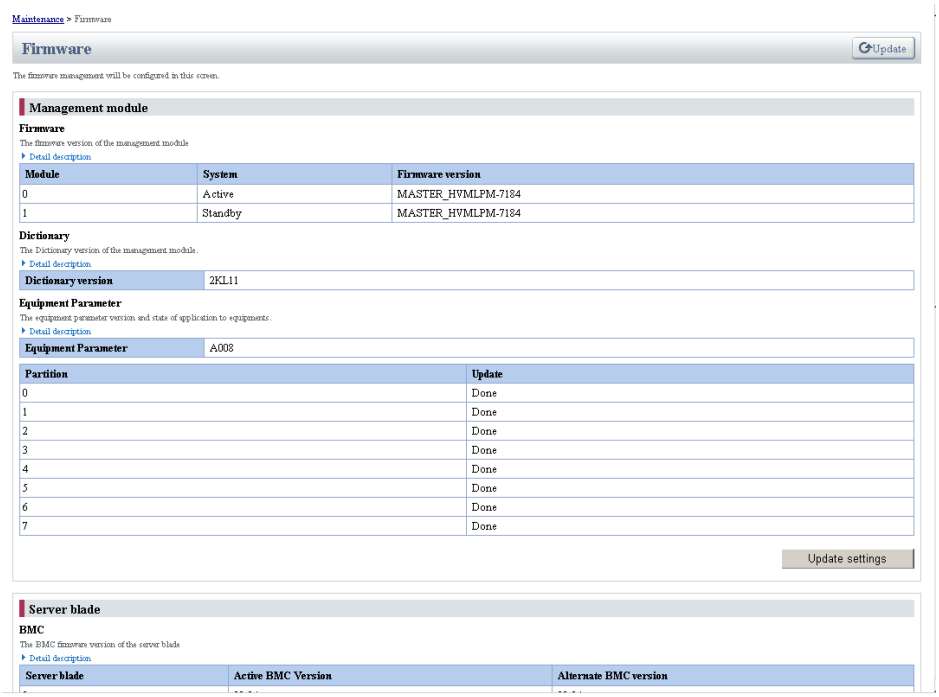
❑ Role-dependent variation in available operations

To display and set the LDAO settings screen, the user must have chassis permission.

Firmware management

In the Firmware management view, you can display and update a range of firmware data.

❑ Firmware management view



Maintenance > Firmware

Firmware — Update

The firmware management will be configured in this screen.

Management module

Firmware

The firmware version of the management module

Detail description

Module	System	Firmware version
0	Active	MASTER_HVMLPM-7184
1	Standby	MASTER_HVMLPM-7184

Dictionary

The Dictionary version of the management module.

Detail description

Dictionary version	2KL11

Equipment Parameter

The equipment parameter version and state of application to equipments.

Detail description

Equipment Parameter	A008

Partition	Update
0	Done
1	Done
2	Done
3	Done
4	Done
5	Done
6	Done
7	Done

Update settings

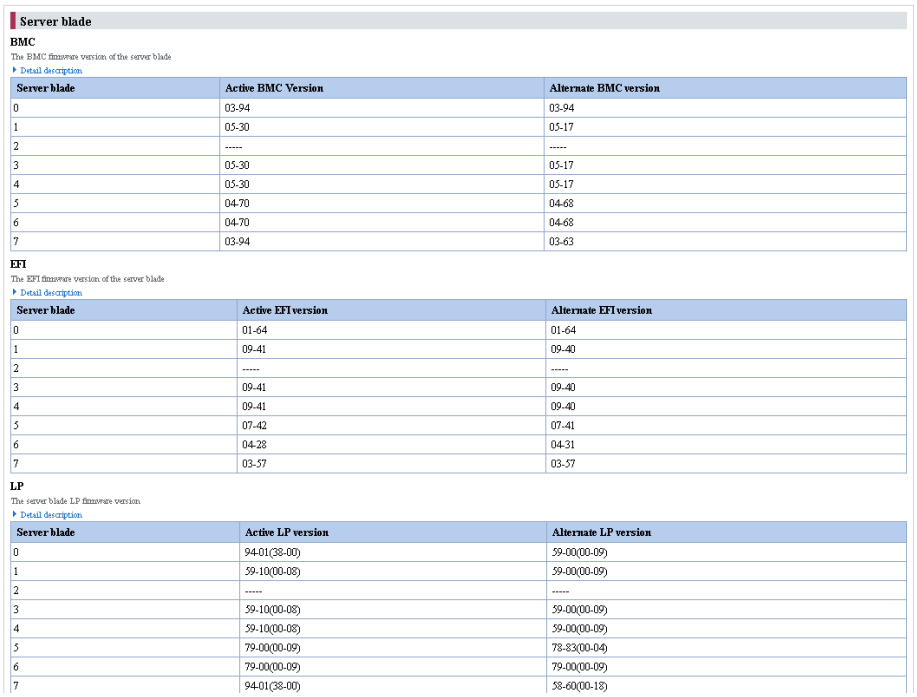
Server blade

BMC

The BMC firmware version of the server blade

Detail description

Server blade	Active BMC Version	Alternate BMC version



Server blade

BMC

The BMC firmware version of the server blade

Detail description

Server blade	Active BMC Version	Alternate BMC version
0	03-94	03-94
1	05-30	05-17
2	-----	-----
3	05-30	05-17
4	05-30	05-17
5	04-70	04-68
6	04-70	04-68
7	03-94	03-63

EFI

The EFI firmware version of the server blade

Detail description

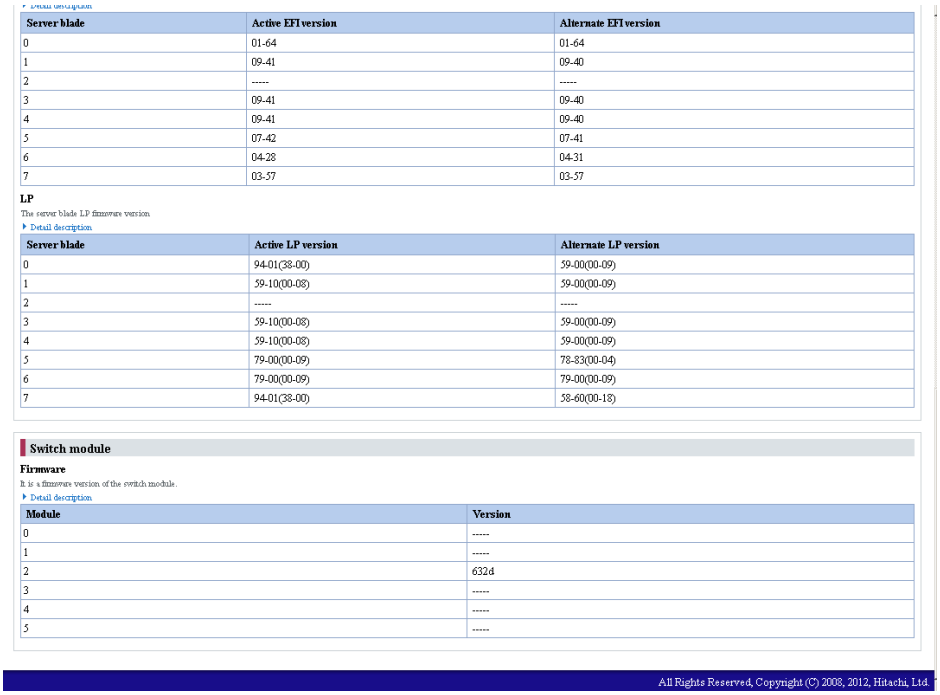
Server blade	Active EFI version	Alternate EFI version
0	01-64	01-64
1	09-41	09-40
2	-----	-----
3	09-41	09-40
4	09-41	09-40
5	07-42	07-41
6	04-28	04-31
7	03-57	03-57

LP

The server blade LP firmware version

Detail description

Server blade	Active LP version	Alternate LP version
0	94-01(38-00)	59-00(00-09)
1	59-10(00-08)	59-00(00-09)
2	-----	-----
3	59-10(00-08)	59-00(00-09)
4	59-10(00-08)	59-00(00-09)
5	79-00(00-09)	78-83(00-04)
6	79-00(00-09)	79-00(00-09)
7	94-01(38-00)	58-60(00-18)



Server blade	Active EFI version	Alternate EFI version
0	01-64	01-64
1	09-41	09-40
2	-----	-----
3	09-41	09-40
4	09-41	09-40
5	07-42	07-41
6	04-28	04-31
7	03-57	03-57

LP

The server blade LP firmware version.

Detail description

Server blade	Active LP version	Alternate LP version
0	94-01(38-00)	59-00(00-09)
1	59-10(00-08)	59-00(00-09)
2	-----	-----
3	59-10(00-08)	59-00(00-09)
4	59-10(00-08)	59-00(00-09)
5	79-00(00-09)	78-83(00-04)
6	79-00(00-09)	79-00(00-09)
7	94-01(38-00)	58-60(00-18)

Switch module

Firmware

It is a firmware version of the switch module.

Detail description

Module	Version
0	-----
1	-----
2	632d
3	-----
4	-----
5	-----

All Rights Reserved, Copyright (C) 2008, 2012, Hitachi, Ltd.

Management module

#	Item	Description	Edit
1	Module	The module number.	-
2	System	Indicates whether the management module is serving as an active or standby system. Set as: Active or Standby	-
3	Firmware version	The firmware version of the management module.	-

Dictionary

#	Item	Description	Edit
1	Dictionary version	The dictionary version used in the translation of event codes.	–

Equipment Parameter

#	Item	Description	Edit
1	Equipment Parameter	Equipment parameter version.	–
2	Partition	Partition number.	–
3	Update	Displays whether or not the equipment parameter is applied to the partition. When there is no partition, “-----“ is displayed.	–

Update

#	Item	Description	Edit
1	Update settings	Click this button to jump to the update settings screen to update firmware. In the screen, specify a file and click **Update**.	

Server blade

#	Item	Description	Edit
1	Server blade	The server blade number.	–
2	BMC version	The version of the BMC firmware in use on the server blade: the version currently used and that of the alternate BMC.	–
3	EFI version	The EFI version in use on the server blade: the version currently used and that of the alternate EFI.	-

LP

#	Item	Description	Edit
1	Server blade	The server blade number.	–
2	Active LP version	The LPAR manager version currently in use on the server blade.	–
3	Alternate LP version	An alternate LPAR manager program which is present on the server blade but not currently in use.	-

Switch module

#	Item	Description	Edit
1	Module	The number of a switch module.	–
2	Version	The firmware version of the switch module is shown as up to four digits. For firmware versions with five or more digits, find it on the switch module console.	–

❑ Role-dependent variation in available operations

To display and use the Firmware management view, the user must have chassis permission.

Log management

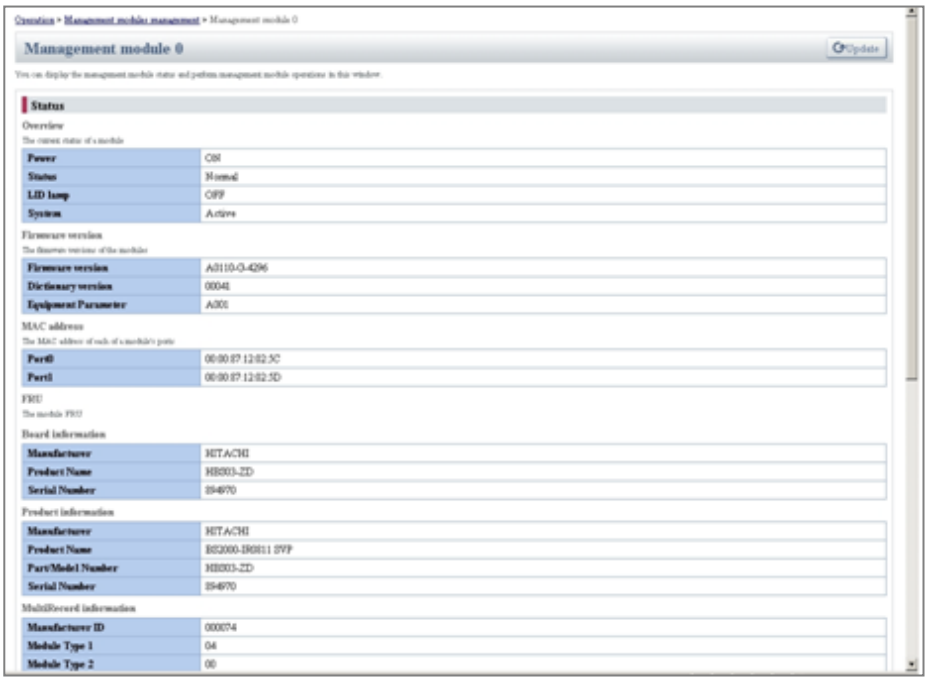
In the Log management view, you can display and download a range of log information.

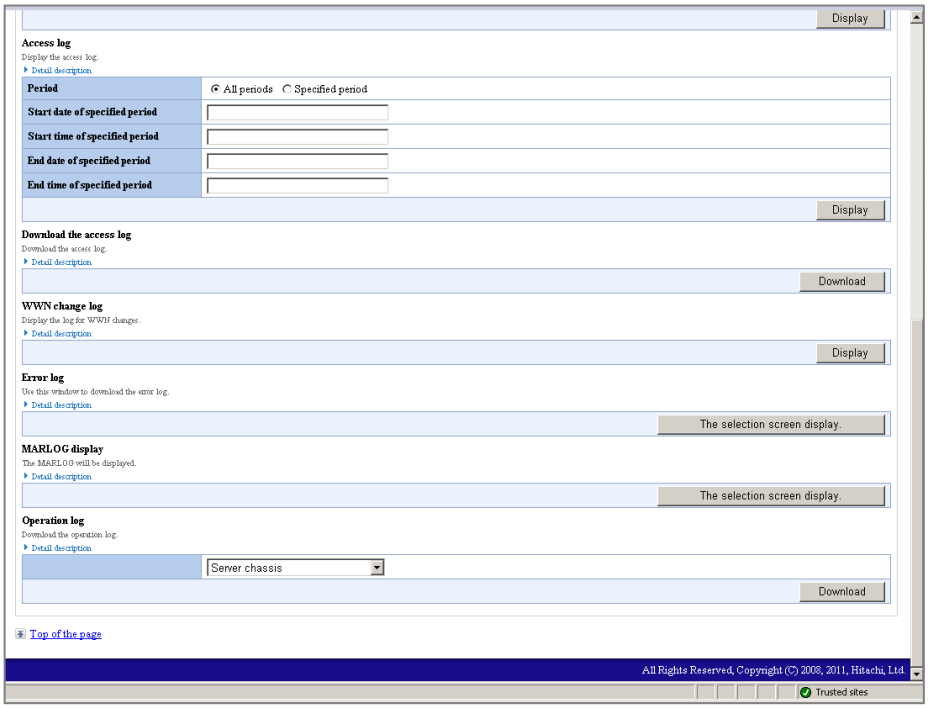
Tip

If the download is blocked by the security protection of the browser, check the security settings of Internet Options and change them to the proper values including those below.

- File download: Enable
- Automatic prompting for file downloads: Enable

❑ Log management view

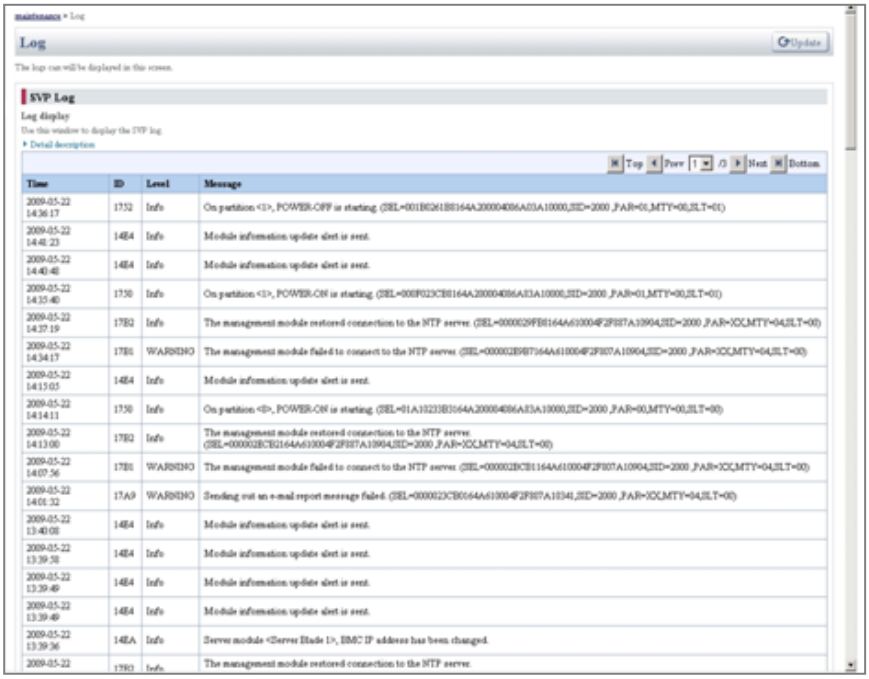




#	Item	Description	Edit
1	Display	Takes you to the SVP Log Display view.	-
2	Display	Takes you to the System Event Log Display view.	-
3	Download	Downloads a dump log. When you click **Download**, a Save As dialog box appears. Specify a file name and click **Save** to download the file.	-
4	Display	Takes you to the Power Status Trend Data view.	-
5	Display	Takes you to the Short-term Environment Log Display view.	-
6	Display	Takes you to the Access Log Display view. You can select whether to display all access log information or information logged during a specific time period.	-
7	Download	Downloads access log information. When you click **Download**, a Save As dialog box appears. Specify a file name to download the file.	-
8	Display	Takes you to the WWN Change log Display view.	-
9	Error log	Takes you to the selection page for system event logs. To download the error log information, select the required System Event Log and click **Download**.	-
10	MARLOG display	Takes you to the selection page for MAR logs. When you click a link in the number of MARLOG required in the selection screen, you can go to the Detail Display of MARLOG.	-
11	Operation log (Download)	Downloads operation logs for management modules. Select Partition or Server chassis from the drop-down list and click **Download** to open a dialog box for saving files. Selectable items depend on the privilege for a login account. **Partition** selected: Downloads logs of operation	

#	Item	Description	Edit
		executable with the partition privilege. **Server chassis** selected: Downloads all operation logs of management modules.	

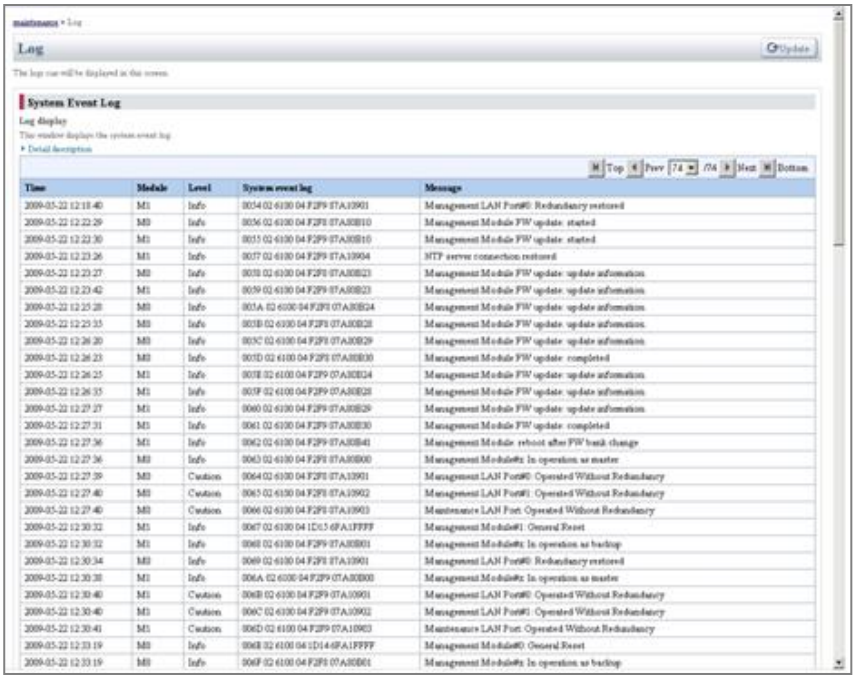
❑ SVP log display view





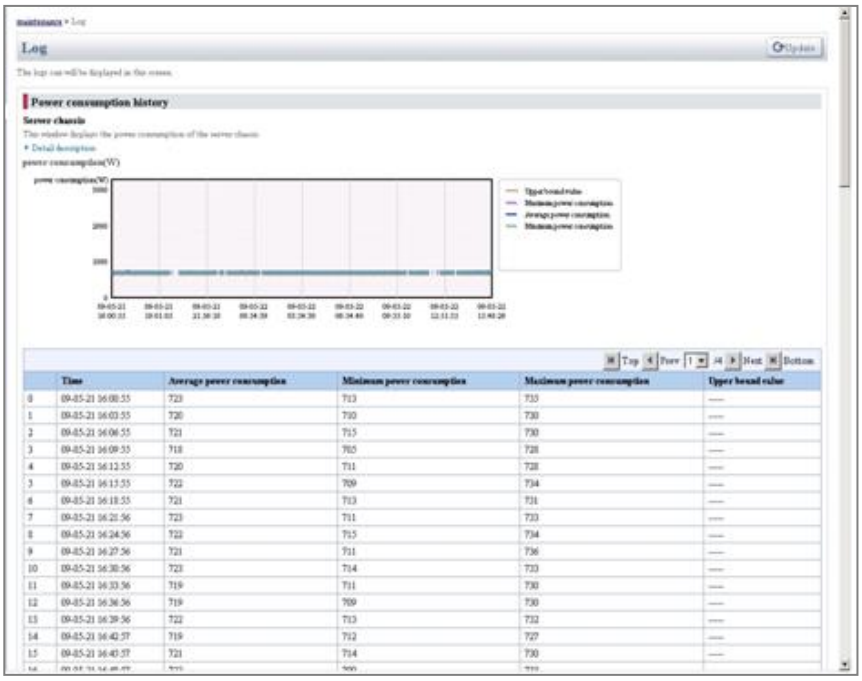
#	Item	Description	Edit
1	Time	The time (in local time) when the event was recorded.	
2	ID	Log ID (alert ID).	
3	Level	The alert level.	
4	Message	The event message.	

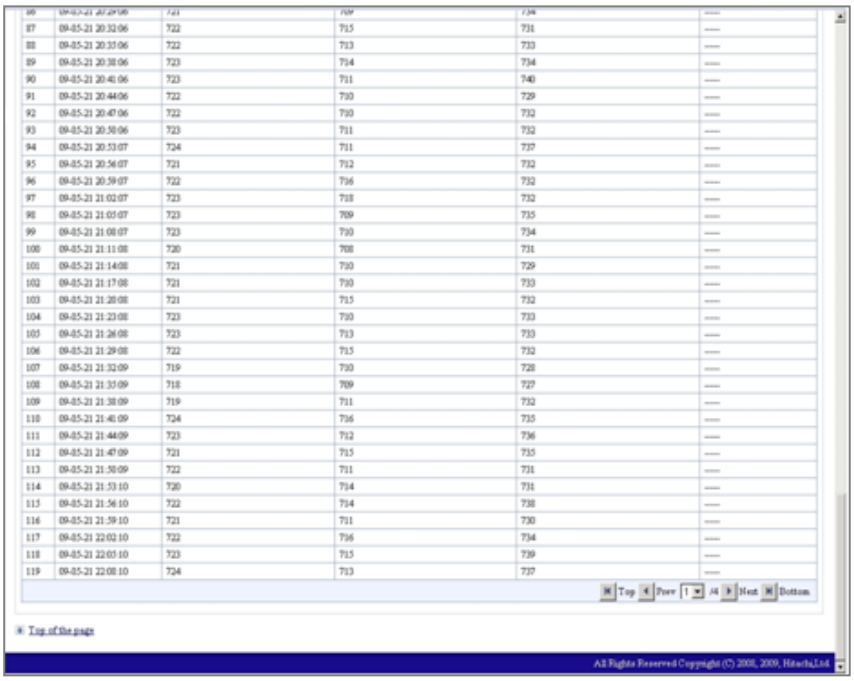
❑ System event log display view



#	Item	Description	Edit
1	Time	The time (in local time) when the event was recorded.	
2	Module	The module that generated the event.	
3	Level	The level of the System Event.	
4	System event log	The event data.	
5	Message	The translation of the event data.	

❑ Power status trend view (chassis)



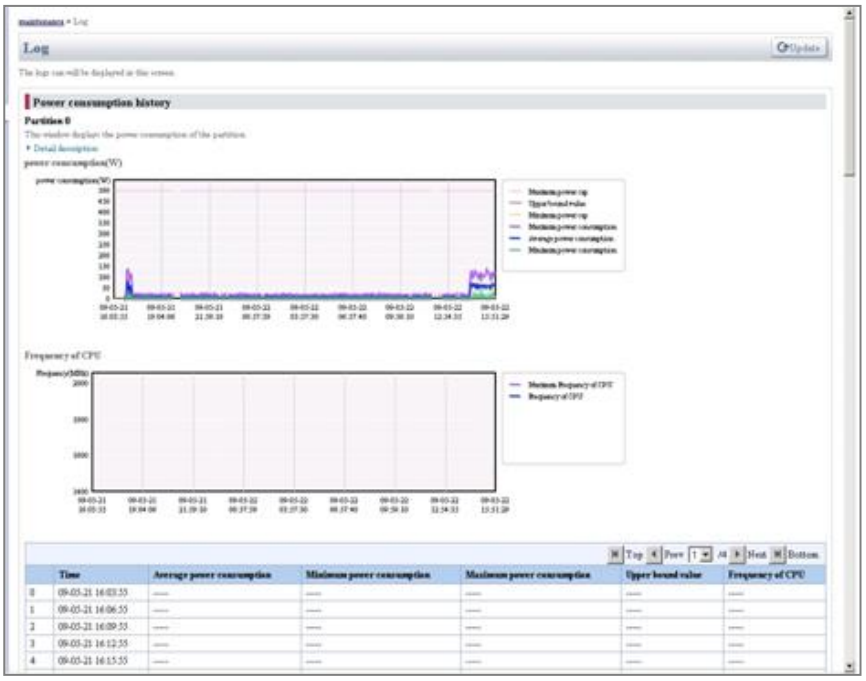


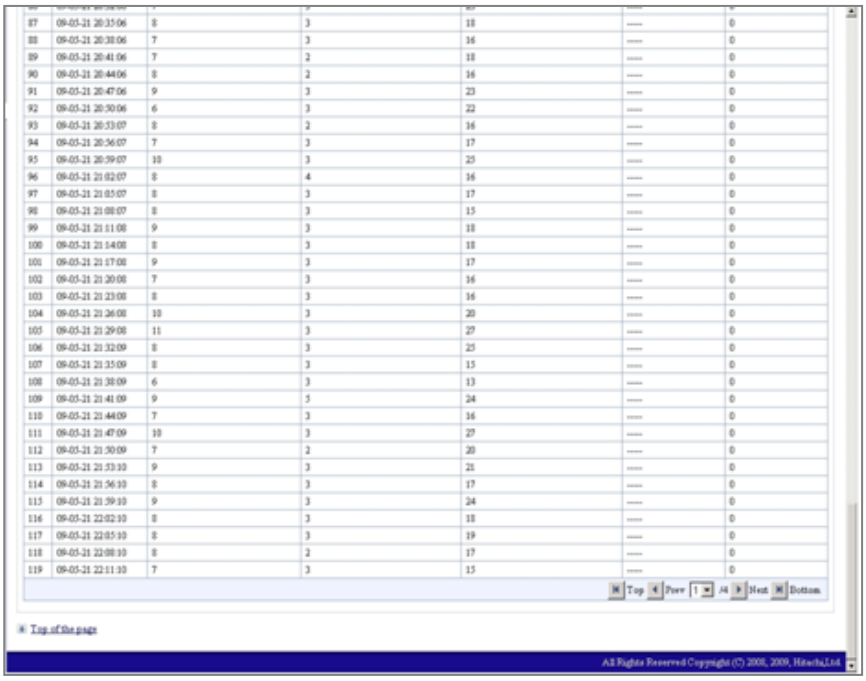
Tip

For Internet Explorer 8 or higher, enable the browser compatibility view. If not, the graph might not display correctly.

#	Item	Description	Edit
1	Time	The time (in local time) when the status was recorded.	
2	Average power consumption	The mean power consumption (DC output) of the server chassis (in watts).	
3	Minimum power consumption	The minimum power consumption (DC output) of the server chassis (in watts).	
4	Maximum power consumption	The maximum power consumption (DC output) of the server chassis (in watts).	
5	Upper bound value	The upper limit imposed on the power consumption of the server chassis (in watts).	

❑ Power status trend view (partition)



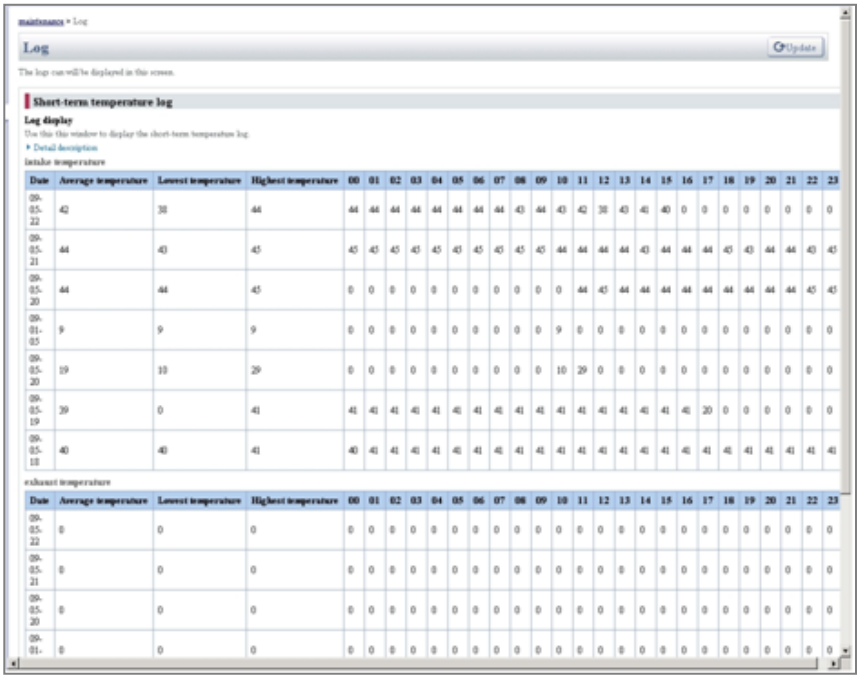


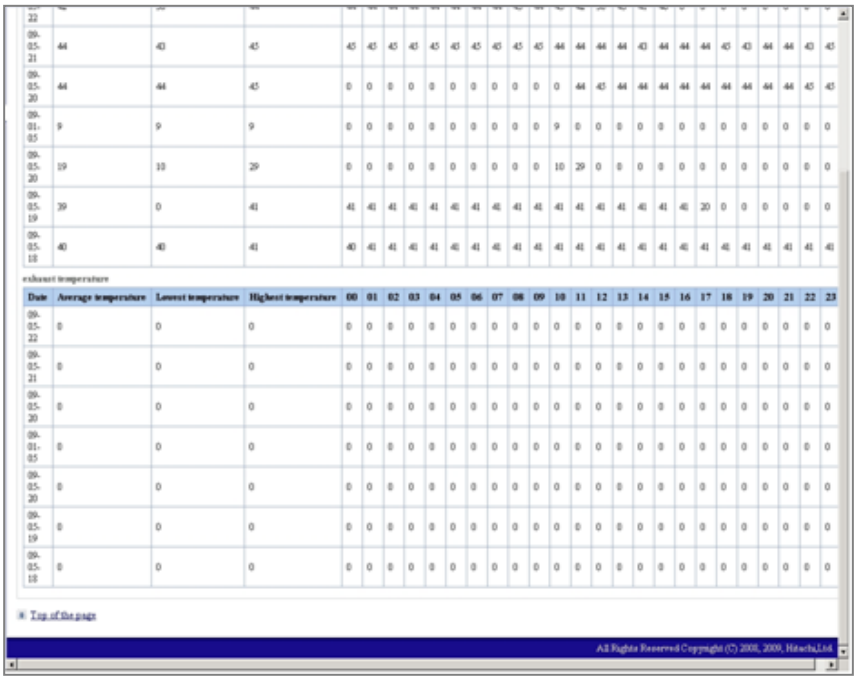
#	Item	Description	Edit
1	Time	The time (in local time) when the log was recorded.	
2	Average power consumption	The mean power consumption of the physical partition (in watts).	
3	Minimum power consumption	The minimum power consumption of the physical partition (in watts).	
4	Maximum power consumption	The maximum power consumption of the physical partition (in watts).	
5	Upper bound value	The upper limit imposed on the power consumption of the physical partition (in watts).	
6	Frequency of CPU	The latest CPU operating frequency (in MHz) of the server blade associated with the physical partition, measured over a three-minute sampling period.	

Tip

For Internet Explorer 8 or later, enable the browser compatibility view. If not, the graph might not display correctly.

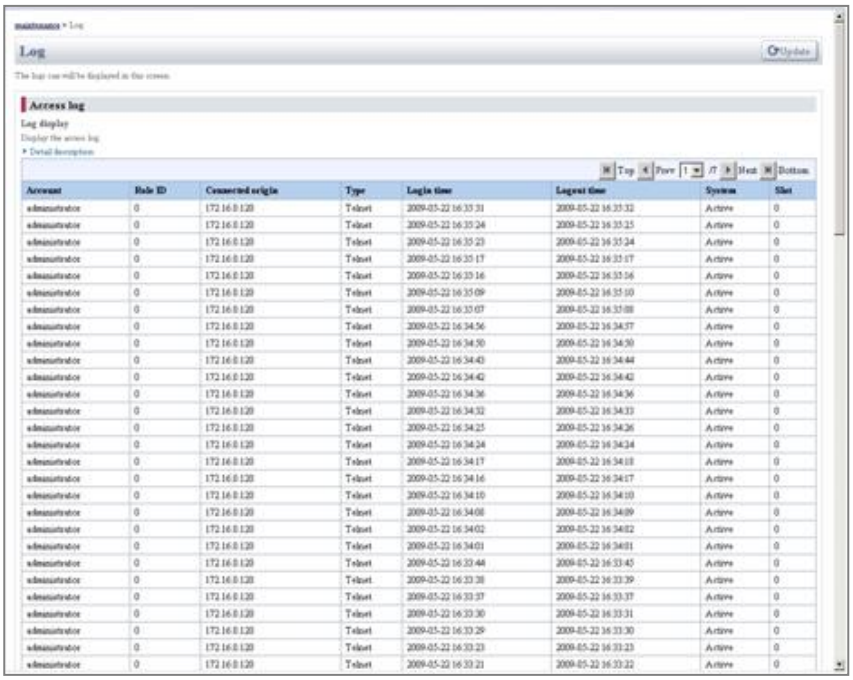
❑ Short-term environment log display view

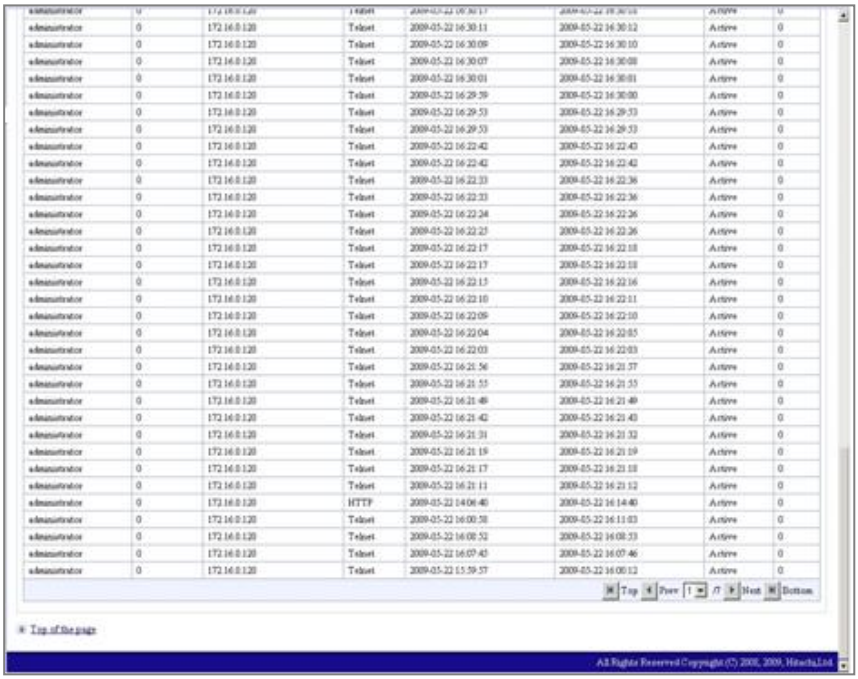




#	Item	Description	Edit
1	Date	The date (in local time) when the data was recorded.	
2	Average temperature	The average temperature reported by the temperature sensor on that day. Temperature readings are in degrees Celsius.	
3	Lowest temperature	The minimum temperature reported by the temperature sensor on that day. Temperature readings are in degrees Celsius.	
4	Highest temperature	The maximum temperature reported by the temperature sensor on that day. Temperature readings are in degrees Celsius.	
5	00 to 23	The average temperature reported hour by hour by the temperature sensor. Temperature readings are in degrees Celsius.	

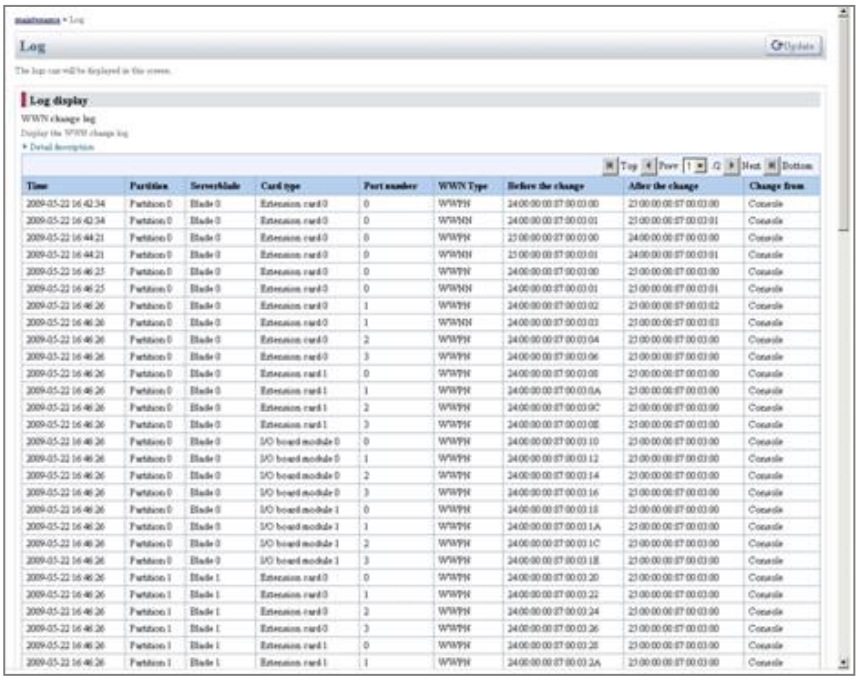
❑ Access log display view





#	Item	Description	Edit
1	Account	The names of the user accounts that established connections to the management module.	
2	Role ID	The name of the role assigned to the user account.	
3	Connected origin	The IP address from which the user connected to the management module. No IP address is displayed for serial connections.	
4	Type	The protocol used to connect to the management module. Displayed as: Serial, Telnet, SSH, or HTTP	
5	Login time	The time when the user logged in.	
6	Logout time	The time when the user logged out.	
7	System	Indicates whether the management module to which the user logged in is serving as an active or standby system. Set as: Active or Standby	
8	Slot	The management module slot to which the user logged in. Set as: 0 or 1	

❑ WWN change log display view



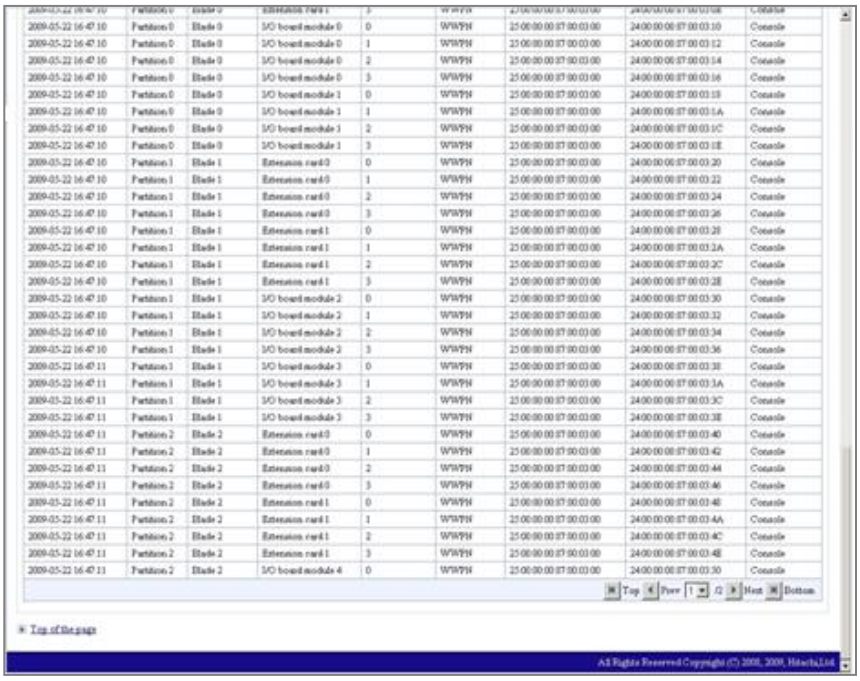
Log

Update

Log display

WWN change log

Time	Partition	Server blade	Card type	Port number	WWN Type	Before the change	After the change	Change from
2009-05-22 16:42:34	Partition 0	Blade 0	Extension card 0	0	WWPN	24:00:00:00:87:00:03:00	23:00:00:00:87:00:03:00	Console
2009-05-22 16:42:34	Partition 0	Blade 0	Extension card 0	0	WWNN	24:00:00:00:87:00:03:01	23:00:00:00:87:00:03:01	Console
2009-05-22 16:44:21	Partition 0	Blade 0	Extension card 0	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:00	Console
2009-05-22 16:44:21	Partition 0	Blade 0	Extension card 0	0	WWNN	23:00:00:00:87:00:03:01	24:00:00:00:87:00:03:01	Console
2009-05-22 16:46:25	Partition 0	Blade 0	Extension card 0	0	WWPN	24:00:00:00:87:00:03:00	23:00:00:00:87:00:03:00	Console
2009-05-22 16:46:25	Partition 0	Blade 0	Extension card 0	0	WWNN	24:00:00:00:87:00:03:01	23:00:00:00:87:00:03:01	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 0	1	WWPN	24:00:00:00:87:00:03:02	23:00:00:00:87:00:03:02	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 0	1	WWNN	24:00:00:00:87:00:03:03	23:00:00:00:87:00:03:03	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 0	2	WWPN	24:00:00:00:87:00:03:04	23:00:00:00:87:00:03:04	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 0	3	WWPN	24:00:00:00:87:00:03:06	23:00:00:00:87:00:03:06	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 1	0	WWPN	24:00:00:00:87:00:03:08	23:00:00:00:87:00:03:08	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 1	1	WWPN	24:00:00:00:87:00:03:0A	23:00:00:00:87:00:03:0A	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 1	2	WWPN	24:00:00:00:87:00:03:0C	23:00:00:00:87:00:03:0C	Console
2009-05-22 16:46:26	Partition 0	Blade 0	Extension card 1	3	WWPN	24:00:00:00:87:00:03:0E	23:00:00:00:87:00:03:0E	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 0	0	WWPN	24:00:00:00:87:00:03:10	23:00:00:00:87:00:03:10	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 0	1	WWPN	24:00:00:00:87:00:03:12	23:00:00:00:87:00:03:12	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 0	2	WWPN	24:00:00:00:87:00:03:14	23:00:00:00:87:00:03:14	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 0	3	WWPN	24:00:00:00:87:00:03:16	23:00:00:00:87:00:03:16	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 1	0	WWPN	24:00:00:00:87:00:03:18	23:00:00:00:87:00:03:18	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 1	1	WWPN	24:00:00:00:87:00:03:1A	23:00:00:00:87:00:03:1A	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 1	2	WWPN	24:00:00:00:87:00:03:1C	23:00:00:00:87:00:03:1C	Console
2009-05-22 16:46:26	Partition 0	Blade 0	I/O board module 1	3	WWPN	24:00:00:00:87:00:03:1E	23:00:00:00:87:00:03:1E	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 0	0	WWPN	24:00:00:00:87:00:03:20	23:00:00:00:87:00:03:20	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 0	1	WWPN	24:00:00:00:87:00:03:22	23:00:00:00:87:00:03:22	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 0	2	WWPN	24:00:00:00:87:00:03:24	23:00:00:00:87:00:03:24	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 0	3	WWPN	24:00:00:00:87:00:03:26	23:00:00:00:87:00:03:26	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 1	0	WWPN	24:00:00:00:87:00:03:28	23:00:00:00:87:00:03:28	Console
2009-05-22 16:46:26	Partition 1	Blade 1	Extension card 1	1	WWPN	24:00:00:00:87:00:03:2A	23:00:00:00:87:00:03:2A	Console



2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 0	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:10	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 0	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:12	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 0	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:14	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 0	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:16	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 1	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:18	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 1	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:1A	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 1	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:1C	Console
2009-05-22 16:47:10	Partition 0	Blade 0	I/O board module 1	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:1E	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 0	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:20	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 0	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:22	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 0	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:24	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 0	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:26	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 1	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:28	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 1	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:2A	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 1	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:2C	Console
2009-05-22 16:47:10	Partition 1	Blade 1	Extension card 1	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:2E	Console
2009-05-22 16:47:10	Partition 1	Blade 1	I/O board module 2	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:30	Console
2009-05-22 16:47:10	Partition 1	Blade 1	I/O board module 2	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:32	Console
2009-05-22 16:47:10	Partition 1	Blade 1	I/O board module 2	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:34	Console
2009-05-22 16:47:10	Partition 1	Blade 1	I/O board module 2	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:36	Console
2009-05-22 16:47:11	Partition 1	Blade 1	I/O board module 3	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:38	Console
2009-05-22 16:47:11	Partition 1	Blade 1	I/O board module 3	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:3A	Console
2009-05-22 16:47:11	Partition 1	Blade 1	I/O board module 3	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:3C	Console
2009-05-22 16:47:11	Partition 1	Blade 1	I/O board module 3	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:3E	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 0	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:40	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 0	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:42	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 0	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:44	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 0	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:46	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 1	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:48	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 1	1	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:4A	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 1	2	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:4C	Console
2009-05-22 16:47:11	Partition 2	Blade 2	Extension card 1	3	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:4E	Console
2009-05-22 16:47:11	Partition 2	Blade 2	I/O board module 4	0	WWPN	23:00:00:00:87:00:03:00	24:00:00:00:87:00:03:50	Console

Top of the page

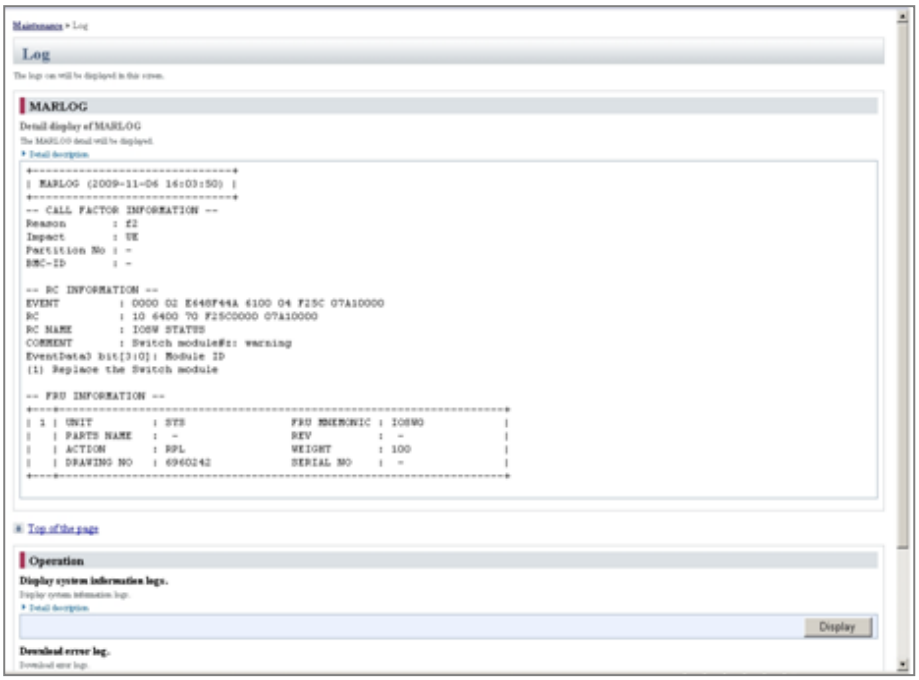
All Rights Reserved Copyright (C) 2008, 2009, Hitachi,Ltd.

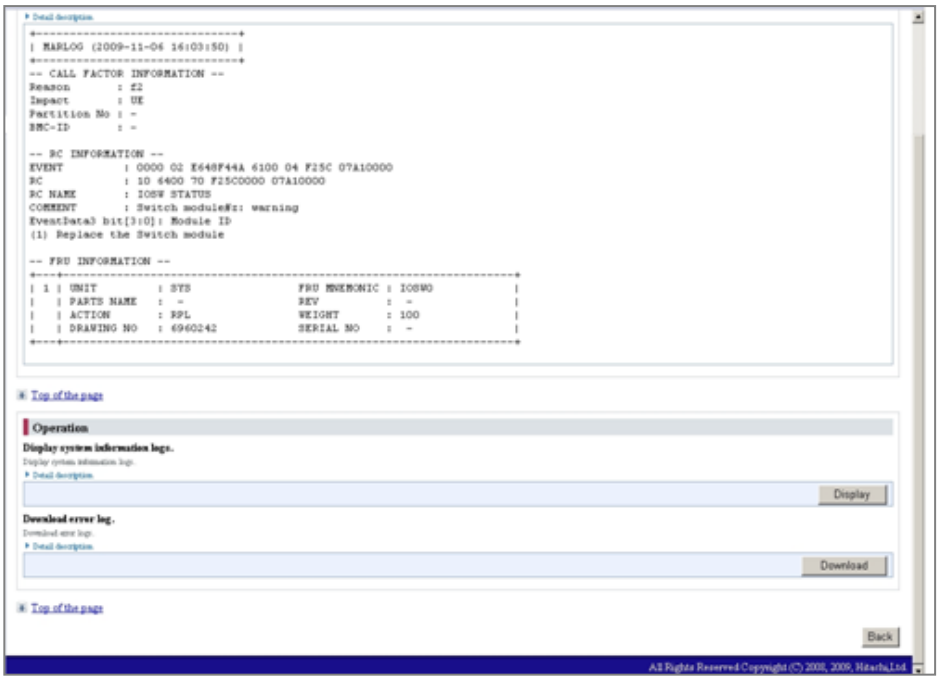
#	Item	Description	Edit
1	Time	The date and time (in local time) when the WWN change was recorded.	
2	Partition	The physical partition number.	
3	Server blade	The server blade number.	
4	Card type	The type of card: Mezzanine cards and I/O adapters For the I/O adapter on the I/O slot expansion unit, displays which I/O slot expansion unit the I/O adapter is connected to.	
5	Port number	The port number.	
6	WWN Type	The WWN type: WWPN or WWNN	
7	Before the change	The WWN of the device before the change was made.	
8	After the change	The WWN of the device after the change was made.	

❑ Role-dependent variation in available operations

To display and use the Log management views, the user must have chassis permission.

Detail display of MARLOG





#	Item	Description	Edit
1	Display system information logs Display button	Displays the selected MARLOG system information logs.	-
2	Download error log Download button	Downloads the error logs when the selected MARLOG is collected.	-

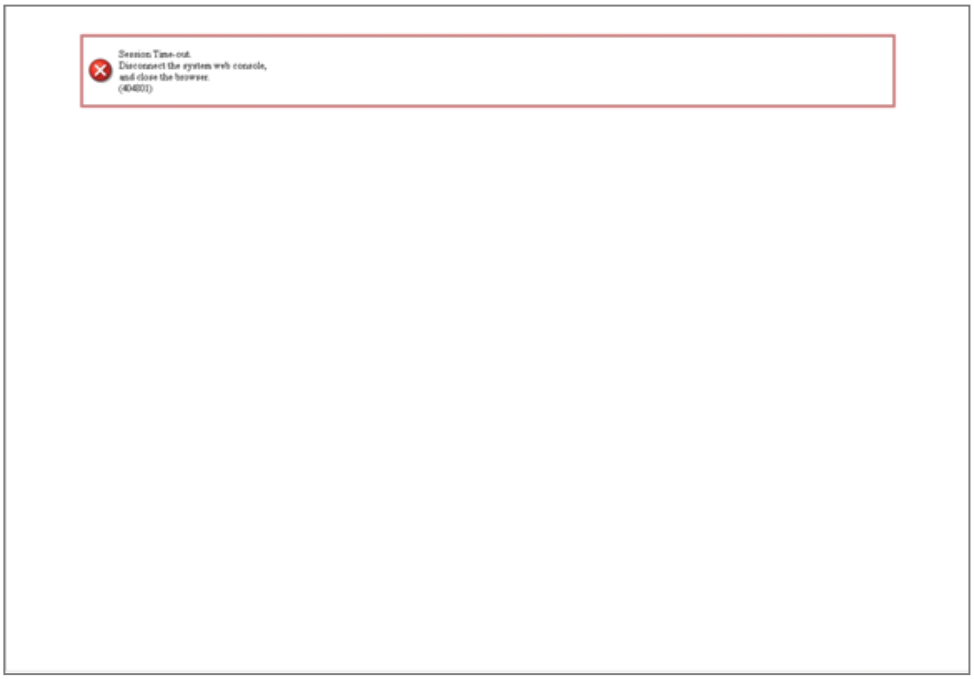
❑ Role-dependent variation in available operations

To display and use the Detail display of MARLOG, the user must have chassis permission.

Error pages

When an error occurs in the system web console, an error page is displayed.

❑ Session timeout



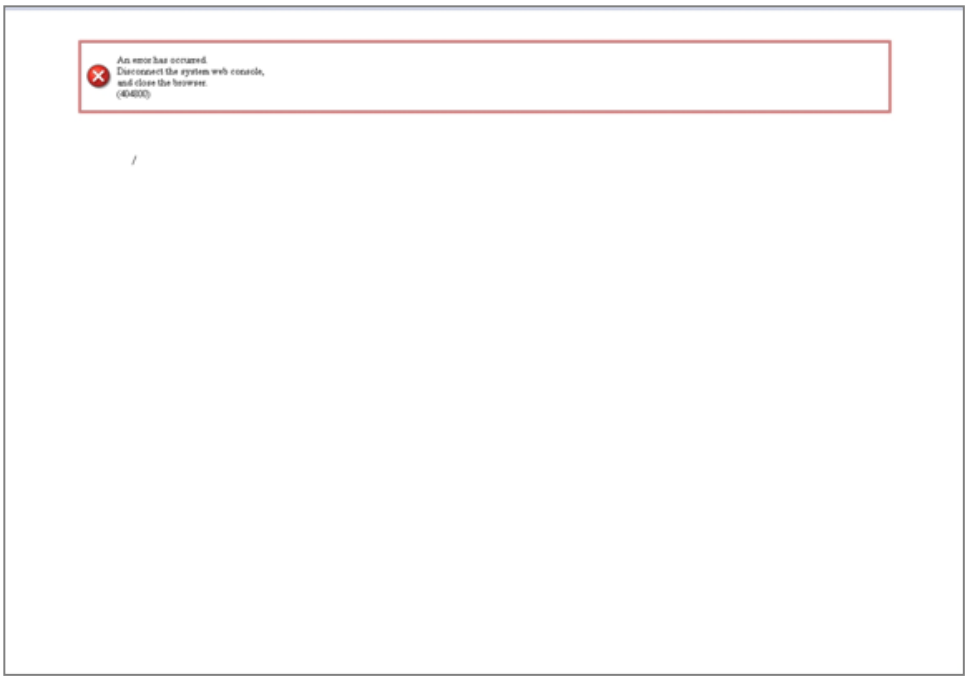
Indicates that the current session has timed out. Close your browser window.

You can establish a new session by logging in again from a new browser window.

A session may time out in the following situations:

- The user did not perform any action in the system web console for a specific period of time (set in the Console Setup view).
- The session was closed.

❑ Internal error



Indicates that an operation performed through the system web console resulted in an error in the internal processing of the management module. Close the browser window.

You can establish a new session by logging in again from a new browser window.

SVP (Service Processor Log) message

(1) Overview of SVP log

The SVP log stores the alerts notified directly to ServerConductor/Blade Server Manager (hereafter referred to as BSM) by the service processor.

The SVP log can be viewed from the BSM console, through the management module's "System Console Command Reference" or from the "System Web Console".

(2) Format of SVP log messages (viewed from the management module serial console)

```
Timestamp           ID    Level   Message
------------------- ----  ------- --------------------
YYYY-MM-DD hh:mm:ss XXXX  XXXXXXX ********************
YYYY-MM-DD hh:mm:ss XXXX  XXXXXXX ********************
```

Timestamp

The date and time when the log message was generated, in the format YYYY (year) – MM (month) – DD (day) hh (hour) – mm (minutes) – ss (seconds)

ID

The message ID

Level

The level of the message: Info (information message), WARNING (warning message), or FAIL (error message)

Message

A message is shown. “%s” in a message stands for characters.

(3) List of messages

ID	Level	Message
Description		
1483	FAIL	Partition <%s1>, Error alert (immediate replacement) is sent by the user request operation.
Meaning: A test of the N+M cold standby function (immediate failover) was performed on the partition indicated by %s1. Action: No particular action is required as the message relates to a test.		
1484	FAIL	Partition <%s1>, Error alert (delayed replacement) is sent by the user request operation.
Meaning: A test of the N+M cold standby function (other than immediate failover) was performed on the partition indicated by %s1. Action: No particular action is required as the message relates to a test.		
14E3	Info	System information update alert is sent.
Meaning: Device information was updated. Upon receiving this alert, BSM will update its internal management information by acquiring the latest information from the management module. Action: No particular action is required.		
14E4	Info	Module information update alert is sent.
Meaning: Module information was updated. Upon receiving this alert, BSM will update its internal management information by acquiring the latest information from the management module. Action: No particular action is required.		
14E5	Info	Module information update alert is sent (error/degradation).
Meaning: Upon receiving this alert, BSM will update its internal management information by acquiring the latest information from the management module. No particular action is required.		
14EA	Info	The BMC IP address of the server blade indicated by %s was updated.
Meaning: Upon receiving this alert, BSM will update its internal management information by acquiring the latest information from the management module. Action: No particular action is required.		
14EB	Info	Partition <%s1>, pre-boot configuration started (Data %s2 procedure).
Meaning: A Smart Configure process was begun on the partition indicated by %s1. %s2 indicates the type of smart configuration being performed. acquisition: Smart Configure for acquiring information from a server blade setting: Smart Configure for setting information on a server blade diagnosis: Smart Configure for testing a server blade Action: No particular action is required.		
14EC	Info	Partition <%s1>, pre-boot configuration completed (Data %s2 procedure).
Meaning: A Smart Configure process ended on the partition indicated by %s1. %s2 indicates the type of smart configuration that was performed (see 14EB). Action: No particular action is required.		
142C	Info	On partition <%s1>, a power-saving event of the server blade was logged. ID=(0x%s2)

ID	Level	Message
Description		
Meaning: An event related to an energy-saving feature was recorded for the partition indicated by %s1. ID indicates the event type. 0x3f: A power consumption value was set. 0x41: The maximum power consumption was changed. 0x42: The minimum power consumption was changed. 0x80: The power consumption limit was changed. Action: No particular action is required.		
142D	WARNING	On partition <%s1>, an attention event related to power-saving of the server blade was logged. ID=(0x%s2)
Meaning: A significant event related to an energy-saving feature was recorded for the partition indicated by %s1. ID indicates the event type. 0x11: Power consumption remained above the power consumption limit for a pre-defined period. 0x12: The partition is operating at the minimum power consumption because the power consumption limit is set below the minimum power consumption value. Action: Review the power control settings as required.		
1470	FAIL	Partition <%s1>, Watchdog timer has expired.
Meaning: A watchdog timer timed out on the partition indicated by %s1. The partition will restart. If the N+M cold standby function is enabled for the partition, processing will fail over to the standby server. Action: Contact your reseller or maintenance personnel.		
1620	Info	On physical partition <%s1>, startup of LP was halted because non-LP compatible server blades exist in the configuration.
Meaning: LPAR manager cannot start because a server blade in the physical partition indicated by %s1 lacks a valid LPAR manager license. Action: Check the LPAR manager license type and whether the license is present and valid. If LPAR manager does not start and this message is output despite the server blade having a valid license, contact your reseller or maintenance personnel.		
1621	Info	On physical partition <%s>, a LP dump was logged.
Meaning: LPAR manager dump was collected from the partition indicated by %s. Action: No action is required.		
1622	FAIL	On physical partition <%s1>, an error that is fatal to the system occurred in LP.
Meaning: A critical error on the physical partition indicated by %s1 caused the system to shut down. Action: Contact your reseller or maintenance personnel.		
1623	FAIL	On physical partition <%s1>, an error occurred in LP.
Meaning: An LPAR manager error occurred on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1624	FAIL	On physical partition <%s1>, an error occurred in LP assist.
Meaning: An error LPAR manager assist error occurred on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1625	FAIL	On physical partition <%s1>, an error occurred in an LPAR.
Meaning: An LPAR error occurred on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1626	FAIL	On physical partition <%s1>, an error that is fatal to the system occurred due to an H/W failure.

ID	Level	Message
Description		
Meaning: A hardware failure and subsequent error on the physical partition indicated by %s1 caused the system to shut down. Action: Contact your reseller or maintenance personnel.		
1627	FAIL	On physical partition <%s1>, an error occurred in LP due to an H/W failure.
Meaning: A hardware failure caused an LPAR manager error on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1628	FAIL	On physical partition <%s1>, an error occurred in LP assist due to an H/W failure.
Meaning: A hardware failure caused an LPAR manager assist error on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1629	FAIL	On physical partition <%s1>, an error occurred in the LPAR due to an H/W failure.
Meaning: A hardware failure caused an LPAR error on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
162F	WARNING	On physical partition <%s>, a communication error occurred between LP and the management module.
Meaning: An error occurred on the physical partition indicated by %s during communication between LPAR manager and the management module. Action: Contact your reseller or maintenance personnel.		
1631	WARNING	On physical partition <%s1>, LP disabled a processor core.
Meaning: LPAR manager placed a faulty processor in the physical partition indicated by %s1 in a degraded state. Action: Contact your reseller or maintenance personnel.		
1632	FAIL	On physical partition <%s1>, LP detected a physical BMC access error.
Meaning: LPAR manager detected an access error with the physical BMC on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1633	FAIL	In CPU <%s2> on physical partition <%s1>, a fatal error occurred.
Meaning: An error occurred in the processor indicated by %s2 on the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1634	WARNING	In CPU <%s2> on physical partition <%s1>, the number of error corrections exceeded the limit.
Meaning: The number of processor-corrected errors in the processor indicated by %s2 in the physical partition indicated by %s1 has exceeded the maximum. Action: Contact your reseller or maintenance personnel.		
1637	FAIL	On physical partition <%s1>, activation of the shared NIC <%s2> failed.
Meaning: The shared NIC %s2 in the physical partition indicated by %s1 could not be initialized, rendering communication through that NIC impossible. Action: Contact your reseller or maintenance personnel.		
1638	FAIL	On physical partition <%s1>, activation of the shared NIC <%s2> failed.

ID	Level	Message
Description		
Meaning: The shared NIC %s2 in the physical partition indicated by %s1 could not be enabled, rendering communication through that NIC impossible. Action: Contact your reseller or maintenance personnel.		
163A	WARNING	On physical partition <%s1>, a link on shared NIC <%s2> is down.
Meaning: The link to the shared NIC %s2 in the physical partition indicated by %s1 is down. Action: Check the connection to the shared NIC. If the problem is not resolved, contact your reseller or maintenance personnel.		
163E	WARNING	On physical partition <%s1>, an interface error occurred on the shared Fibre-channel <%s2>.
Meaning: An interface error occurred in the shared FC %s2 in the physical partition indicated by %s1. Action: Check the connection to the shared FC. If the problem is not resolved, contact your sales or service representative.		
163F	WARNING	On physical partition <%s1>, a link on shared Fibre-channel <%s2> is down.
Meaning: The link to the shared FC %s2 in the physical partition indicated by %s1 is down. Action: Check the connection to the shared FC. If the problem is not resolved, contact your sales or service representative.		
1642	WARNING	On physical partition <%s1>, a recoverable H/W failure occurred on the shared Fibre-channel <%s2>
Meaning: A temporary hardware error occurred in the shared FC %s2 in the physical partition indicated by %s1. Action: Contact your sales or service representative.		
1643	FAIL	On physical partition <%s1>, a non-recoverable H/W failure occurred on the shared Fibre-channel <%s2>.
Meaning: A persistent hardware error occurred in the shared FC %s2 in the physical partition indicated by %s1. Action: Contact your sales or service representative.		
1644	FAIL	On physical partition <%s1>, a PCI bus error occurred on the shared Fibre-channel <%s2>.
Meaning: A PCI bus error occurred in the shared FC %s2 in the physical partition indicated by %s1. Action: Contact your sales or service representative.		
1645	WARNING	On physical partition <%s1>, an error occurred in the flash memory for LP.
Meaning: LPAR manager encountered an access error when accessing the LPAR manager flash memory in the physical partition indicated by %s1. Action: Contact your reseller or maintenance personnel.		
1646	WARNING	On physical partition <%s>, LP disabled a part of memory.
Meaning: LPAR manager degraded memory at the physical partition %s. Action: Contact your reseller or maintenance personnel.		
1700	Info	On module <%s1>, the temperature <%s2> exceeded the normal level.
Meaning: The temperature of the component indicated by %s2 in the module indicated by %s1 is above a reference value, but has not yet reached a warning threshold. Action: No particular action is required because the temperature is not at a level that will affect system operation. However, if this message recurs, make sure that the equipment's cooling is not impaired.		
1701	WARNING	On module <%s1>, the temperature <%s2> exceeded the warning level.

ID	Level	Message
Description		
Meaning: The temperature of the component indicated by %s2 in the module indicated by %s1 is above a warning threshold. Action: Although the module can continue operating, a higher warning level (1702) may be reached at any time. Make sure that the equipment's cooling is not impaired. Impaired cooling may be caused by inadequate air conditioning, a malfunctioning fan module, or blocked vents in the equipment.		
1702	FAIL	On module <%s1>, the temperature <%s2> rose too far above tolerable levels.
Meaning: The temperature of the component indicated by %s2 in the module indicated by %s1 is exceedingly high. Action: The affected module may be shut down to protect its hardware. Contact your sales or service representative. Also, make sure that the equipment's cooling is not impaired. Impaired cooling may be caused by inadequate air conditioning, a malfunctioning fan module, or blocked vents in the equipment.		
1703	WARNING\	On module <%s1>, the temperature <%s2> fell below the warning level.
Meaning: The temperature of the component indicated by %s2 in the module indicated by %s1 is below a warning threshold. Action: The module can continue operating, but check the temperature at the installation site.		
1705	Info	On module <%s1>, the temperature <%s2> has been restored to a tolerable level.
Meaning: The temperature of the component indicated by %s2 in the module indicated by %s1 is below a warning threshold. Action: This message indicates recovery from a problem, and no particular action is required.		
1710	WARNING	On module <%s1>, the voltage <%s2> exceeded the warning level.
Meaning: The voltage at the component indicated by %s2 in the module indicated by %s1 is above a warning threshold. Action: Although the module can continue operating, a higher warning level (1711) may be reached at any time. Contact your sales or service representative.		
1711	FAIL	On module <%s1>, the voltage <%s2> rose too far above tolerable levels.
Meaning: The voltage at the component indicated by %s2 in the module indicated by %s1 is exceedingly high. Action: The affected module may be shut down to protect its hardware. Contact your sales or service representative		
1712	FAIL	On module <%s1>, the voltage <%s2> became abnormal.
Meaning: An abnormal voltage value is detected at the component indicated by %s2 in the module indicated by %s1. Action: The affected module may be shut down to protect its hardware. Contact your sales or service representative.		
1713	WARNING	On module <%s1>, the voltage <%s2> became abnormal.
Meaning: The voltage at the component indicated by %s2 in the module indicated by %s1 is below a warning threshold. Action: Although the module can continue operating, a higher warning level (1714) may be reached at any time. Contact your sales or service representative.		
1714	FAIL	On module <%s1>, the voltage <%s2> became abnormal.
Meaning: The voltage at the component indicated by %s2 in the module indicated by %s1 is below a warning threshold. Action: Although the module can continue operating, a higher warning level (1714) may be reached at any time. Contact your sales or service representative.		
1715	Info	On module <%s1>, the voltage <%s2> has been restored to a

ID	Level	Message
Description		
		normal level.
Meaning: The voltage at the component indicated by %s2 in the module indicated by %s1 has recovered to a level within the reference range. Action: This message indicates recovery from a problem, and as such no particular action is required.		
1720	Info	On module <%s1>, the temperature of the CPU <%s2> exceeded the normal level.
Meaning: The temperature of the CPU indicated by %s2 in the module indicated by %s1 is above a reference value, but has not yet reached a warning threshold. Action: No particular action is required because the temperature is not at a level that will affect system operation. However, if this message recurs, make sure that the equipment's cooling is not impaired.		
1721	WARNING	On module <%s1>, the temperature of the CPU <%s2> exceeded the warning level.
Meaning: The temperature of the CPU indicated by %s2 in the module indicated by %s1 is above a warning threshold. Action: Although the module can continue operating, a higher warning level (1722) may be reached at any time. Make sure that the equipment's cooling is not impaired. Impaired cooling may be caused by inadequate air conditioning, a malfunctioning fan module, or blocked vents in the equipment.		
1722	FAIL	On module <%s1>, the temperature of the CPU <%s2> became abnormal.
Meaning: An abnormal temperature value is detected at the CPU indicated by %s2 in the module indicated by %s1. Action: The affected module may be shut down to protect its hardware. Contact your sales or service representative. Also, make sure that the equipment's cooling is not impaired. Impaired cooling may be caused by inadequate air conditioning, a malfunctioning fan module, or blocked vents in the equipment.		
1723	Info	On module <%s1>, the temperature of the CPU <%s2> has been restored to a normal level.
Meaning: The temperature of the CPU indicated by %s2 in the module indicated by %s1 has recovered to a level within the reference range. Action: This message indicates recovery from a problem, and as such no particular action is required.		
1730	FAIL	On module <%s1>, an error occurred in CPU <%s2>.
Meaning: An error occurred in the CPU indicated by %s2 in the module indicated by %s1. Action: Contact your sales or service representative.		
1731	WARNING	On module <%s1>, an error occurred in CPU <%s2>.
Meaning: An error occurred in the CPU indicated by %s2 in the module indicated by %s1. Action: Contact your sales or service representative.		
1732	WARNING	On module <%s1>, CPU <%s2> is disabled.
Meaning: The CPU indicated by %s2 in the module indicated by %s1 is running in a degraded state. Action: The system can continue to operate but with reduced performance. Contact your sales or service representative.		
1733	WARNING	On module <%1$s>, core of the CPU <%2$s> is disabled.
Meaning: The CPU indicated by %s2 in the module indicated by %s1 is in a degraded state. Action: Contact your reseller or maintenance personnel.		
1734	FAIL	On module <%s1>, an error occurred in the internal HDD.

ID	Level	Message
Description		
Meaning: An error occurred in the internal HDD of the module indicated by %s1. Action: Contact your sales or service representative.		
1738	Info	On module <%s1>, a 1-bit error correction occurred in the memory.
Meaning: A recoverable error occurred in the memory of the module indicated by %s1, and the error was successfully corrected. Action: No particular action is required.		
1739	FAIL	On module <%s1>, a 2-bit error occurred in the memory.
Meaning: An unrecoverable error occurred in the memory of the module indicated by %s1. Action: Contact your sales or service representative.		
173A	WARNING	On module <%s1>, the number of 1-bit error corrections exceeded the limit.
Meaning: A recoverable error occurred in the memory of the module indicated by %s1. Although the error was successfully corrected, the maximum number of recoverable errors has been exceeded. Action: The system can continue to operate, but may develop a fault that causes unrecoverable errors in the future. Contact your sales or service representative.		
173B	WARNING	On module <%s1>, part of the installed memory was disabled.
Meaning: The memory of the module indicated by %s1 was found to be partially defective, and the module was started with the defective memory isolated. Action: The system can continue to operate but with reduced performance. Contact your sales or service representative.		
173C	WARNING	On module <%s1>, the fuse (for I/O) on the motherboard has blown.
Meaning: The fuse indicated by %s2 on the board in the module indicated by %s1 has blown. Action: Contact your sales or service representative.		
173F	FAIL	On module <%s1>, an abnormal event occurred.
Meaning: A fault occurred in the module indicated by %s1. Action: Contact your sales or service representative.		
1740	WARNING	On module <%s1>, an abnormal event occurred.
Meaning: A fault occurred in the module indicated by %s1. Action: Contact your sales or service representative.		
1741	Info	On module <%s1>, the abnormal event was corrected.
Meaning: The module indicated by %s1 recovered from a fault. Action: No particular action is required.		
1742	WARNING	On module <%s1>, an AC input error occurred.
Meaning: A power supply problem was detected in the module indicated by %s1. Action: Make sure that the power supply to the equipment (at the breaker or wall socket) is normal. If the power supply is normal, contact your sales or service representative.		
1743	Info	On module <%s1>, the AC input error has been corrected.
Meaning: Power has been restored to the module indicated by %s1. Action: No particular action is required.		
1744	WARNING	On module <%s1>, the fan rotation speed is abnormally high or low.
Meaning: A fault has occurred in the fan module indicated by %s1. Action: Contact your sales or service representative.		
1745	Info	On module <%s1>, the fan rotation speed has been restored a normal level.
Meaning: The fan module indicated by %s1 recovered from a fault. Action: No particular action is required.		

ID	Level	Message
Description		
1747	WARNING	On module <%s1>, an access error to <%s2> occurred.
Meaning: A communication error identified by %s2 occurred in the module indicated by %s1. Action: If the communication error was temporary, this message is followed by a recovery message (ID: 1748). In this case, no action is required. If the recovery message does not appear in the log, contact your sales or service representative.		
1748	Info	On module <%s1>, the access error to <%s2> has been corrected.
Meaning: The module indicated by %s1 recovered from the communication error identified by %s2. Action: No particular action is required.		
1749	WARNING	On module <%s1>, POWER-ON is inhibited.
Meaning: The supply of power to the module indicated by %s1 is suppressed. Potential causes are: A configuration problem or invalid setting (such as an invalid hardware combination or inadequate power supply). Power supply is suppressed so that a maintenance task can take place (the module is under maintenance or faulty). Action: Resolve the problem causing the suppression. If the reason why the power supply is being suppressed remains unclear, contact your sales or service representative.		
174A	FAIL	On partition <%s>, An error occurred in FibreChannel card.
Meaning: An error occurred in a Fibre-channel card on the partition indicated by %s. Action: Contact your sales or service representative.		
174B	FAIL	On partition <%s>, A link down occurred in FibreChannel card.
Meaning: A linkdown occurred in a Fibre-channel card on the partition indicated by %s. Action: Contact your sales or service representative.		
174C	WARNING	On partition <%s>, A warning event occurred in FibreChannel card.
Meaning: A failure occurred in a Fibre-channel card on the partition indicated by %s. Action: Contact your sales or service representative.		
174D	Info	On partition <%s>, FibreChannel card has recovered from an error.
Meaning: A Fibre-channel card on the partition indicated by %s has recovered from an error. . Action: Contact your sales or service representative.		
174F	FAIL	On partition <%s>, An error occurred in PCI card.
Meaning: An error occurred in a PCI card on the partition indicated by %s. Action: Contact your sales or service representative.		
1750	Info	On partition <%s1>, POWER-ON is starting.
Meaning: Power was turned on for the partition indicated by %s1. Action: No particular action is required.		
1751	Info	On partition <%s1>, RESET is occurring.
Meaning: The partition indicated by %s1 was reset. Action: No particular action is required.		
1752	Info	On partition <%s1>, POWER-OFF is starting.
Meaning: Power was shut off for the partition indicated by %s1. Action: No particular action is required.		
1753	Info	On partition <%s1>, an NMI was issued.
Meaning: A non-maskable interrupt (NMI) was issued in the partition indicated by %s1. Action: No particular action is required.		
1754	Info	On partition <%s1>, the panel button was pressed, and an NMI was

ID	Level	Message
Description		
		issued.
Meaning: A non-maskable interrupt (NMI) was issued in the partition indicated by %s1. Action: No particular action is required.		
1756	FAIL	On partition <%s1>, the system failed to start.
Meaning: An attempt to turn on the power for the partition indicated by %s1 failed. Action: Contact your sales or service representative.		
1757	Info	On partition <%s1>, POWER-ON due to a scheduled POWER-ON request is starting.
Meaning: Power was turned on for the partition indicated by %s1 according to a schedule set from BSM. Action: No particular action is required.		
1758	Info	On partition <%s1>, POWER-ON due to a request from the management server is starting.
Meaning: Power was turned on for the partition indicated by %s1 as a result of a request issued from BSM. Action: No particular action is required.		
1759	Info	On partition <%s1>, forced POWER-OFF due to a request from the management server is starting.
Meaning: Power was shut off for the partition indicated by %s1 as a result of a request issued from BSM. Action: No particular action is required.		
175A	FAIL	On partition <%s>, An error occurred in LAN card.
Meaning: An error occurred in a LAN card on the partition indicated by %s failed. Action: Contact your sales or service representative.		
175B	FAIL	On partition <%s>, A link down occurred in LAN card.
Meaning: A linkdown occurred in a LAN card on the partition indicated by %s failed. Action: Contact your sales or service representative.		
175C	WARNING	On partition <%s>, A warning event occurred in LAN card.
Meaning: A failure occurred in a LAN card on the partition indicated by %s failed. Action: Contact your sales or service representative.		
175D	Info	On partition <%s>, LAN card has recovered from an error.
Meaning: A LAN card on the partition %s has recovered from an error. Action: No particular action is required.		
1760	Info	On partition <%s1>, the time in the BMC was updated.
Meaning: The BMC time was updated on the partition indicated by %s1. Action: No particular action is required.		
1761	Info	On partition <%s1>, the schedule data was updated.
Meaning: A scheduling setting was updated in the partition indicated by %s1. Action: No particular action is required.		
1770	Info	On partition <%s1>, the server blade BMC logged an event.
Meaning: An event was recorded in the partition indicated by %s1. Action: No particular action is required.		
1771	WARNING	On partition <%s1>, the server blade BMC logged a warning.
Meaning: A warning was recorded in the partition indicated by %s1. Action: Contact your sales or service representative.		
1772	FAIL	On partition <%s1>, the server blade BMC logged an error.

ID	Level	Message
Description		
Meaning: A failure was recorded in the partition indicated by %s1. Action: Contact your sales or service representative.		
1778	Info	On partition <%s1>, the server blade firmware logged an event.
Meaning: An event was recorded in the partition indicated by %s1. Action: No particular action is required.		
1779	WARNING	On partition <%s1>, the server blade firmware logged a warning.
Meaning: A warning was recorded in the partition indicated by %s1. Action: Contact your sales or service representative.		
177A	FAIL	On partition <%s1>, the server blade firmware logged an error.
Meaning: A failure was recorded in the partition indicated by %s1. Action: Contact your sales or service representative.		
1780	Info	On partition <%s1>, the server blade BMC restarted.
Meaning: The server blade BMC was restarted on the partition indicated by %s1. Action: No particular action is required.		
1788	FAIL	On partition <%s1>, a failure requiring an immediate N+M cold standby failover occurred.
Meaning: A failure which is subject to immediate failover by the N+M cold standby function occurred on the partition indicated by %s1. The affected partition will now fail over to its counterpart in the standby system. Action: Contact your sales or service representative.		
1789	FAIL	On partition <%s1>, a failure requiring a delayed N+M cold standby failover occurred.
Meaning: A failure which is subject to delayed failover by the N+M cold standby function occurred on the partition indicated by %s1. The affected partition will now fail over to its counterpart in the standby system. Action: Contact your sales or service representative.		
178C	FAIL	On partition <%s1>, a failure occurred in <%s2> during Pre-configure.
Meaning: In the partition indicated by %s1, a failure occurred during a Smart Configure process in the component indicated by %s2. Action: Contact your sales or service representative.		
178D	WARNING	On partition <%s1>, an invalid setting was found in <%s2> during Pre-configure.
Meaning: A Smart Configure process in the partition indicated by %s1 failed because the component indicated by %s2 was set up incorrectly. Action: %s2 is an HBA slot number or a port number. Review and amend the HBA BIOS settings for the specified slot, and then manually run the Smart Configure process. If the same message appears again, contact your sales or service representative.		
178E	FAIL	On partition <%s1>, a Pre-configure error was detected.
Meaning: A failure was detected in a Smart Configure process running on the partition indicated by %s1. Action: Contact your sales or service representative.		
178F	WARNING	On partition <%s1>, an error occurred when Pre-configure was being performed.
Meaning: An error occurred during execution of a Smart Configure process on the partition indicated by %s1. Action: Contact your sales or service representative.		
1790	Info	Module <%s1> was installed.

ID	Level	Message
Description		
Meaning: The module indicated by %s1 was installed. Action: No particular action is required.		
1791	Info	Module <%s1> was removed.
Meaning: The module indicated by %s1 was removed. Action: No particular action is required.		
1792	Info	Module <%s1> restored redundancy.
Meaning: The module indicated %s1 is operating in a redundant configuration. Action: No particular action is required.		
1793	WARNING	Module <%s1> lacks redundancy.
Meaning: The module indicated %s1 is no longer operating in a redundant configuration. Action: The module can continue operating, but lacks redundancy. Contact your sales or service representative.		
1794	FAIL	Module <%s1> an insufficient quantity of this module is installed.
Meaning: There are too few of the modules indicated by %s1 in the system. The system will shut down if there are no longer enough power supply modules or fan modules in operation. Action: Make sure that the modules indicated by %s1 are installed correctly, and then contact your sales or service representative.		
1799	FAIL	A system configuration error was found.
Meaning: There is a problem with the system configuration. Action: If you changed an aspect of the system configuration before the message was output, check whether there is a problem with the change you made. If there is nothing wrong with the configuration, contact your sales or service representative.		
179A	WARNING	A warning about the system configuration was detected.
Meaning: There is a problem with the system configuration. Action: If you changed an aspect of the system configuration before the message was output, check whether there is a problem with the change you made. If there is nothing wrong with the configuration, contact your sales or service representative.		
17A0	WARNING	LAN port <%s1> lacks redundancy.
Meaning: The LAN port indicated by %s1 is no longer operating in a redundant configuration. Action: Check the connection to the specified LAN port. The network status may cause the LAN port to temporarily lose redundancy. If this message is followed by the recovery message 17A1, the problem is resolved.		
17A1	Info	LAN port <%s1> redundancy was restored.
Meaning: The LAN port indicated by %s1 is again operating in a redundant configuration. Action: No particular action is required.		
17A2	Info	LAN port <%s1> has switched to another port.
Meaning: When redundancy is enabled for the LAN port indicated by %s1, this message indicates that data will now be routed through an alternate path. Action: If this message appears on its own, then the LAN port is working with the redundancy intact and no action is required. If the message 17A0 is also output, check the connection status of the specified LAN port.		
17A3	Info	LAN port <%s1> has recovered from an error.
Meaning: The alternate routing implemented with message 17A2 has returned to its former state. Action: No particular action is required.		
17A8	WARNING	Sending out an e-mail report message failed. It will be retried.

ID	Level	Message
Description		
Meaning: Email notification has failed. Wait for the retry. Action: Make sure that the management module can communicate with the email server. Also, review the email notification settings, and correct any problems you find.		
17A9	WARNING	Sending out an e-mail report message failed.
Meaning: Email notification has failed. Action: Make sure that the management module can communicate with the email server. Also, review the email notification settings, and correct any problems you find.		
17AA	Info	Collecting error data for an e-mail report failed.
Meaning: An attempt to collect data for email notification failed. Some data may be missing from the email attachment. Action: No particular action is required, but contact your sales or service representative if the message recurs.		
17AB	Info	Sending out an e-mail report message succeeded.
Meaning: The e-mail was successfully sent. Action: No particular action is required.		
17AE	Info	The time limit for transmitting and receiving an SVP alert has been exceeded.
Meaning: Attempts to exchange alert data with the BSM failed, and retry attempts were unsuccessful for the duration of the retry period. Alerts issued during this period have not reached the BSM. Action: Check whether communication is possible between the BSM server and the management module. Also, review the BSM connection settings, and correct any problems you find. Message 17E0 is output when communication is restored. If a comparison of the alert messages at the BSM console and the SVP log messages shows that some have not reached the BSM console, take the recommended action for those messages.		
17B0	Info	The time of the management module was updated.
Meaning: The system time was changed on the management module. Action: No particular action is required.		
17B1	WARNING	The management module failed to connect to the NTP server.
Meaning: The management module failed to connect to the NTP server. Action: Check whether communication is possible between the management module and the NTP server. Check the NTP server settings in the management module. Make sure that the time is set correctly on the management module.		
17B2	Info	The management module restored connection to the NTP server.
Meaning: The connection between the management module and the NTP server has recovered. Action: Make sure that the time is set correctly on the management module.		
17B4	WARNING	On HA monitor (cluster <%s>), a communication error occurred in the reset path between management modules.
Meaning: A communication error has occurred in the reset path between management modules on HA monitor cluster %s. Action: Check whether or not communication between the indicated management module and management module as a cluster manager is available. If the HA monitor settings has some trouble, correct it. When the communication is recovered, ID: 17B5 is output.		
17B5	Info	On HA monitor (cluster <%s>), a communication error in the reset path between management modules was corrected.
Meaning: A communication error in the reset path between management modules on the HA monitor was corrected on HA monitor cluster %s. Action: No particular action is required.		

ID	Level	Message
Description		
17B6	WARNING	On HA monitor (cluster <%s>), cluster manager is suspended because other cluster managers exist.
Meaning: Multiple cluster managers exist on the HA monitor cluster %s. Action: Correct the HA monitor setting to set a cluster manager to a cluster. Then, resume the HA monitor from the cluster manager to confirm that this message is not output.		
17B7	WARNING	On HA monitor (cluster <%s>), there is a management module whose cluster management is not enabled.
Meaning: management modules with the cluster management feature disabled exist on the HA monitor cluster %s. Action: Correct the HA monitor setting to enable the cluster management feature in all management module.		
17C0	Info	The management module logged an event.
Meaning: An event was recorded on the management module. Action: No particular action is required.		
17C1	WARNING	The management module logged a warning.
Meaning: A warning-level error has occurred on the management module. Action: Contact your sales or service representative.		
17C2	FAIL	The management module logged an error.
Meaning: A failure-level error has occurred on the management module. Action: Contact your sales or service representative.		
17D0	Info	On partition <%s1>, updating the server blade BMC F/W has started.
Meaning: The process of updating the server blade firmware has begun on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: Do not connect to or operate the indicated partition until the update process has completed.		
17D1	Info	On partition <%s1>, updating the server blade BMC F/W has completed.
Meaning: The process of updating the server blade firmware has completed on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: No particular action is required.		
17D2	Info	On partition <%s1>, updating the server blade F/W has started.
Meaning: The process of updating the server blade firmware has begun on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: Do not connect to or operate the indicated partition until the update process has completed.		
17D3	Info	On partition <%s1>, updating the server blade F/W completed.
Meaning: The process of updating the server blade firmware has completed on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: No particular action is required.		
17D4	Info	Updating the management module F/W has started.
Meaning: The process of updating the management module firmware has begun. The nature of the maintenance task may cause this message to be output multiple times. Action: Do not connect to or operate the management module until the update process has completed.		
17D5	Info	Updating the management module F/W completed.

ID	Level	Message
Description		
Meaning: The process of updating the management module firmware has completed. The nature of the maintenance task may cause this message to be output multiple times. Action: No particular action is required.		
17DC	Info	On module <%s1>, maintenance mode was set.
Meaning: A maintenance task has begun on the module indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: A maintenance task is in progress on the indicated module. Do not connect to or operate the indicated module until the task has completed.		
17DD	Info	On module <%s1>, maintenance mode was cancelled.
Meaning: A maintenance task has completed on the module indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: No particular action is required.		
17DE	Info	On the partition <%s1>, maintenance mode was set.
Meaning: A maintenance task has begun on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: A maintenance task is in progress on the indicated partition. Do not connect to or operate the indicated partition until the task has completed.		
17DF	Info	On the partition <%s1>, maintenance mode was cancelled.
Meaning: A maintenance task has completed on the partition indicated by %s1. The nature of the maintenance task may cause this message to be output multiple times. Action: No particular action is required.		
17E0	Info	The management module sent out a connection request alert.
Meaning: The management module issued a connection request to the BSM. Action: No particular action is required.		
17E2	Info	The IP address of the management module changed.
Meaning: The IP address of the management module has been changed. Action: No particular action is required.		

HCSM (Hitachi Compute Systems Manager) alert message

(1) Table headings of HCSM alert messages

ID: Message ID

Level: Level of the message: Information; Warning; Error

Message: Alert messages are shown. “X” and “Y” in a message stands for character strings.

(2) List of alert messages

ID	Level	Message
Description and Action		
FD00	Warning	Temperature of chassis became warning level. (Temp(X),Location:Y)
Description: The temperature of the location shown as Y has reached Warning level. X shows either Upper (high temperature) or Lower (low temperature) at warning level. Action: Check if anything interferes with the cooling system since the state may go up to a higher error level, FD01, although you can keep operations running. When finding some factors interfering with cooling, such as a malfunction in the cooling equipment or in fan modules in the system, and dust-covered intake, remove the problem factor. If the temperature does not return to the normal when you have removed it, contact your reseller or maintenance personnel.		
FD01	Error	Temperature of chassis became error level. (Temp(X),Location:Y)
Description: The temperature of the location shown as Y has reached Error level. X shows either Upper (high temperature) or Lower (low temperature) at error level. Action: The specified module may be stopped for hardware protection. Contact your reseller or maintenance personnel. Check if anything interferes with the cooling system. When finding some factors interfering with cooling, such as a malfunction in the cooling equipment or in fan modules in the system, and dust-covered intake, remove the problem factor. If the temperature does not return to the normal when you have removed it, contact your reseller or maintenance personnel.		
FD02	Information	Temperature of chassis has been restored to a normal level. (Temp(X),Location:Y)
Description: The temperature of the location shown as Y has recovered to the normal level. X shows either Upper (high temperature) or Lower (low temperature) at error or warning level. Action: None. This is a recovery message.		
FD03	Warning	Temperature of CPU became warning level. (Temp(X),Location:Y)
Description: The temperature of the CPU in Location Y has reached Warning level. X shows either Upper (high temperature) or Lower (low temperature) at warning level. Action: Check if anything interferes with the cooling system since the state may go up to a higher error level, FD04, although you can keep operations running. When finding some factors interfering with cooling, such as malfunction in the cooling equipment or in fan modules in the system, and dust-covered intake, remove the problem factor. If the temperature does not return to the normal when you have removed it, contact your reseller or maintenance personnel.		
FD04	Error	Temperature of CPU became error level. (Temp(X),Location:Y)

ID	Level	Message
Description and Action		
Description: The temperature of the CPU in Location Y has reached Error level. X shows either Upper (high temperature) or Lower (low temperature) at error level. The specified module may be stopped for hardware protection. Action: The specified module may be stopped for hardware protection. Contact your reseller or maintenance personnel. Check if anything interferes with the cooling system. When finding some factors interfering with cooling, such as malfunction in the cooling equipment or in fan modules in the system, and dust-covered intake, remove the problem factor. If the temperature does not return to the normal when you have removed it, contact your reseller or maintenance personnel.		
FD05	Information	Temperature of CPU has been restored to a normal level. (Temp(X),Location:Y)
Description: The temperature of the CPU in Location Y has recovered to the normal level. X shows either Upper (high temperature) or Lower (low temperature) at error or warning level. Action: None. This is a recovery message.		
FD10	Warning	Voltage became warning level. (Voltage(X), Location:Y)
Description: The voltage of the location shown as Y has reached Warning level. X shows either Upper (high voltage) or Lower (low voltage) at warning level. Action: The state may go up to a higher error level, FD11, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD11	Error	Voltage became error level. (Voltage(X), Location:Y)
Description: The voltage of the location shown as Y has reached Error level. X shows either Upper (high voltage) or Lower (low voltage) at error level. Action: The specified module may be stopped for hardware protection. Contact your reseller or maintenance personnel.		
FD12	Information	Voltage has been restored to a normal level. (Voltage(X),Location:Y)
Description: The voltage of the location shown as Y has recovered to the normal level. X shows either Upper (high voltage) or Lower (low voltage) at error or warning level. Action: None. This is a recovery message.		
FD30	Information	Module is installed. (Location:X)
Description: The module shown in Location X is installed. Action: None.		
FD31	Information	Module is removed. (Location:X)
Description: The module shown in Location X is removed. Action: None.		
FD38	Error	Watchdog timer has expired. (Location:X)
Description: A watchdog timeout is detected in Location X. Action: Contact your reseller or maintenance personnel.		
FD40	Warning	On server, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the server blade. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD41	Error	On server, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the server blade. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD42	Information	Server has been restored to a normal level. (Location:X,Event:Y)
Description: The server blade has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		

ID	Level	Message
Description and Action		
FD43	Warning	On physical partition, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the server blade. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD44	Error	On physical partition, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the server blade. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD46	Warning	On power supply, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the power supply module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD47	Error	On power supply, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the power supply module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD48	Information	Power supply has been restored to a normal level. (Location:X,Event:Y)
Description: The power supply module has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		
FD49	Warning	On cooling fan, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the cooling fan module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD4A	Error	On cooling fan, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the cooling fan module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD4B	Information	Cooling fan has been restored to a normal level. (Location:X,Event:Y)
Description: The cooling fan module has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		
FD4C	Warning	On switch module, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the switch module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD4D	Error	On switch module, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the switch module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD4E	Information	Switch module has been restored to a normal level. (Location:X,Event:Y)
Description: The switch module has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		
FD50	Error	On disk, an error event occurred. (Location:X,Event:Y)

ID	Level	Message
Description and Action		
Description: An error event has occurred in the HDD. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD51	Information	Disk has been restored to a normal level. (Location:X,Event:Y)
Description: The HDD has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		
FD52	Warning	On management module, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in the management module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD53	Error	On management module, an error event occurred. (Location:X,Event:Y)
Description: An error event has occurred in the management module. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD54	Information	Management module has been restored to a normal level. (Location:X,Event:Y)
Description: The management module has recovered to the normal state. X shows a position that the event occurred; Y describes the event. Action: None. This is a recovery message.		
FD58	Warning	On other module, a warning event occurred. (Location:X,Event:Y)
Description: A warning event has occurred in other than server blades, power supply modules, cooling fan modules, switch modules, HDDs, and management modules. X shows a position that the event occurred; Y describes the event. Action: Contact your reseller or maintenance personnel.		
FD60	Warning	The cooling fan rotation speed is abnormally high or low. (Location:X)
Description: RPM of the cooling fan module shown in Location X indicates an improper value. Action: Contact your reseller or maintenance personnel.		
FD61	Information	The cooling fan rotation speed has been restored a normal level. (Location:X)
Description: RPM of the cooling fan module shown in Location X has recovered to the normal state. Action: None. This is a recovery message.		
FD64	Warning	On chassis, an AC input is lost. (Location:X)
Description: AC power is lost in the power supply module shown in Location X. Action: Check the AC power supply. If the AC power is properly supplied, contact your reseller or maintenance personnel.		
FD65	Information	On chassis, the AC input error has been corrected. (Location:X)
Description: AC power supply has recovered to the power supply module shown in Location X. Action: None. This is a recovery message.		
FD68	Error	Uncorrectable CPU error occurred. (Location:X)

ID	Level	Message
Description and Action		
Description: An uncorrectable error has occurred in the CPU in Location X. Action: Contact your reseller or maintenance personnel.		
FD69	Warning	Corrected CPU error threshold exceeded. (Location:X)
Description: A correctable error, which occurred in the CPU in Location X, was corrected. But the number of those errors that occurred has gone beyond the threshold. Action: The error may become an uncorrectable one, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD6B	Error	Uncorrectable memory error occurred. (Location:X)
Description: An uncorrectable memory error has occurred in the memory shown in Location X. Action: Contact your reseller or maintenance personnel.		
FD6C	Warning	Corrected memory error threshold exceeded. (Location:X)
Description: A correctable error, which occurred in the memory shown in Location X, was corrected. But the number of correctable errors that occurred has gone beyond the threshold. Action: The error may become an uncorrectable one, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD70	Warning	CPU is disabled. (Location:X)
Description: The CPU shown in Location X is disabled. Action: Performance slows down, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD71	Warning	Memory is disabled. (Location:X)
Description: The CPU shown in Location X is disabled. Action: Performance slows down, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD78	Warning	Module lacks redundancy. (Location:X)
Description: Redundancy for the module shown in Location X is lost. Action: Redundancy is lost, although you can keep operations running. Contact your reseller or maintenance personnel.		
FD79	Information	Module restored redundancy. (Location:X)
Description: Redundancy is restored to the module shown in Location X. Action: None. This is a recovery message.		
FD7F	Information	Event is logged. (Location:X,Event:Y)
Description: The event that occurred in Location X is logged. Y indicates the event logged. Action: None.		
FD85	Warning	On server, power-on is inhibited. (Location:X)
Description: Power on is not available to the server blade shown in Location X. Possible causes: Problems with configuration and settings, including incorrect hardware configuration and lack of power. When maintenance is being performed, the server blade is targeted for maintenance, or power to the server blade with error is controlled. Action: Find and solve the problem to stop power on. If the problem is unknown, contact your reseller or maintenance personnel.		
FD90	Information	Server is powered on. (Location:X)
Description: The server blade shown in Location X is powered on. Action: None.		
FD91	Information	Server is powered off. (Location:X)

ID	Level	Message
Description and Action		
Description: The server blade shown in Location X is powered off. Action: None.		
FD92	Information	Server is reset. (Location:X)
Description: The server blade shown in Location X is reset. Action: None.		
FD93	Error	Server failed to power-on. (Location:X)
Description: The server blade shown in Location X failed to power on. Action: Contact your reseller or maintenance personnel.		
FD9C	Information	Switch module is powered on. (Location:X)
Description: The switch module shown in Location X is powered on. Action: None.		
FD9D	Information	Switch module is powered off. (Location:X)
Description: The switch module shown in Location X is powered off. Action: None.		
FD9F	Error	Switch module failed to power-on. (Location:X)
Description: The switch module shown in Location X failed to power on. Action: Contact your reseller or maintenance personnel.		
FDA8	Information	Power supply is powered on. (Location:X)
Description: The power supply module shown in Location X is powered on. Action: None.		
FDA9	Information	Power supply is powered off. (Location:X)
Description: The power supply module shown in Location X is powered off. Action: None.		
FDAB	Error	Power supply failed to power-on. (Location:X)
Description: The power supply module shown in Location X failed to power on. Action: Contact your reseller or maintenance personnel.		
FDAC	Warning	Power supply failed to power-off. (Location:X)
Description: The server blade shown in Location X failed to power off. Action: Contact your reseller or maintenance personnel.		
FDAE	Information	Management module is powered on. (Location:X)
Description: The management module shown in Location X is powered on. Action: None.		
FDAF	Information	Management module is powered off. (Location:X)
Description: The management module shown in Location X is powered off. Action: None.		
FDBA	Information	Panel button was pressed, and NMI was issued. (Location:X)
Description: NMI was issued from the server blade shown in Location X. Action: None.		
FDC0	Information	Time is updated. (Location:X)
Description: Time is updated in the module shown in Location X. Action: None.		
FDC8	Information	Updating firmware has started. (Location:X)
Description: Firmware update has started on the module shown in Location X . Action: None.		
FDC9	Information	Updating firmware has completed. (Location:X)

ID	Level	Message
Description and Action		
Description: Firmware update has completed on the module shown in Location X. Action: None.		
FDD0	Warning	Warning about the system configuration is detected.
Description: The system configuration has problems. Action: When you have changed the system configuration before the message appears, check if there is anything wrong with the change. If there was no change in the configuration or nothing wrong with the changed configuration, contact your reseller or maintenance personnel.		
FDD1	Error	System configuration error is detected.
Description: The system configuration has problems. Action: When you have changed the system configuration before the message appears, check if there is something wrong with the change. If there was no change in the configuration or nothing wrong with the changed configuration, contact your reseller or maintenance personnel.		
FDD2	Warning	System power activation is deterred for system configuration error. (Location:X)
Description: Improper system configuration has deterred the system from powering on. Location X is unavailable for activation. Possible causes: Problems with configuration and settings, including incorrect hardware configuration and lack of power . When maintenance is being performed, the server blade is targeted for maintenance or power to the server blade with error is controlled. Action: Find and solve the problem to stop power on. If the problem is unknown, contact your reseller or maintenance personnel.		
FDD3	Error	Power supply capacity is insufficient.
Description: Power supply capacity is not enough. Action: Check if power supply modules are properly installed. If they are, contact your reseller or maintenance personnel.		
FDD5	Error	The total number of cooling fan modules is insufficient.
Description: The total number of cooling fan modules is not enough. Action: Check if cooling fan modules are properly installed. If they are, contact your reseller or maintenance personnel.		
FF05	Information	LAN port <X> has switched to another port.
Description: A LAN port shown as X, for which redundancy is enabled, has switched to another port. Action: When this message alone is displayed, there is no problem due to redundancy enabled. If FD78 is displayed together with this FF05, check connection of the specified LAN port. If the message is shown when the LAN cable is correctly attached and is not broken, follow the action shown in ID: FD78.		
FF06	Information	LAN port <X> has recovered from an error.
Description: The LAN port shown as X, which switched to another port in message ID: FF05, has switched back. Action: None.		
FF08	Warning	The synchronization of time is not performed. (Location:X)
Description: Time synchronization by NTP server is not performed in Location X. Action: Check if communication is available between the management module and NTP server. Also check the NTP server settings in the management module, and NTP server connection and settings. Check the time clock in the specified module, and correct the time if necessary.		

ID	Level	Message
Description and Action		
FF09	Information	The synchronization of time is resumed. (Location:X)
Description: Time synchronization by NTP server has resumed in Location X. Action: Check the time clock in the specified module, and correct the time if necessary.		
FF0B	Error	A report to a support center failed. (Report: x)
Description: A failure occurred at the communication function shown as x, and the support center is disconnected. Action: Contact maintenance personnel.		
FF0F	Information	A report is resumed. (Report:X)
Description: A report shown as X is resumed. Action: None.		
FF10	Information	Power saving event occurred. (Location:X,Event:Y)
Description: A power saving event shown as Y, which occurred in location X, is logged. Action: None.		
FF11	Warning	Power saving <warning> event occurred. (Location:X,Event:Y)
Description: A warning event for power saving shown as Y, which occurred in location X, is logged. Action: Check and correct settings for power saving if necessary. If the message is still shown without problems in the power saving settings, contact your reseller or maintenance personnel,		
FF18	Information	On <X>, maintenance mode is started.
Description: Maintenance work has started in Location X. This message may be displayed several times. Action: Since Location X is in maintenance mode, do not operate the module in Location X.		
FF19	Information	On <X>, maintenance mode is ended.
Description: Maintenance work has been completed in Location X. This message may be displayed several times. Action: None.		
FF22	Error	On <X>, a failure occurred in <Y> during smart configure.
Description: When a smart configure process is performed in the server blade shown in Location X, an error occurred in Location Y. Action: Contact your reseller or maintenance personnel.		
FF23	Warning	On <X>, an invalid setting was found in <Y> during pre-boot configuration.
Description: A smart configure process in the server blade shown in Location X failed due to incorrect settings in Location Y. Action: An HBA slot number and port number are shown in Y. Find and correct HBA BIOS settings in the specified slot. Then perform Smart Configure manually. If the same message is displayed after the correction, contact your reseller or maintenance personnel.		
FF24	Error	On <X>, a smart configure error was detected.
Description: An error was detected in Smart Configure on the server blade in Location X. Action: Contact your reseller or maintenance personnel.		
FF25	Warning	On <X>, an error occurred when smart configure was being performed.
Description: An error occurred when a smart configure process was being performed on the server blade in Location X. Action: Contact your reseller or maintenance personnel.		

ID	Level	Message
Description and Action		
FF28	Info	On <X>, error alert (immediate replacement) is sent by the user request operation.
Meaning: A test of the N+M cold standby function (immediate failover) was performed on the partition indicated by X. Action: No particular action is required as the message relates to a test.		
FF29	Info	On <X>, error alert is sent by the user request operation.
Meaning: A test of the N+M cold standby function (delayed failover) was performed on the partition indicated by X. Action: No particular action is required as the message relates to a test.		
FF2A	FAIL	On <X>, a failure requiring an immediate failover occurred.
Meaning: A failure which is subject to immediate failover by the N+M cold standby function occurred on the partition indicated by X. The affected partition will now fail over to its counterpart in the standby system. Action: Contact your sales or service representative.		
FF2B	FAIL	On <X>, a failure requiring a failover occurred.
Meaning: A failure which is subject to delayed failover by the N+M cold standby function occurred on the partition indicated by X. The affected partition will now fail over to its counterpart in the standby system. Action: Contact your sales or service representative.		
FFC0	Information	Management Module sent a connection request alert.
Description: The management module sent a connection request to HCSM. Action: None.		
FFC1	Information	Management Module sent a connection establishment alert.
Description: Connection between the management module and HCSM has established. Action: None.		
FFC2	Information	Management Module sent a keep-alive alert.
Meaning: This message is an alert for confirming connection between the management module and HCSM. Action: No particular action is required.		
FFC3	Information	On <X>, smart configure started (Data Y procedure).
[Description A smart configure process has started in the server blade shown in X. Y shows a type of smart configuration as follows. acquisition: Acquires information from the server blade. setting: Sets information in the server blade. diagnosis: Diagnoses problems in the server blade. Action: None.		
FFC4	Information	On <X>, smart configure succeeded (Data Y procedure).
Description:] Smart configuration has successfully completed in the server blade shown in X. Y shows a type of smart configuration. (See FFC3.) Action: None.		
FFC5	Information	On <X>, smart configure failed (Data Y procedure).
Description: Smart configuration has failed in the server blade shown in X. Y shows a type of smart configuration. (See FFC3.) Action: Another alert will be sent, describing the reason for failure. Follow the Action shown in the alert.		
FFCA	Information	The IP address of the management module changed.
Description: The management module IP address has been changed. Action: None.		

ID	Level	Message
Description and Action		
FFCB	Information	Module information of <X> changed.
Description: Information on the module shown as X has been updated. Action: None.		
FFCC	Information	Module information(constitution setting) of <X> changed.
Description: Information on the module shown as X has been updated. Action: None.		
FFCD	Information	System information changed.
Description: The system information has been updated. Action: None.		

Messages in the table above are shown when you use the management module firmware version A0360 or later and SEL dictionary version 00290 or later. With firmware earlier than A0360 or SEL dictionary earlier than 00290, some messages are different from those above.

7

Configuring the LAN switch module

This chapter provides important information on the system administrator's password setting that is required during initial installation, adding and deleting user IDs, and the module operations.

For the details concerning the operation of the local area network (LAN) switch module, see the manual in the CD-ROM that came with the compact disc- Read Only Memory (CD-ROM) switch module.

Notes on use 800
Connection to setup terminal 802
Command input mode overview 805
Initial installation operation overview 807
Backup and restore of module information 810
Connection with the server blades 813
Uplink failover overview 814
LAN switch module web console 816

Notes on use

⚠ CAUTION

- Do not look directly into the laser beam. Do not look into the laser beam using an optical instrument. 10GBASE-R transceiver uses laser beam that can damage your eyes, which is colorless, transparent, and invisible.
- Do not remove the cover of an unused board. Under the laser module cover, the laser beam is being emitted.

- In the default settings, the port of line 1 is configured for a dedicated virtual local area network (VLAN) for management and cannot communicate with a server blade and other external ports. Therefore, you need to change the switch settings suitable for your system configuration. After the changes, be sure to save the configuration information using the save command, otherwise, the data is lost when the system is powered off.
- In the default settings, the ports of line 5 to 12 and line 15 to 22 connected to the server blade are configured as edge ports (portfast). This setting aims to prevent the network from being affected by operations such as rebooting of the server blade. When you change the setting, it is recommended to set the port as edge port.
- The switch module is provided with Spanning tree as standard configuration. The external ports of line 2 to 4 cannot be communicated for 30 seconds after the cable is connected.
- A different type of LAN controller is installed in each server blade model. Connection ports for server blades, line 5 to 12 (slot 0 to 5) and line 15 to 22 (slot 2 to 5), are set by default as shown in the table below. Use a port setting value specific to each server blade to avoid communication errors.

Server blade model	Setting for server blade connection port
X55A1/X55A2/X57A1/X57A2: Models launched in or before March 2012	speed 1000 duplex full
X55R3/X55S3: Models launched in or after April 2012	speed auto* duplex auto*

* You need not specify the value in a configuration file because it is set before configuration.

- To restore the factory-set configuration, use one of the following methods:

  Enter the device manager mode and execute the erase configuration command.

  The CD attached to this device contains the *default file*.
  Apply the default file as described in "Restoring configuration (applying to startup-config)".
  In this case, use the “default” file according to “readme.txt” in the CD attached to this device.
- Since line 1 to line 4 of 10 Gbps LAN switch module and line 1 to line 4 of 1 Gbps LAN switch module are based upon Auto-MDI/MDI-X, both cross and straight cables are usable.

  This function is operational when auto negotiation is effective. Medium dependent interface crossover (MDI-X) is usable when fixed half duplex or fixed full duplex is specified.
- When connecting to the LAN switch module over the segment, make sure to set the default gateway. Set the static routing to set the default gateway of the LAN switch module. The example of the setting is shown below.

  ip route `0.0.0.0  0.0.0.0  192.168.1.1`

  `*: ”192.168.1.1”` is the address of the default gateway.

  For the detail about the ip route command, see “Configuration Command Reference Vol.2” in the CD-ROM attached to this device.
- The default configuration during shipment includes the management port settings to connect the LAN switch module to the management module.

Do not change or delete the management port setting because the management module might not be able to monitor.

- Note that from lines 13 to 24 (slot 0, 1), and lines 13, 14, 23, 24 (slot 2-5) in the LAN switch module cannot be used. Do not change the default configuration from shipment.
- Slots for the 10BASE-R are Line 25 and 26 on the 10 Gbps LAN switch module. Transceivers 10GBASE-LR and the 10GBASE-SR are available. Note that the 10GBASE-ER is unavailable.
- The 10GBASE-R transceiver is available as an option and you can purchase and use the optional item. For details, see the List of Options. If you use any other 10GBASE-R transceiver other than the option, correct operation or safety is not guaranteed.
- Laser light is used for the 10GBASE-R transceiver. (Laser light is colorless and transparent, meaning that it is invisible to the human eye.) Never look directly into the light-transmitting/receiving unit.
- In the default configuration, limit-queue-length of transmission in physical ports is set to 1976, and also “flowcontrol send on” is set to all ports.
- When you start the switch module, restart it by unplugging and plugging, or restart the switch module using an operational command, linkup (1), linkdown (2), and linkup (3) might be detected for a couple of seconds in the onboard LAN and LAN mezzanine card of the server blade at the linkup immediately after the boot. Usually a linkup (3) is detected once. Since this occurs immediately after the switch module starts, operation will not have any problem. Logs of (1), (2), and (3), however, might be collected in the log information of OS (Windows or Linux).

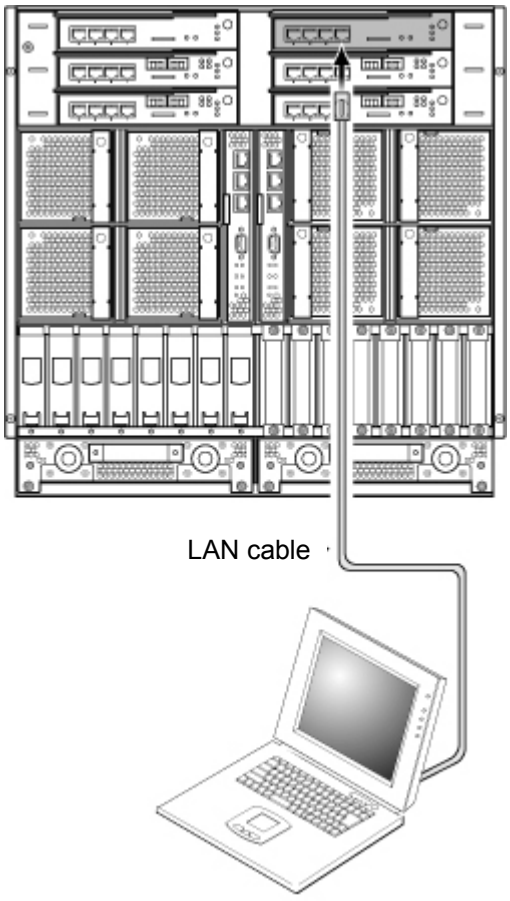
Connection to setup terminal

A setup terminal connected via a LAN or serial cable is initially required.

This section describes how to connect a terminal to the module in each method.

LAN interface connection

As shown below, connect your PC and the port (line 1) of the switch module with a LAN cable. Prepare the LAN cable for connection.



Network connection specifications (shipment setting)

Item	Setting
IP address	192.168.0.254 or switch module0: 192.168.0.60 switch module1: 192.168.0.61 switch module2: 192.168.0.62 switch module3: 192.168.0.63 switch module4: 192.168.0.64 switch module5: 192.168.0.65
Subnet mask	255.255.255.0
Type of cable	Cross/Straight (Based on Auto-MDI/MIDX)
Transmission rate	Auto-Negotiation



Use the telnet client with CRLF disabled. For information on how to disable the carriage return/line feed (CRLF), see Help of each telnet client or other materials.

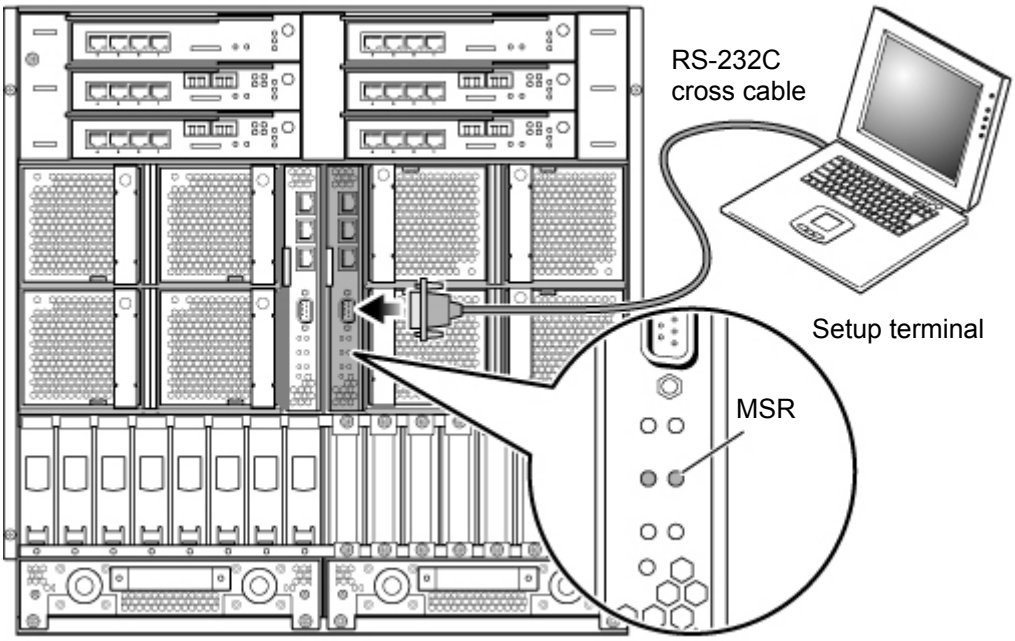
Server blade model	Port setting for server connection
X55A1/X55A2/X57A1/X57A2	Speed 1000 Duplex full
X55R3/X55S3	255.255.255.0

Serial interface connection

Select a LAN switch module to connect using the SCO command. Connect your setup terminal to the serial port on the management module installed in the system equipment using the RS-232C cross cable.

When two management modules are installed, connect to the management module with the Master (MSR) light emitting diode (LED) that lights solid green.

Prepare the RS-232C cross cable for connection.



Setup terminal requirements

Item		Specification
Communication port		RS-232C port
Communication software		Any of the following communications software products or its equivalent communication software - Hyper terminal attached to Windows 2000 or Windows XP - Tera Term Pro (Version 2.3)
Communication setting	Communication protocol	ZMODEM protocol
	Communication parameter	8 bits, 1 stop bit, no parity
	Communication rate *1	19200bit/s, 9600bit/s, 4800bit/s, 2400bit/s, 1200bit/s

*1 In the shipment settings of this system, the communication speed of the console port is set in 9600 bits/s. To use another rate, see the Speed command for operation terminal connection, “Configuration Command Reference Vol.1” in the CD-ROM attached to this device.

Command input mode overview

The command line interface for the system supports two command input modes: operation command mode and configuration command mode.

You can execute operation commands in the operation command mode, and you can execute configuration commands in the configuration command mode.

The command line interface for the system is classified into two user levels: a general user level and a system administrator level. Operation command mode supports both the general user level and system administrator level. Configuration command mode has only the system administrator level.

The following table lists features of command input modes and details on how to access and exit command input modes.

Command input modes

Command input mode	User level	Accessed by:	Prompt	Exited by:	Note
Operation command	General user	login: <user-ID>	>	> logout	You can use some operation commands.
	System administrator	> enable	#	# disable	You can use all operation commands.
Configuration command	System administrator	# configure	(config)#	(config)# exit	You can use all configuration commands.

Operation command mode (for the general user)

If you log in to the system, this mode will be set.

In this mode, you can run some operation commands that are enabled for the general user level.

You cannot register a new user account and delete a user account in the general user level. The registration and deletion requires the system administrator level.

Operation command mode (for the system administrator)

If you enter the enable command in the general user mode, this mode will be set.

In this mode, you can use all operation commands.

The enable command is not initially assigned a password. To prevent security deterioration, it is recommended that you assign a password to the enable command and restrict system administrator qualifications to a specific user.

Configuration command mode

If you enter the configure command in the system administrator mode, this mode will be set.

You can configure or reconfigure the system by using the configuration command in this mode.



- The configuration command mode provides a hierarchical structure. The configuration command (config)# in the table above (config)# is called the global configuration mode, and supports input modes classified depending on a command type. For details about configuration command mode, see the *Configuration Guide*"
- Information on the user levels in which you can run the operation command is described in the *Operation Command Reference in the Software Manual*. Information on input modes in which you can run the configuration command is described in *the Configuration Command Reference*.

Initial installation operation overview

This section outlines required operations at initial installation.

For details on the operations, see the following sections.



The operations below are indispensable during initial installation. For details about operations after the initial installation, see the manual described in "Details on how to operate the system."

1 Login.

Log in to the system. Use user ID "operator" set during initial installation. ("operator" is not assigned any passwords and, therefore, you can log in to the system without authentication.)

2 Setting the system administrator's password.

Set the system administrator's password, which is not initially set. To prevent security deterioration, set that password.

3 Adding a user ID and deleting "operator".

Create a new user ID.

When not using login user "operator" set during initial installation as the qualified login user, you should delete it after a new login user created by the rmuser command to prevent security deterioration.

Login

Starting the system, you will see the login prompt appear. Following the login prompt, enter the user ID to log in to the system.

```
login: operator ···Enter user ID "operator".

Copyright (c) 2005-2009 ALAXALA Networks Corporation. All rights reserved.

>
```



In the following descriptions, information might be different depending on the software version. Basic operations, however, are unchanged.

Setting the system administrator's password

Set the system administrator's password.

```
> enable ···Qualified as the system administrator.
# password enable-mode ···Allows you to set the system administrator's password.
Changing local password for admin.
New password: ******** ···Set the system administrator's password.
Retype new password: ******** ···For confirmation, re-type in the password.
#
```



The password must consist of 6 to 128 characters. If you enter more than 128 characters, up to 128 characters will be registered as the password. The system rejects a password consisting of lowercase alphabetic characters only. You have to enter uppercase alphabetic, numeric or special characters in addition to lowercase alphabetic characters.

Adding a user ID and deleting "operator"

❑ Creating a user ID and setting a login password

Create a new user ID and set a login password.

The example below explains how to create a new user ID "newuser" and set a login password.

```
# adduser newuser ···Set new user ID "newuser".
User(empty password) add done. Please setting password.
Password: ******** ···Assign a login password to user ID "newuser".
Retype new password: ******** ···For confirmation, re-type in the password.
# disable ···Takes you back to general user mode.
> logout ···Log out of the system.
```



The password must consist of 6 to 128 characters. If you enter more than 128 characters, up to 128 characters will be registered as the password. The system rejects a password consisting of lowercase alphabetic characters only. You have to enter uppercase alphabetic, numeric, or special characters in addition to lowercase alphabetic characters.

❑ Deleting user ID "operator"

Delete the user ID "operator" that set during initial installation.

Backup and restore of module information

To protect against unexpected problems, you should back up module information. The information to be backed up includes switch module information and configurations.

The switch module information is the information customized by a user such as configuration including switch software and passwords, which is used to take the switch module back to the status before replacement. The configurations are files for a switch such as VLAN and have the following types:

- startup-config: a setting file referred to when a module starts
- running-config: a file to save the configurations that a module is using



If you change configuration and do not save it, startup-config is different from running-config.

You can back up and restore information separately by using the backup and copy/cp commands. You can copy the data into the ftp server or the optional memory card (MC). The following shows an example of using commands.

Backing up configuration

1 Backup using the ftp server (Server address: `192.168.0.128 / user name: staff`)

```
> enable    <= Press [Enter].
# copy startup-config ftp://staff@192.168.0.128/bakcup.conf    <= Press [Enter].
Configuration file copy to ftp://staff@192.168.0.128/bakcup.conf ?
(y/n): y   <= Press [Enter].
Authentication for 192.168.0.128.
User: staff    <= Press [Enter].
Password:xxx    <= Enter the staff password.
Transferring///
Data transfer succeeded.
#
```

2 Backup using the MC (Stored into the MC)

```
> cd/usr/home/operator    <= Press [Enter].
> enable    <= Press [Enter].
# copy running-config bakcup.conf    <= Press [Enter].
Configuration file copy to /user/home/operator/bakcup.conf?
(y/n): y   <= Press [Enter].
# exit    <= Press [Enter].
> cp backup.conf mc-file backup.conf    <= Press [Enter].
```

Backing up the entire switch module

1 Backup using the ftp server (Server address: `192.168.0.128/user name: staff`).

```
> enable    <= Press [Enter].
# backup ftp ftpserver MCBackup.dat    <= Press [Enter].
# ./backup ftp 192.168.0.128 MCBackup.dat    <= Press [Enter].
Backup information to FTP (192.168.0.128) MCBackup.dat.
Input username: staff  <= Press [Enter].
Input password:.
ftp transfer start.
ftp transfer succeeded.
```

2 Backup using the MC (Stored into the MC).

```
> enable    <= Press [Enter].
# backup mc MCBackup.dat    <= Press [Enter].
Backup information to MC (MCBackup.dat).
Copy file to MC…
Backup information success!
```

Restoring the switch module information

1 Restore using the ftp server (Server address: `192.168.0.128/user name: staff`).

```
> enable    <= Press [Enter].
# restore ftp 192.168.0.128 MCBackup.dat no-software    <= Press [Enter].
Restore information from FTP (192.168.0.128) MCBackup.dat.
Input username: staff    <= Press [Enter].
Input password:    <= Enter the password and press [Enter].
ftp transfer start.

Operation normal end.
ftp transfer succeeded.
restore finished.
```

2 Restore using the MC (Read from the MC).

```
> enable    <= Press [Enter].
# restore mc MCBackup.dat no-software    <= Press [Enter].
Restore information from MC (MCBackup.dat).
Copy file from MC…
restore finished.
```



You can take a backup the switch module information including switch software by the restore command. However, the switch software has the hardware related information, therefore, it might not run on the new hardware. Use the no-software option when you restore it after replacing the hardware.



You have to operate this in the administrator mode.

Restoring the configuration (apply to startup-config)

1 Restore using the File Transfer Protocol (ftp) server (Server address: `192.168.0.128/user name: staff`).

```
> enable    <= Press [Enter].
# copy ftp://staff@[192.168.0.128]/Backup.conf startup-config    <= Press [Enter].
Configuration file copy to startup-config? (y/n): y    <= Press [Enter].

Authentication for 192.168.0.128
User: staff
Password:
Transferring…
Data transfer succeeded.
```

2 Restore using the MC (Read from the MC).

```
> cd/usr/home/operator    <= Press [Enter].
> cp mc-file backup.conf backup.conf    <= Press [Enter].
> enable    <= Press [Enter].
# copy /usr/home/operator/backup.conf startup-config    <= Press [Enter].
Configuration file copy to startup-config? (y/n): y    <= Press [Enter].
```

Connection with the server blades

The server blade provides ten LAN ports that are connected to the LAN switch as follows.

Server blade slot number	LAN port number on the server blade		LAN switch module slot number	LAN switch module line number
0	LAN1	82576	0	line 5
	LAN2		1	line 5
	LAN3	82576	2	line 5
	LAN4		3	line 5
	LAN5	82576	2	line15
	LAN6		3	line15
	LAN7	82576	4	line 5
	LAN8		5	line 5
	LAN9	82576	4	line 15
	LAN10		5	line 15
1	LAN1	82576	0	line 6
	LAN2		1	line 6
	LAN3	82576	2	line 6
	LAN4		3	line 6
	LAN5	82576	2	line 16
	LAN6		3	line 16
	LAN7	82576	4	line 6
	LAN8		5	line 6
	LAN9	82576	4	line 16
	LAN10		5	line 16
:				
:				
7	LAN1	82576	0	line 12
	LAN2		1	line 12
	LAN3	82576	2	line 12
	LAN4		3	line 12
	LAN5	82576	2	line 22
	LAN6		3	line 22
	LAN7	82576	4	line 12
	LAN8		5	line 12
	LAN9	82576	4	line 22
	LAN10		5	line 22



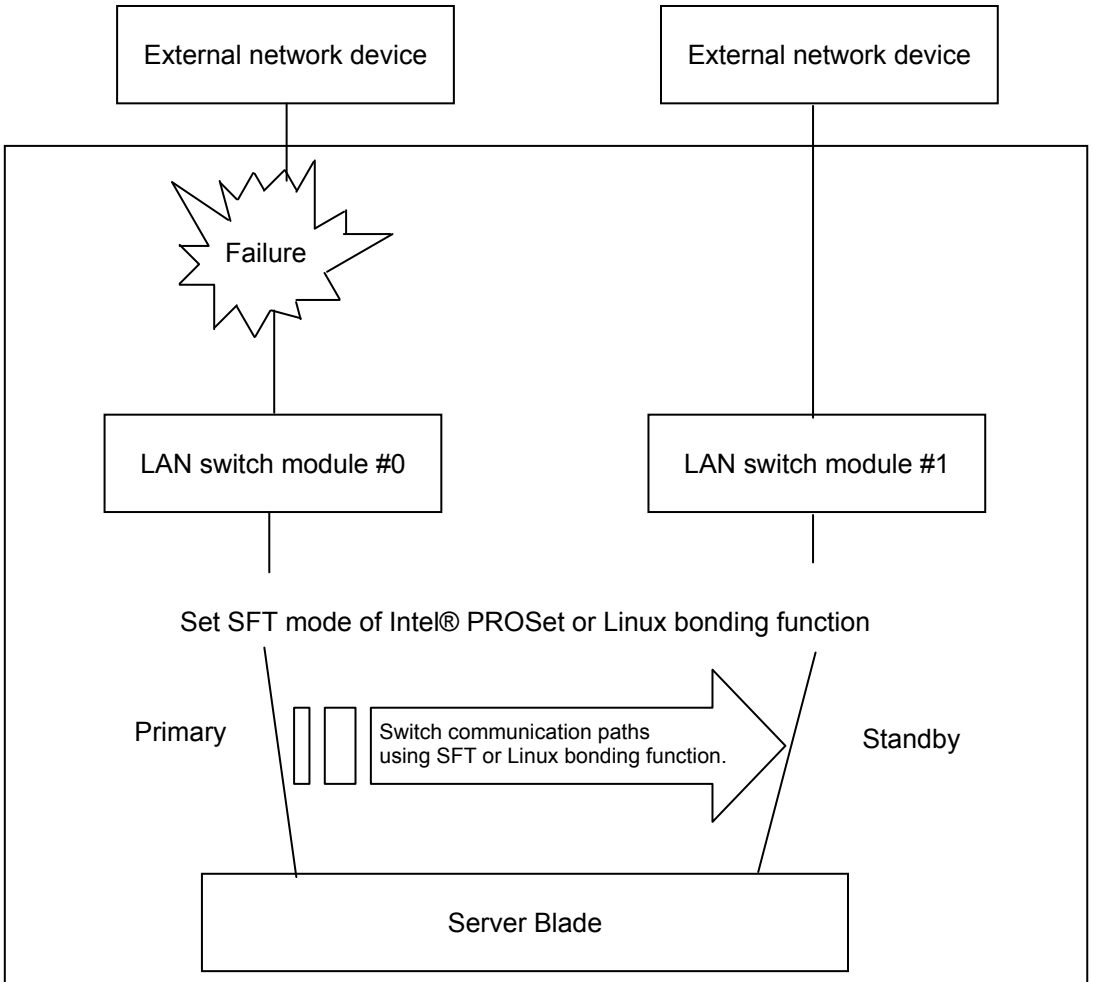
To use LAN3 to LAN10, both an expansion card and expansion switch module are required.

Referring to the table above, if you are going to connect multiple internal ports, you need to use the proper VLAN configuration or to use the Intel driver in Windows or ‘bonding’ in Linux.

Uplink failover overview

Uplink failover is a fault tolerance function that changes communication paths in failure of the LAN switch module or external network device. It is implemented by using together with SFT (Switch Fault Tolerance), a teaming function of Intel® PROSet, or Linux bonding function on a server blade.

The following figure shows the uplink failover operation.




```
[Setting outline]

1. Teaming setting to NIC on the server blade
  (1) Set the SFT mode or Linux bonding function.
  (2) Set the preferred primary (SFT), and Master (Linux binding function)
      (The primary system is used as the communication routing.
2. Set uplink failover to the LAN switch module.
  (1) Set uplink failover to the external port of the primary LAN switch module.
```

Tip

- This uplink failover function handles the external network failure where linkdown occurs in the physical layer.
- This uplink failover function switches paths when detecting the following linkdown as failure.
  - The shutdown command is executed to the target port;
  - The primary LAN switch module or the external network device connected to the primary LAN switch module is powered off; and
  - Reboot.
- When the channel group for link aggregation is targeted for this uplink failover function, the communication path will not be switched unless all ports belonging to the channel group link down.

❑ Failure recovery

When all target ports for this function are linked up in the primary LAN switch module, inactive connection ports for server blades will be activated. When the channel group for link aggregation is targeted for this function, linkup of a single port, which belongs to the channel group, will activate those server blade connection ports. Server blades detect that those server blade connection ports are activated, and then redundancy configuraiton will be restored. With NIC teaming set as described in the previous page, the primary communication path will be recovered.

NOTICE

- This function cannot be set with spanning tree, Gigabit Switch Redundancy Protocol (GSRP), or Virtual Router Redundancy Protocol (VRRP).
- When setting this function to the port of a link aggregation, set this the channel group to which the port belongs.
- Set this function only when the target external port and the link aggregation channel group have linked up.

See “Configuration Command” in the Firmware & Accessory CD for Compute Blade Built-in LAN Switch Module that is attached to the device for the uplink failover function setting.

Tip

You can specify any uplink port and port for connection to the server blade and then use the uplink failover function on the target port.

See *Configuration Settings* in the Firmware & Accessory CD for Compute Blade Built-in LAN Switch Module attached to the device.

LAN switch module web console

This section describes the LAN switch module Web console.

LAN switch module web console functions

The LAN switch module Web console is a management module function, which you can configure each function of the LAN switch module using the GUI from the web browser of the client PC. The LAN switch Web console can be opened using the Connection button on the Switch Module Details View in Chapter 6.



The LAN switch module Web console can be used with a 1 G / 10 G LAN switch module in which the firmware version 10.7 or later is installed. With the firmware version earlier than 10.7, an error might occur. You can check the firmware version on Display version screen.



When you have changed settings with the LAN switch module Web console, the new settings directly affect the LAN switch module. If you restart the LAN switch module, however, the new settings will be lost because they are stored in the temporary memory in the LAN switch module. Save the new settings to the LAN switch module on the SAVE screen.

❑ Functions of the LAN switch module web console

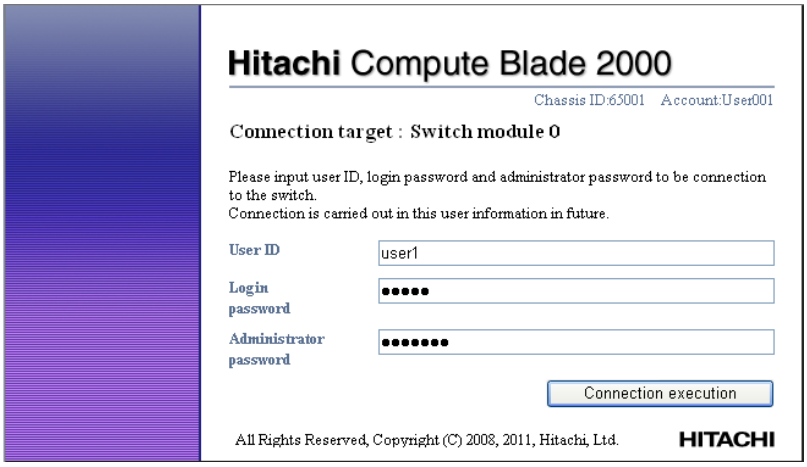
The following table describes settings and views that you can operate with the LAN switch module Web console.

#	Menu	Description	Screen
1	Display version	Displays the firmware version of the LAN switch module.	Display version screen
2	Time	Sets a time zone.	Time zone setting screen
3	NTP server	Sets Network Time Protocol (NTP) server settings.	NTP server list screen
4	Spanning tree	Enable or disable the spanning tree function.	Spanning tree setting screen
5	VLAN	Sets VLAN settings	VLAN list screen
6	Link aggregation	Sets link aggregation settings	Link aggregation list screen
7	Ethernet port	Sets Ethernet port settings	Ethernet ports screen
8	Uplink failover	Sets uplink failover settings.	Uplink failover setting screen
9	IPv4 static route	Sets IPv4 static route settings	IPv4 static route setting screen
10	Log output	Sets log output settings.	Log output setting screen
11	Operation terminal connection	Sets operation terminal connection settings.	Operation terminal connection setting screen
12	SAVE	Saves new settings.	SAVE screen
13	Copy configuration file	Configures LAN switch module settings with the configuration file.	Configuration setting screen

Connection to a LAN switch module

When the LAN switch module Web console is opened, the following window might appear, asking you to type the user ID, Login password, and Administrator password to connect to the LAN switch module.

When this window appears, type the user ID, Login password, and Administrator password, which are registered in the LAN switch module, and click **Connection execution**. The input information is stored in the management module, and you can connect to the module automatically the next time.



Operation

When having successfully connected to the LAN switch module, you will go to the Display version screen.

The following screen shows the basic structure of the LAN switch module Web console.

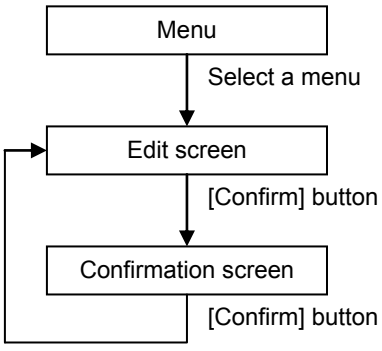


To move among screens, select a screen to display from the left navigation menu bar.

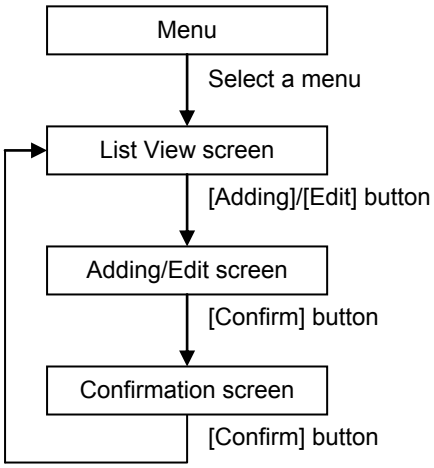
To finish the LAN switch module Web console, click **Close** on the upper right of the screen.

The following flow charts show the basic procedure for the LAN switch module Web console operation.

Screen with the list view



Screen without the list view



Display version

This section shows the screen to display a LAN switch module firmware version.

Use the firmware version 10.7 or later. If a version earlier than 10.7 is used, an error might occur when you open a setting screen.

❑ Display version screen

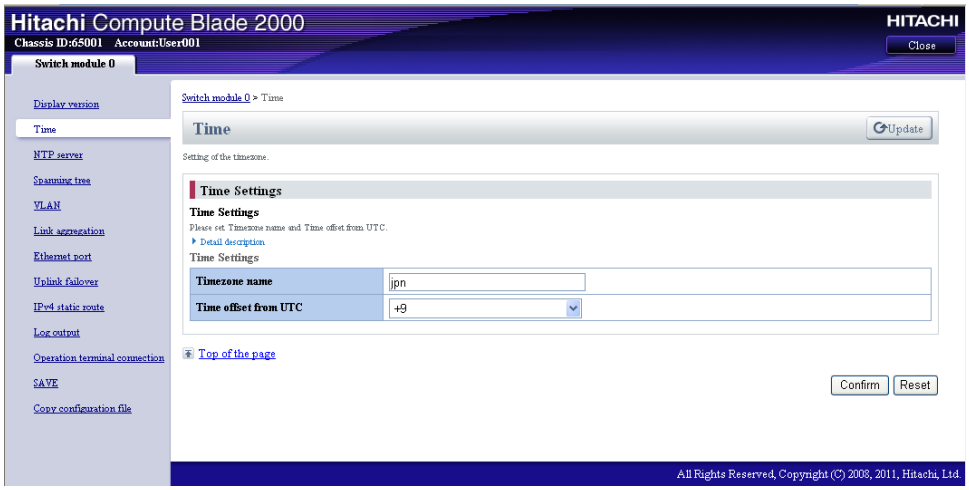


#	Item	Description	Edit
1	Switch module firmware version	Displays the firmware version of the LAN switch module.	-

Time

This section shows the screen for time zone setting.

❑ Time zone setting screen



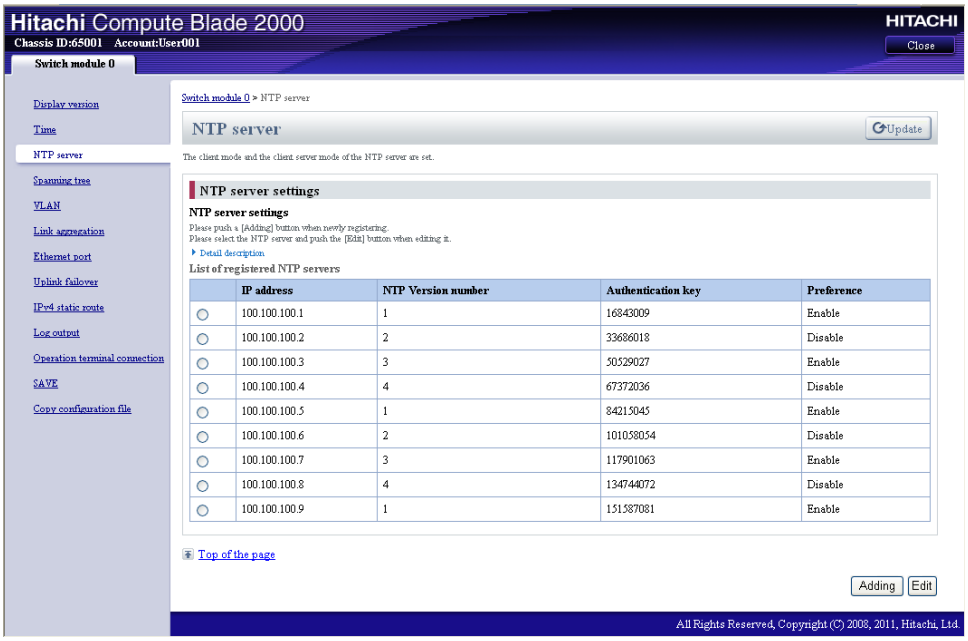
#	Item	Description	Edit
1	Timezone name	Put a name to identify the time zone using up to 7 alphanumeric characters.	Available
2	Time offset from UTC	Set a time offset from Greenwich Mean Time.	Available

NTP server

This section shows the screen for registering NTP servers with which a LAN switch module synchronizes time.

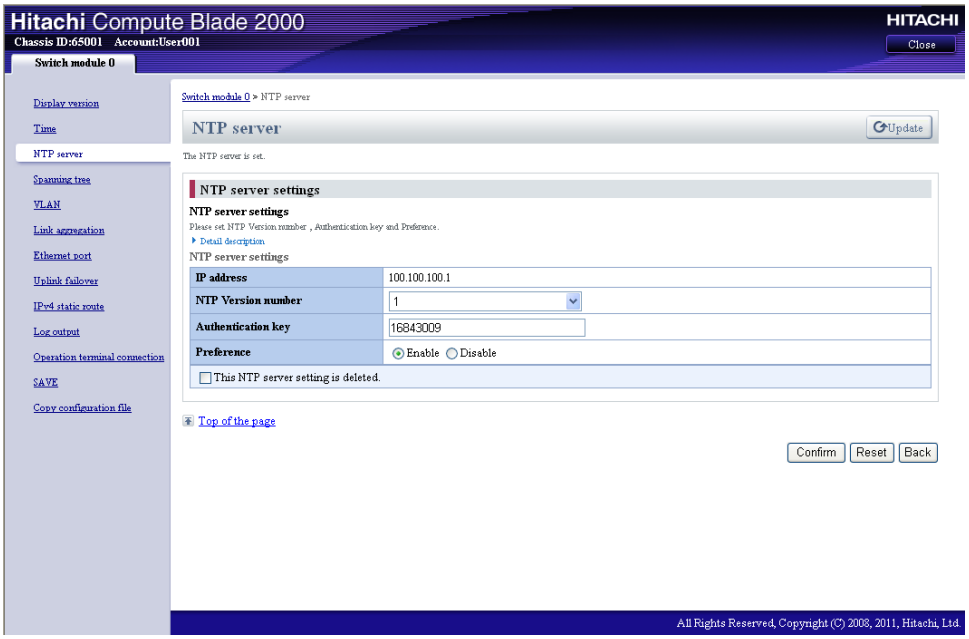
❑ NTP server list screen

The following screen lists all NTP servers registered. When changing settings of an NTP server, select the NTP server and click **Edit**.



#	Item	Description	Edit
1	IP address	Displays IP addresses of NTP servers to synchronize time with.	-
2	NTP version number	Displays NTP version numbers.	-
3	Authentication key	Displays authentication keys for access.	-
4	Preference	Displays preference.	-
5	Adding	Moves to the screen for adding an NTP server.	-
6	Edit	Moves to the screen for editing the selected NTP server.	-

❑ NTP adding/editing screen



#	Item	Description	Edit
1	IP address	Type an IP address of the NTP server to synchronize time with.	Available
2	NTP version number	Select the NTP version number.	Available
3	Authentication key	Edit the authentication key for access, which is a value from 1 to 4294967295.	Available
4	Preference	Select preference: Enable or Disable. With multiple NTP servers, those with Enable this item are preferred.	Available
5	This NTP server setting is deleted.	If deleting this NTP server, check this item.	Available

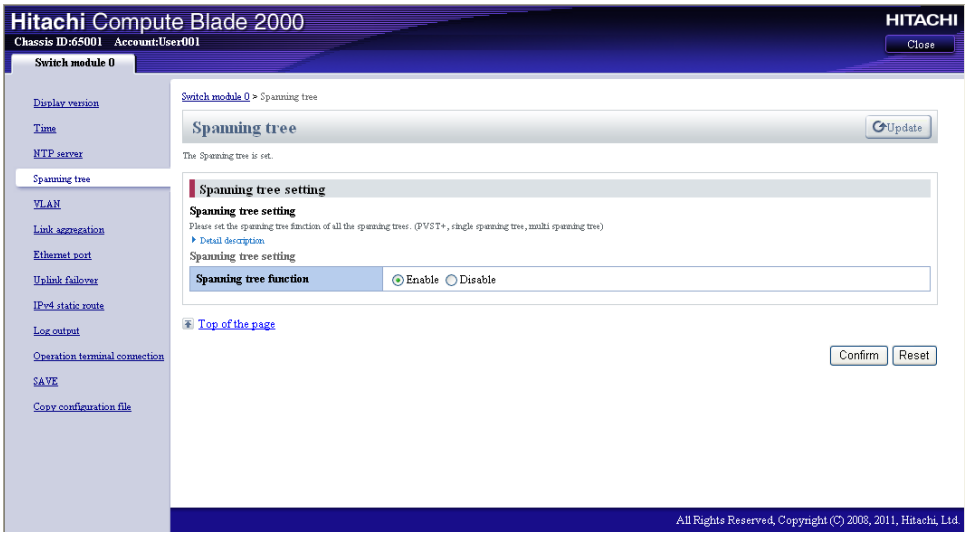
Tip

- You can type an IP address only when displaying this screen with the **Adding** button.
- The **This NTP server setting is deleted** checkbox is displayed only when you have clicked **Edit** on the NTP server list screen.

Spanning tree

This section shows the screen for enabling or disabling the spanning tree function.

❑ Spanning tree setting screen



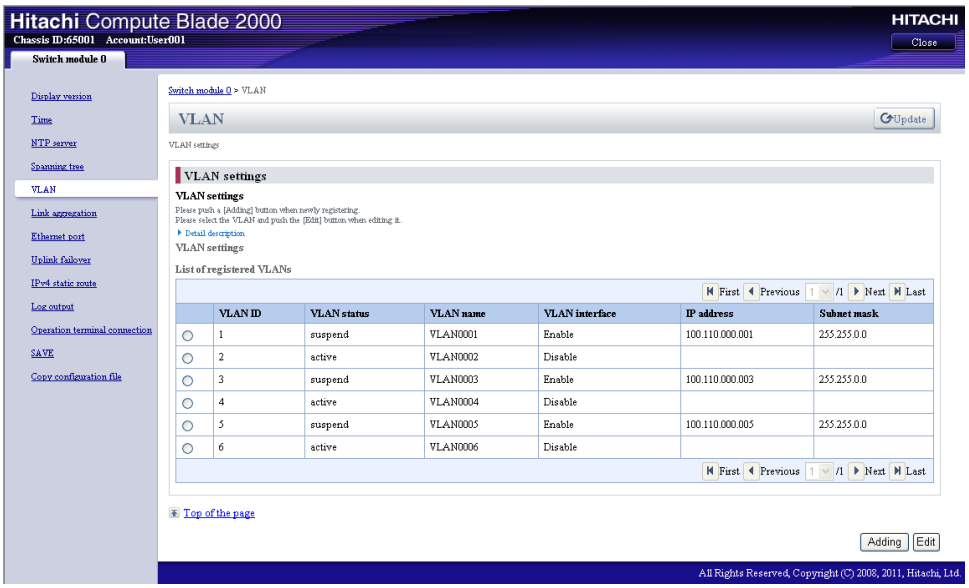
#	Item	Description	Edit
1	Spanning tree function	Select from Enable and Disable the spanning tree function.	Available

VLAN

This section shows the screen for registering VLANs.

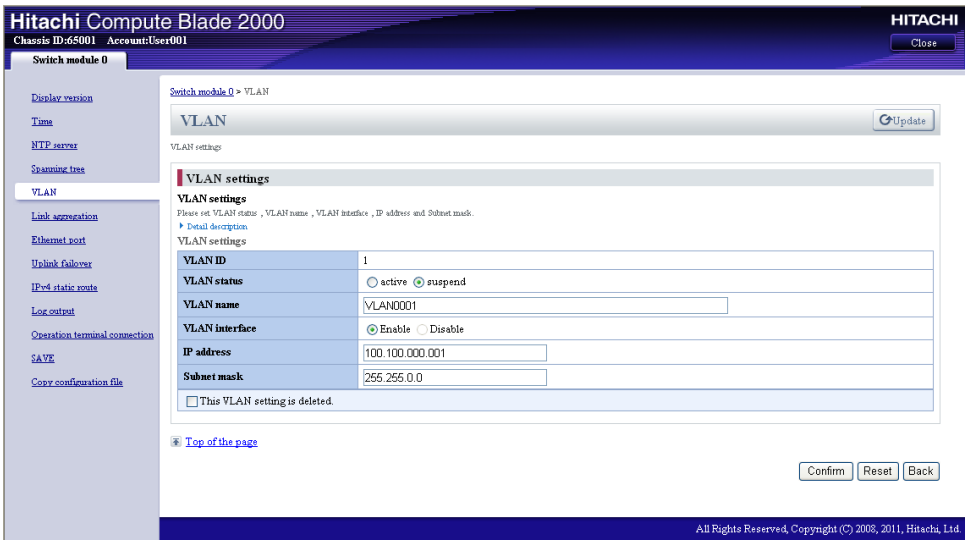
❑ VLAN list screen

The following screen lists all VLANs registered. When changing settings of a VLAN, select the VLAN and click **Edit**. A single screen displays up to 100 VLANs. With more than 100 VLANs registered, move among pages using the navigation buttons on the upper right of the List of registered VLANs.



#	Item	Description	Edit
1	VLAN ID	Displays VLAN IDs.	-
2	VLAN status	Displays VLAN status.	-
3	VLAN name	Displays VLAN names.	-
4	VLAN interface	Displays VLAN interfaces.	-
5	IP address	Displays IP addresses.	-
6	Subnet mask	Displays subnet masks.	-
7	Adding	Moves to the screen of adding VLANs.	-
8	Edit	Moves to the screen for editing the selected VLAN.	-

❑ VLAN adding/editing screen



#	Item	Description	Edit
1	VLAN ID	Type a VLAN ID. The value is from 1 to 4094.	Available
2	VLAN status	Select a VLAN state.	Available
3	VLAN name	Edit the VLAN name. The value is comprised of up to 32 alphanumeric characters.	Available
4	VLAN interface	Select from Enable and Disable the VLAN interface.	Available
5	IP address	Edit the IP address.	Available
6	Subnet mask	Edit the subnet mask.	Available
7	This VLAN setting is deleted.	If deleting this VLAN setting, check this item.	Available

Tip

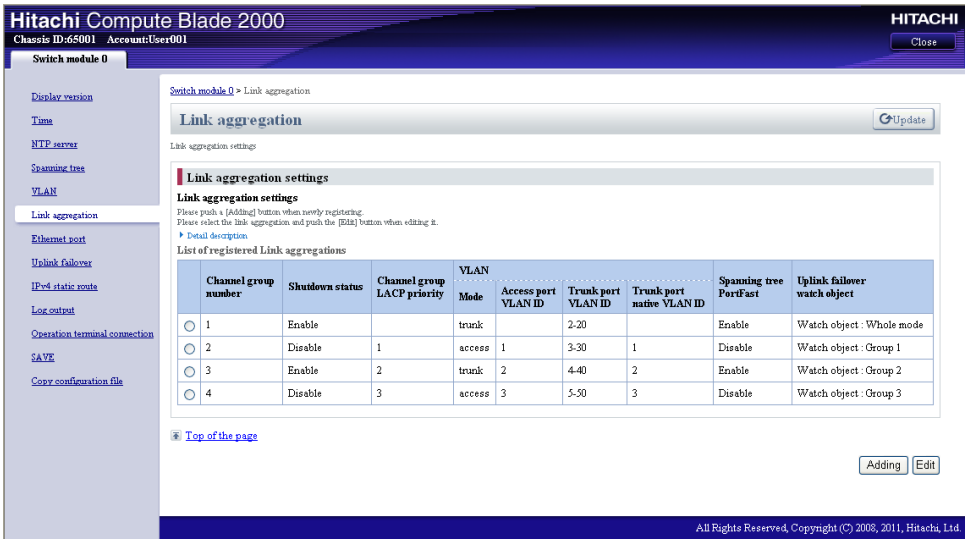
- You can type an IP address only when displaying this screen with the **Adding** button.
- The **This VLAN setting is deleted.** checkbox is displayed only when you have clicked **Edit** on the VLAN list screen.
- When setting an IP address, type both the IP address and subnet mask, and enable the VLAN intrerface. Click **Confirm**. With the VLAN interface disabled, values of the IP address and subnet mask are ignored.
- VLAN interface settings cannot be changed from Enable to Disable. If you need to change the value, delete the VLAN and then recreate a VLAN.

Link aggregation

This section shows the screen for registering link aggregation.

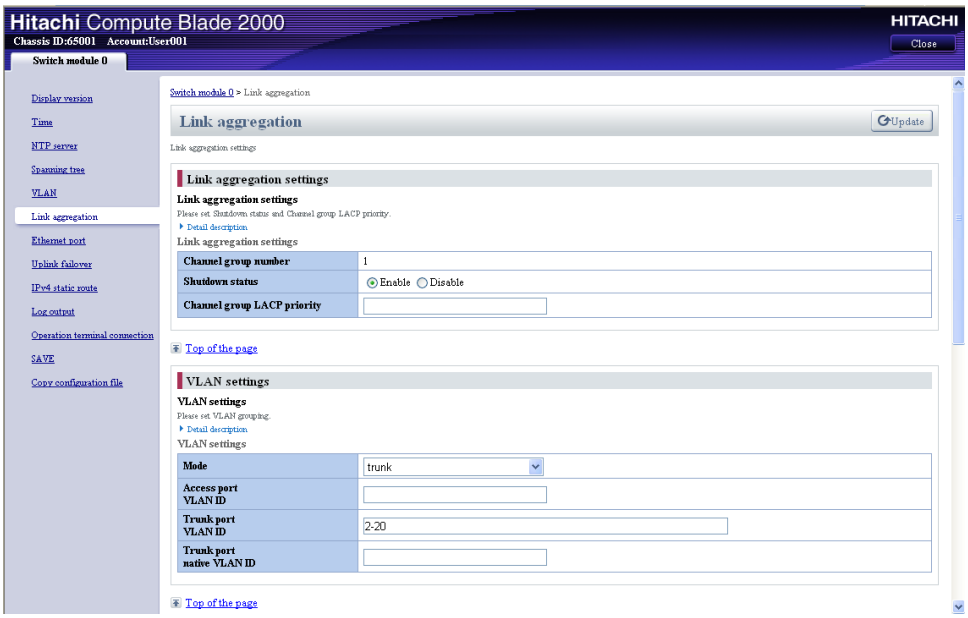
❑ Link aggregation list screen

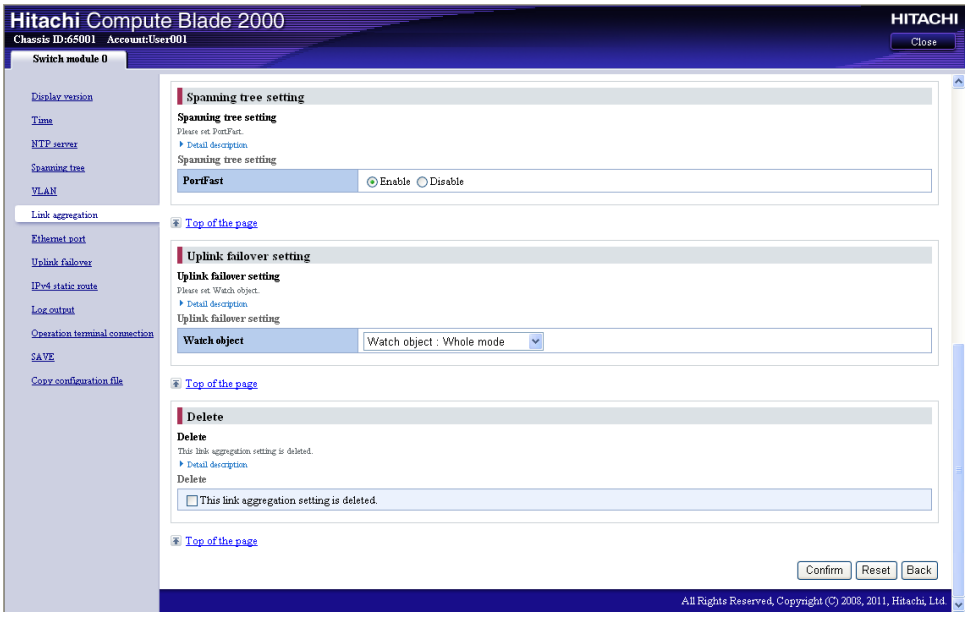
The following screen lists all link aggregations registered. When changing settings of a link aggregation, select a link aggregation and click **Edit**.



#	Item	Description	Edit
1	Channel group number	Displays channel group numbers.	-
2	Shutdown status	Displays shutdown status: Enable or Disable	-
3	Channel group LACP priority	Displays channel group Link Aggregation Control Protocol (LACP) priority.	-
4	VLAN mode	Displays VLAN modes.	-
5	Access port VLAN ID	Displays access port VLAN IDs.	-
6	Trunk port VLAN ID	Displays trunk port VLAN IDs.	-
7	Trunk port native VLAN ID	Displays trunk port native VLAN IDs.	-
8	Spanning tree PortFast	Displays spanning tree PortFast: Enable or Disable	-
9	Uplink failover watch object	Displays uplink failover watch objects.	-
10	Adding	Moves to the screen for adding a link aggregation.	-
11	Edit	Moves to the screen for editing the selected link aggregation.	-

❑ Link aggregation adding/editing screen





#	Item	Description	Edit
1	Channel group number	Type a channel group number from 1 to 32.	Available
2	Shutdown status	Select a shutdown state: Enable or Disable	Available
3	Channel group LACP priority	Edit the channel group LACP priority. The value is from 1 to 65535.	Available
4	VLAN mode	Select a VLAN mode.	Available
5	Access port VLAN ID	Edit the access port VLAN ID. The value is from 1 to 4094.	Available
6	Trunk port VLAN ID	Edit the trunk port VLAN IDs. The value is from 1 to 4094, which can be a range such as 10-20. Up to 8 values, separated by commas, can be typed	Available
7	Trunk port native VLAN ID	Edit the trunk port native VLAN ID from 1 to 4094.	Available
8	Spanning tree PortFast	Select a value for the spanning tree PortFast: Enable or Disable.	Available
9	Uplink failover watch object	Select an uplink failover watch object.	Available
10	This link aggregation setting is deleted.	If deleting this link aggregation setting, check this item.	Available



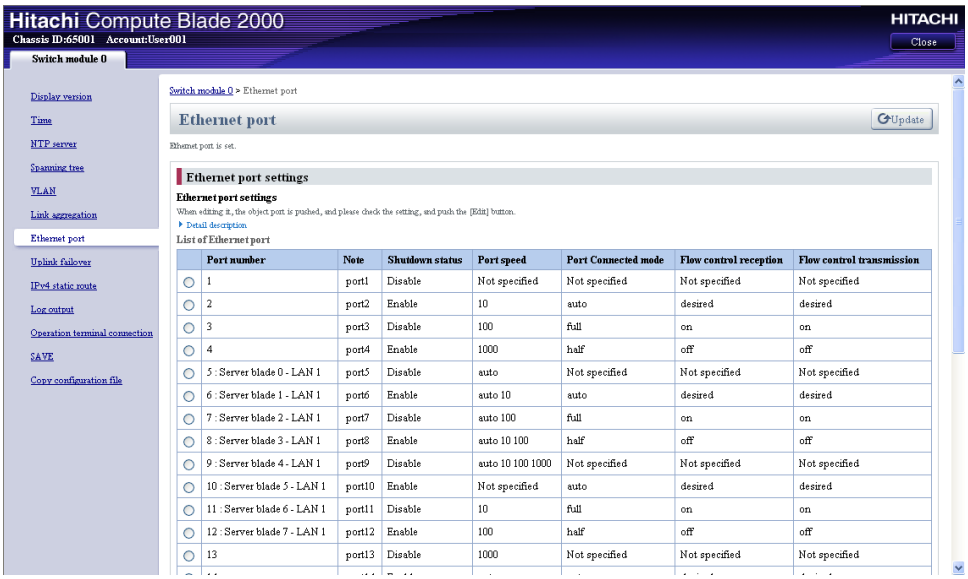
- You can type a channel group number only when displaying this screen with the **Adding** button.
- The **This link aggregation setting is deleted.** checkbox is displayed only when you have clicked **Edit** on the Link aggregation list screen.

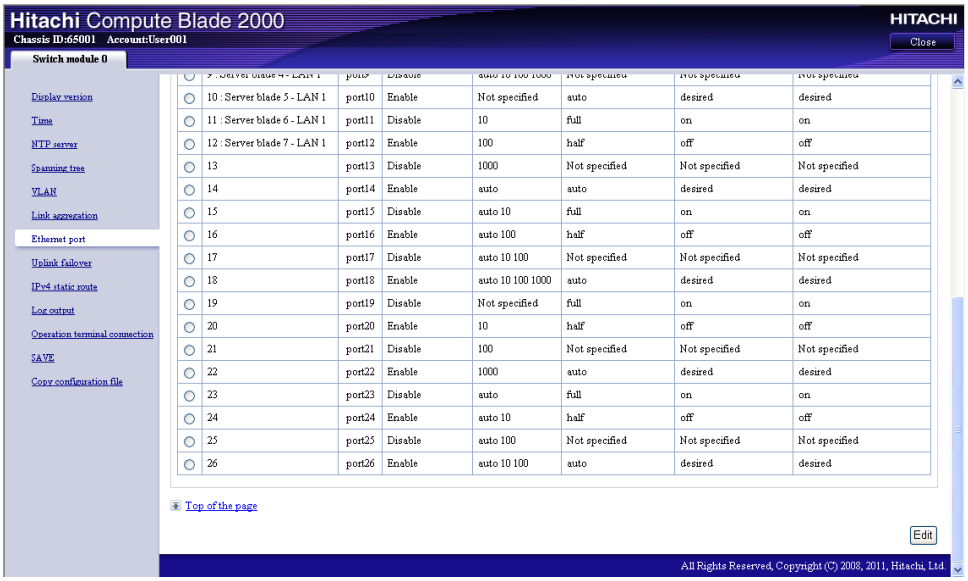
Ethernet port

This section shows the screen for setting Ethernet ports.

❑ Ethernet ports screen

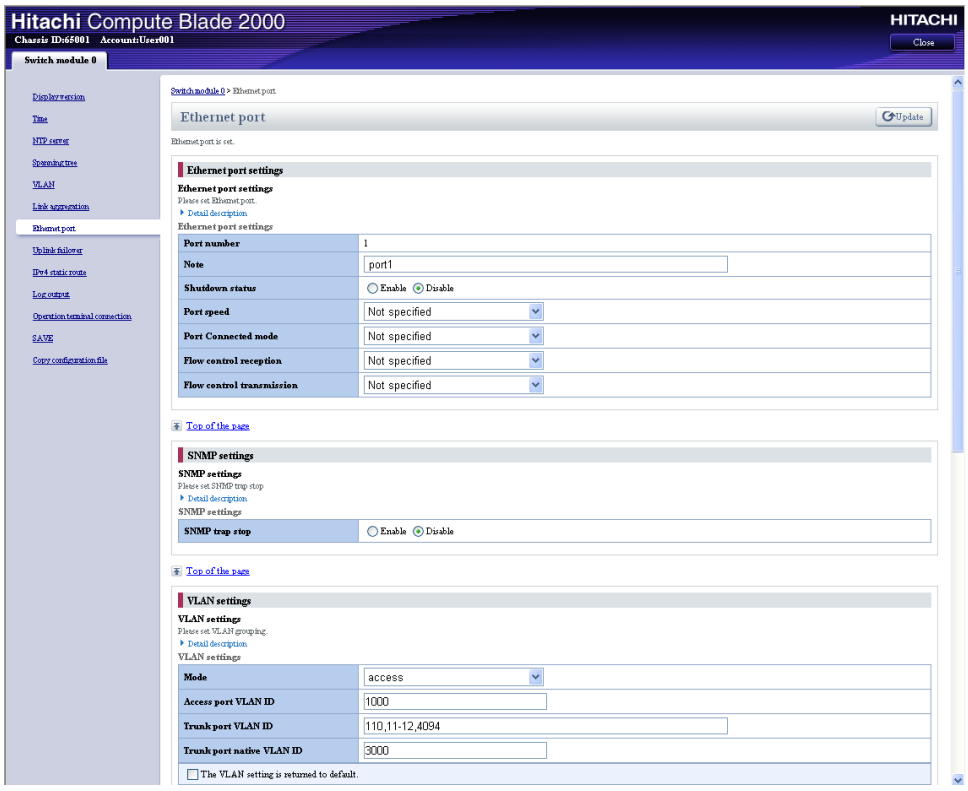
The following screen lists all Ethernet ports. When changing settings of an Ethernet port, select the Ethernet port and click **Edit**.

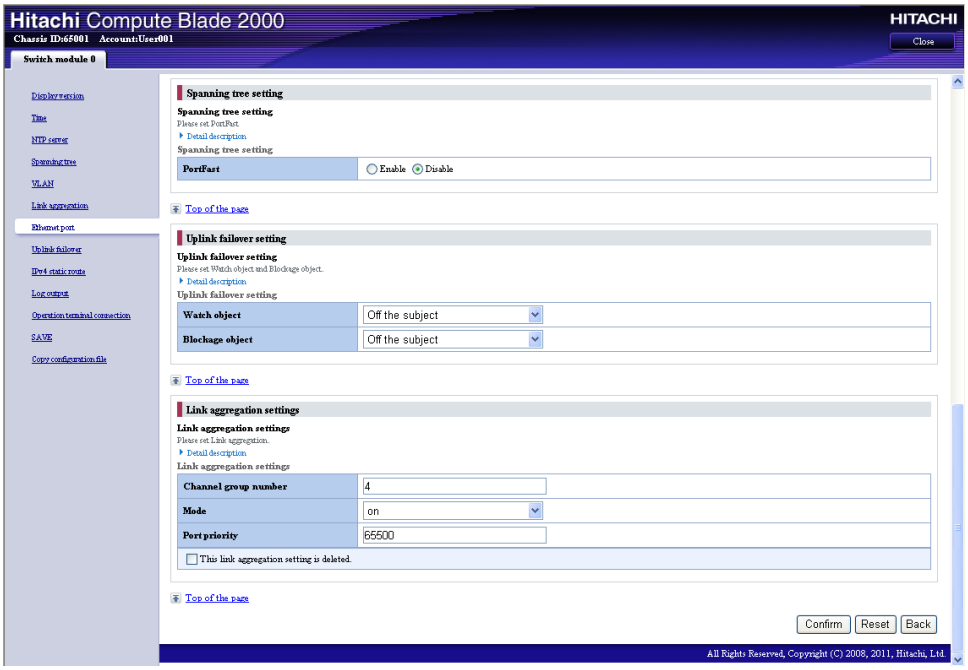




#	Item	Description	Edit
1	Port number	Displays port numbers.	-
2	Note	Provides supplementary information.	-
3	Shutdown status	Displays shutdown status: Enable or Disable	-
4	Port speed	Displays port speeds.	-
5	Port Connected mode	Displays port connected modes.	-
6	Flow control reception	Displays flow control receptions.	-
7	Flow control transmission	Displays flow control transmissions.	-
8	Edit	Moves to the screen of editing the selected Ethernet port.	-

❑ Ethernet port editing screen





#	Item	Description	Edit
1	Port number	Displays port numbers.	-
2	Note	Edit supplementary information using up to 64 alphanumeric characters.	Available
3	Shutdown status	Select shutdown status: Enable or Disable	Available
4	Port speed	Select a port speed.	Available
5	Port connected mode	Select a port connected mode. - When a parameter including “auto” or the “auto” itself is assigned to the port speed or port connected mode, auto-negotiation is performed. - When not using auto-negotiation, set the port speed to 10 or 100 and also the duplex to full or half. - When you have changed the port speed to 10 or 100 and the duplex to half for the server connection port, the mode becomes “auto” without applying the changed values. The values, however, are changed on the Web console. - When not using auto-negotiation with the server connection port, make sure to select 1000 for the port speed and full for the port connection mode. - When selecting auto 1000 for the port speed of the server connection port, do not change the port connection mode. The port might be linked down and then linked up.	Available
6	Flow control reception	Select a value for flow control reception. - desired: With the fixed mode specified, pose packets are received. With auto-negotiation specified, pose packet receptions are determined by communicaiton between devices.	Available

#	Item	Description	Edit
		- on Pose packets are received. - off No pose packet is received.	
7	Flow control transmission	Select a value for flow control transmission. - desired: With the fixed mode specified, pose packets are transmitted. With auto-negotiation specified, pose packet transmissions are determined by communicaiton between devices. - on Pose packets are transmitted. - off No pose packet is transmitted.	Available
8	SNMP trap stop	Select the value for SNMP trap stop.	Available
9	VLAN mode	Select a VLAN mode	Available
10	Access port VLAN ID	Set an access port VLAN ID from 1 to 4094.	Available
11	Trunk port VLAN ID	Set a trunk port VLAN ID from 1 to 4094. The value can be a range such as 10-20. Up to 8 values, separated by commas, can be typed.	Available
12	Trunk port native VLAN ID	Set a trunk port native VLAN ID from 1 to 4094.	Available
13	The VLAN setting is returned to default.	If returning the VLAN setting to the default, check this item.	Available
14	Spanning tree Port Fast	Select a value for PortFast: Enable or Disable.	Available
15	Uplink failover watch object	Select a value for uplink failover watch object.	Available
16	Uplink failover blockage object	Select an uplink failover watch object.	Available
17	Link aggregation channel group number	Set a number for the link aggregation channel group from 1 to 32.	Available
18	Link aggregation mode	Select a value for link aggregation mode. - active Link aggregation is performed with LACP, and Link Aggregation Control Protocol data unit (LACPDU) is transmitted regardless of the other end device. - on Link aggregation is performed statically. - passive Link aggregation is performed with LACP, and LACPDU is transmitted only when LACPDU is received from the other end device.	Available
19	Link aggregation port priority	Set a value for link aggregation port priority from 0 to 65535. The smaller the value, the higher the priority.	Available
20	This link aggregation setting is deleted.	If deleting the link aggregation setting, check this item.	Available

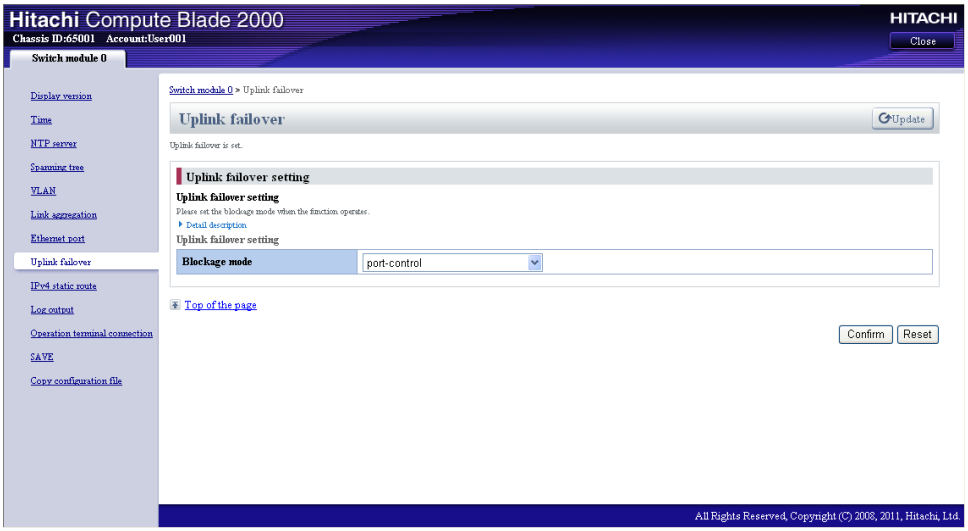


With a 10 G LAN switch module, Port speed and Port connection mode for ports 25 and 26 cannot be changed.

Uplink failover

This section shows the screen for setting uplink failover.

❑ Uplink failover setting screen

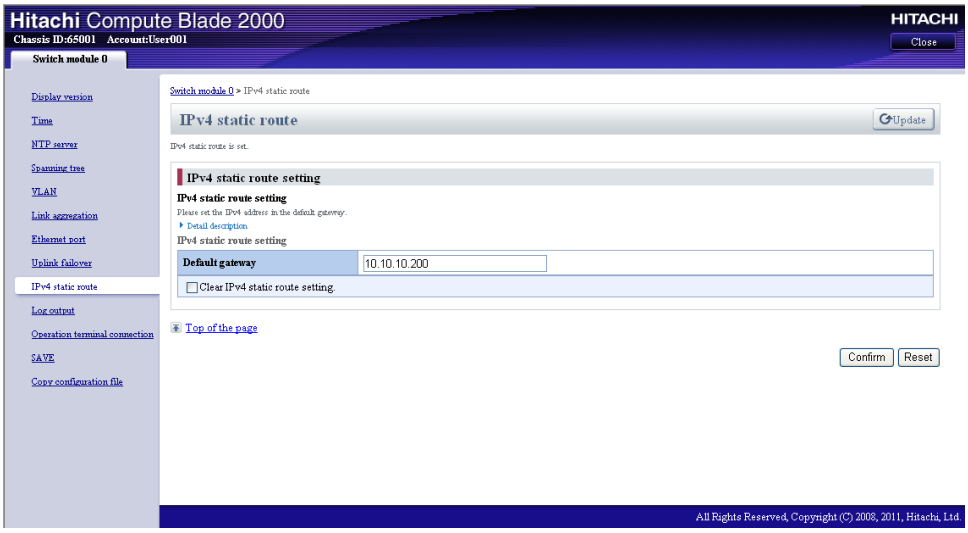


#	Item	Description	Edit
1	Blockage mode	Select a value for blockage mode. - partial-mode Enables the partial control function per port. - port-control Enables the control function per port. - whole-control Enables the function to block every server connection port.	Available

Ipv4 static route

This section shows the screen for setting IPv4 static route.

❑ IPv4 static route setting screen

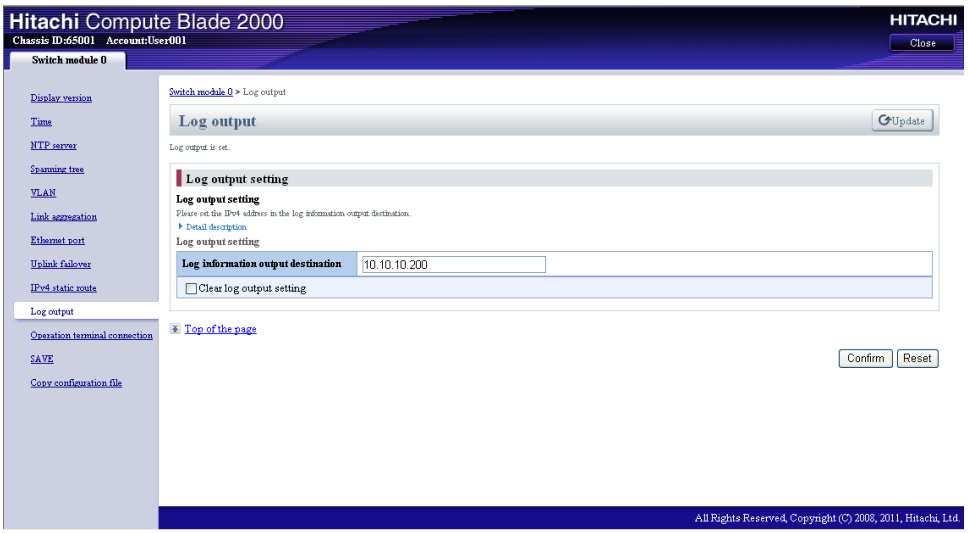


#	Item	Description	Edit
1	Default gateway	Type an IP address to set.	Available
2	Clear IPv4 static route setting.	If deleting the IPv4 static route setting, check this item.	Available

Log output

This section shows the screen for setting a log output destination.

❑ Log output setting screen

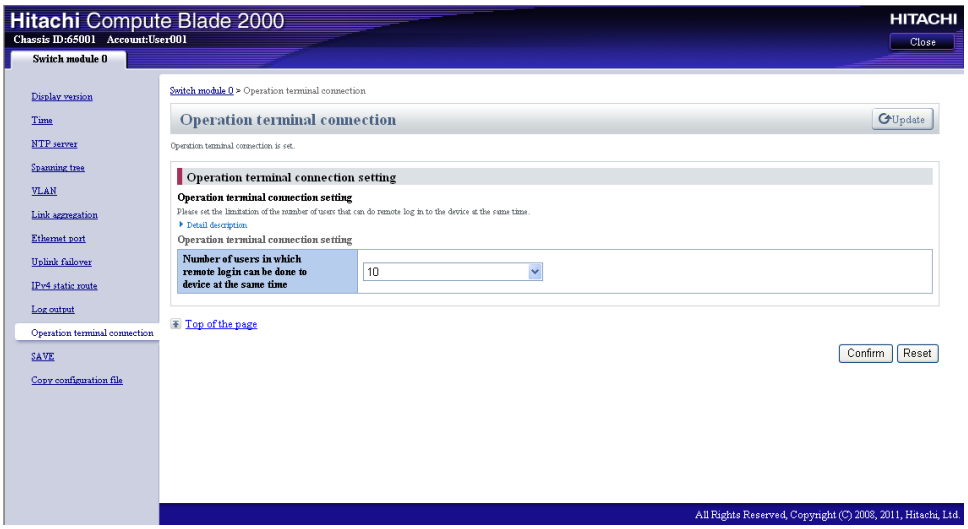


#	Item	Description	Edit
1	Log information output destination	Type an IP address to set.	Available
2	Clear log output setting.	If deleting the log output setting, check this item.	Available

Operation terminal connection

This section shows the screen for setting operation terminal connection.

❑ Operation terminal connection setting screen



#	Item	Description	Edit
1	Number of users in which remote login can be done to device at the same time	Select the number of users who can remotely log in to the device at the same time.	Available

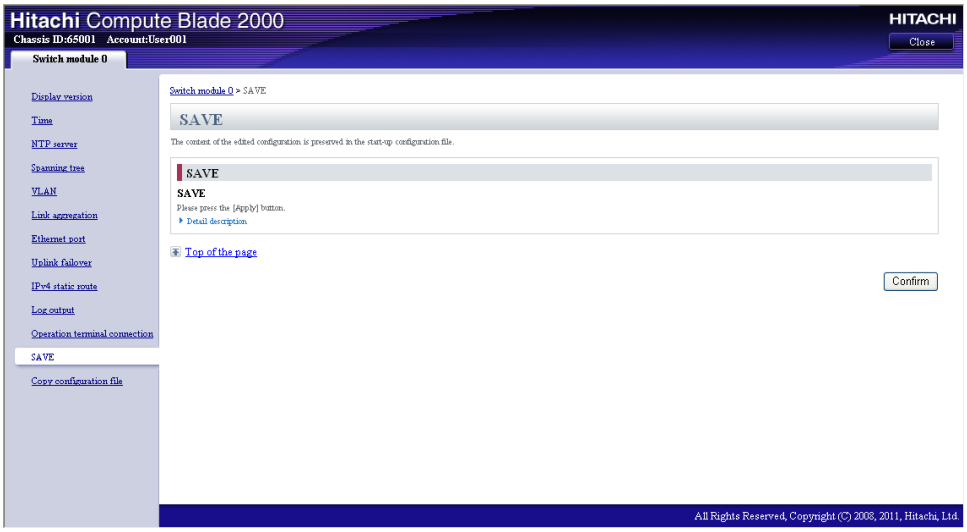
Tip

Set the number of users who can remotely log in the device at the same time to a number from 3 to 16.

SAVE

This section shows the screen for saving the settings configured on each screen into the LAN switch module. If you restart the LAN switch module without performing SAVE, the new settings will be lost. Make sure to write the settings on this screen after completing the LAN switch settings.

❑ SAVE screen

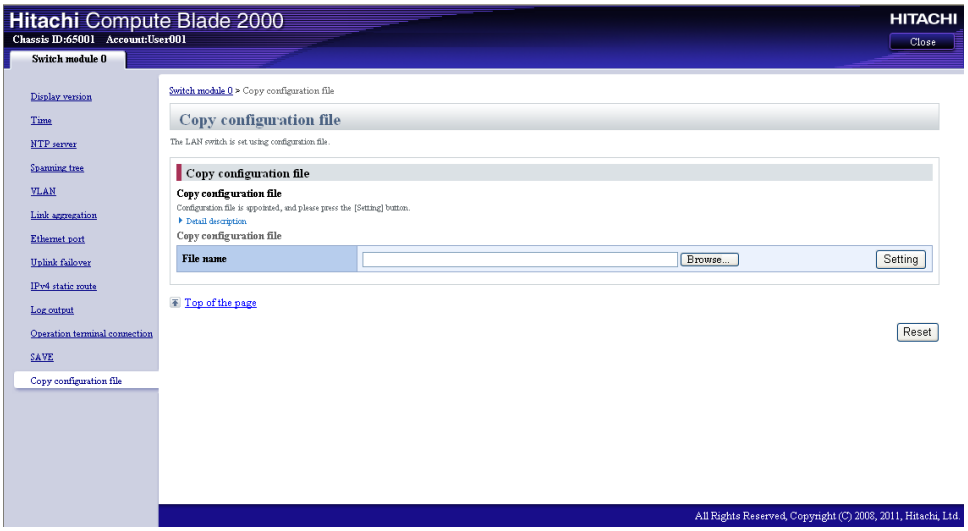


Copy configuration file

This section shows the screen for setting the LAN switch module using the configuration file.

Select a configuration file and click **Setting**. You can use the configuration file backed up for the LAN switch module. See Backup and restore of module information.

❑ Configuration setting screen



8

Configuring the 10-Gb DCB switch module

This chapter provides information about the switch module administrator's password setting that is required at initial installation, adding and deleting user IDs, and module operations.

For details about the operation of the switch module, see the manual in the CD-ROM that came with the switch module.

Notes on use 842
Connection to setup terminal 843
Initial installation operation overview 844
Backup and restore of module information 846
Connection with the server blades 847

Notes on use

- When you have just configured the switch module, the settings will be lost by powering off the switch module. Make sure to perform the copy running-config startup-config command to save the setting information.
- The 10GBASE-R transceiver is available as an option. You can purchase and use the optional item. If you use any 10GBASE-R transceiver other than the option, correct operation or safety is not guaranteed.

Connection to setup terminal

A setup terminal connected via local area network (LAN) or serial cable is initially required. Connect a setup terminal to an external interface of a management module. See “Cable Connection for the System Console” in Chapter 6.

For LAN connection, IP addresses shown in the table below are assigned to switch module slots for 10 Gb Data Center Bridging (DCB) switch modules.

Network connection specifications (shipment setting)

Item	Setting
IP address	switch module2: 192.168.253.37 switch module3: 192.168.253.38 switch module4: 192.168.253.39 switch module5: 192.168.253.40
Subnet mask	255.255.255.240

For serial cable connection, select a 10 Gb DCB switch module to connect using SCO command. See Chapter 6 > System Console Command Reference > Basic operation > SCO Command.

Initial installation operation overview

This section outlines required operations at initial installation.

For details about each operation, see the following sections.



For details about operations other than the operations described below, see the manual contained in the compact disc- Read Only Memory (CD-ROM that came with the module.

1 Login.

Log in to the switch module. Use the user ID "admin" for initial installation. The following table shows factory default settings for the user ID and password.

Item	Factory default setting
User ID	admin
Password	password

2 Setting the switch module administrator’s password.

Set the switch module administrator's password, which is initially fixed as the factory default value. To ensure security against unauthorized access, change the password.

Login

When starting the switch module, you will see the "VDX6746 console login:" prompt.

Following the "VDX6746 console login:", type the user ID. The "Password:" prompt appears. Type `password` to log in to the switch.

```
VDX6746 console login: admin
Password: **************
switch#
```

Note: "`password`" is factory-configured.

Setting the administrator's password

Set the switch module administrator's password.

```
switch# username admin password <specified
password> role admin enable true

(A password for admin is to be the specified password.)
```

Note: "`password`" is factory-configured.

Backup and restore of module information

To protect against unexpected failure, it is recommended that you back up configuration information. Backup information can be used for restoring the previous information when you have changed switch modules.

Backing up configuration

A File Transfer Protocol (FTP) server is required for backing up configuration information. Make sure that your network switch module is connected to the FTP server.

1 Back up configuration using the FTP server.

Example: FTP server IP address: 192.168.0.42; user name: staff; password: password

```
# copy startup-config
ftp://staff:password@192.168.0.42/Bakcup.config_<switch
name>_<date> <= Press [Enter].
```

The backup configuration file, (Backup_config_<switch name>_<date>), is saved in the FTP server by the command above.

2 Store the configuration file saved on the FTP server in media, such as FD and USB memory, and store it in a safe place.

Restoring configuration

An FTP server is required for backing up configuration information. Make sure that your network switch module is connected to the FTP server.

1 Restore configuration using the FTP server.

Example: FTP server IP address: 192.168.0.42; user name: staff; password: password

```
# copy
ftp://staff:password@192.168.0.42/Bakcup.config_<switch
name>_<date> startup-config <= Press [Enter].
```

The backup configuration file is reflected to startup-config by the command above.

2 Perform “reload” to reflect the configuration to the switch module.

```
# reload <= Press [Enter].
```

Connection with the server blades

The following table shows connection between 10 Gb LAN expansion cards and 10 Gb DCB switch modules.

Server blade slot number	Expansion card number	10 Gb LAN port number on the server blade		Switch module slot number	10 Gb DCB switch module line number (factory default)
0	0	NIC0-0	Blade Engine3	2	9
		NIC0-1		3	9
		NIC1-0		2	17
		NIC1-1		3	17
	1	NIC0-0	Blade Engine3	4	9
		NIC0-1		5	9
		NIC1-0		4	17
		NIC1-1		5	17
1	0	NIC0-0	Blade Engine3	2	10
		NIC0-1		3	10
		NIC1-0		2	18
		NIC1-1		3	18
	1	NIC0-0	Blade Engine3	4	10
		NIC0-1		5	10
		NIC1-0		4	18
		NIC1-1		5	18
:		:			
7	0	NIC0-0	Blade Engine3	2	16
		NIC0-1		3	16
		NIC1-0		2	24
		NIC1-1		3	24
	1	NIC0-0	Blade Engine3	4	16
		NIC0-1		5	16
		NIC1-0		4	24
		NIC1-1		5	24



10 Gb DCB switch modules can be installed in switch module slots #2 to #5.

Referring to the table above, if you are going to connect to multiple internal ports of a DCB switch module from a single server blade, you need to use the proper VLAN configuration for the DCB switch module or to use the Intel driver in Windows or ‘bonding’ in Linux for the server blade.

9

Configuring the LAN pass-through module

This chapter describes the local area network (LAN) pass-through module.

1 Gb LAN pass-through module 850
10 Gb LAN pass through module 854

1 Gb LAN pass-through module

Notes on Use

- Line0 to 15 of the LAN pass-through module, which is based on Auto-MDI/MDIX, can be connected with either a cross cable or a straight cable. The line rate of Line0 to 15 is 1000BASE-T only.
- When you use a cable with a covered plug, the cover may interfere with cable connection. If so, remove the cover from the plug to connect it.
- If the cable is difficult to remove, you can use a cable removal tool (CBL) for removing LAN cables as described in the following steps.
  1. Insert the plug firmly to unlock the plug.
  2. Place the tip of the CBL removal tool, which is attached to the LAN pass-through module, on the latch of the plug, and press the latch.
  3. While pressing the latch, pull out the cable.
- Keep the CBL removal tool for removing a LAN cable attached to the LAN pass-through module.

Connection with Server Blades

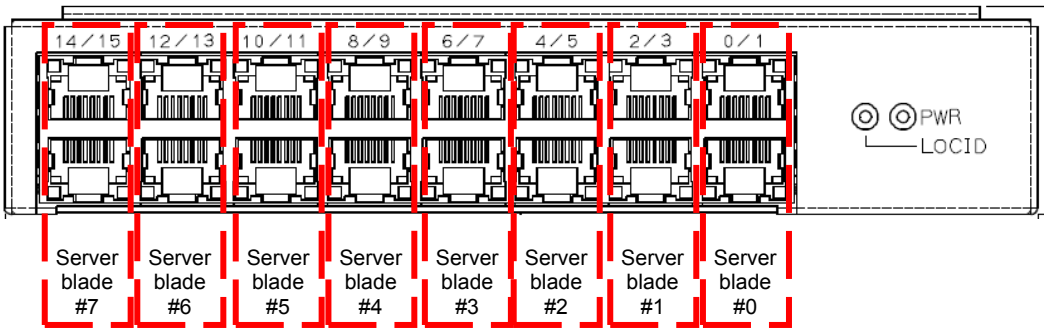
Each server blade equips ten LAN ports. Connection between these LAN ports and the LAN pass-through module is shown in the table below:

Slot number of server blade	1 Gb LAN port number on server blade		Slot number: 1 Gb LAN pass-through module installed	Line number of 1 Gb LAN pass-through module
0	LAN1	82576	0	Line0
	LAN2		1	Line0
	LAN3	82576	2	Line0
	LAN4		3	Line0
	LAN5	82576	2	Line1
	LAN6		3	Line1
	LAN7	82576	4	Line0
	LAN8		5	Line0
	LAN9	82576	4	Line1
	LAN10		5	Line1
1	LAN1	82576	0	Line2
	LAN2		1	Line2
	LAN3	82576	2	Line2
	LAN4		3	Line2
	LAN5	82576	2	Line3
	LAN6		3	Line3
	LAN7	82576	4	Line2
	LAN8		5	Line2
	LAN9	82576	4	Line3
	LAN10		5	Line3
2	LAN1	82576	0	Line4
	LAN2		1	Line4
	LAN3	82576	2	Line4
	LAN4		3	Line4
	LAN5	82576	2	Line5
	LAN6		3	Line54
	LAN7	82576	4	Line4
	LAN8		5	Line4
	LAN9	82576	4	Line5
	LAN10		5	Line5
3	LAN1	82576	0	Line6
	LAN2		1	Line6
	LAN3	82576	2	Line6
	LAN4		3	Line6
	LAN5	82576	2	Line7
	LAN6		3	Line7

Slot number of server blade	1 Gb LAN port number on server blade		Slot number: 1 Gb LAN pass-through module installed	Line number of 1 Gb LAN pass-through module
	LAN7	82576	4	Line6
	LAN8		5	Line6
	LAN9	82576	4	Line7
	LAN10		5	Line7
4	LAN1	82576	0	Line8
	LAN2		1	Line8
	LAN3	82576	2	Line8
	LAN4		3	Line8
	LAN5	82576	2	Line9
	LAN6		3	Line9
	LAN7	82576	4	Line8
	LAN8		5	Line8
	LAN9	82576	4	Line9
	LAN10		5	Line9
5	LAN1	82576	0	Line10
	LAN2		1	Line10
	LAN3	82576	2	Line10
	LAN4		3	Line10
	LAN5	82576	2	Line11
	LAN6		3	Line11
	LAN7	82576	4	Line10
	LAN8		5	Line10
	LAN9	82576	4	Line11
	LAN10		5	Line11
6	LAN1	82576	0	Line12
	LAN2		1	Line12
	LAN3	82576	2	Line12
	LAN4		3	Line12
	LAN5	82576	2	Line13
	LAN6		3	Line13
	LAN7	82576	4	Line12
	LAN8		5	Line12
	LAN9	82576	4	Line13
	LAN10		5	Line13
7	LAN1	82576	0	Line14
	LAN2		1	Line14
	LAN3	82576	2	Line14
	LAN4		3	Line14
	LAN5	82576	2	Line15
	LAN6		3	Line15
	LAN7	82576	4	Line14

Slot number of server blade	1 Gb LAN port number on server blade		Slot number: 1 Gb LAN pass-through module installed	Line number of 1 Gb LAN pass-through module
	LAN8		5	Line14
	LAN9	82576	4	Line15
	LAN10		5	Line15

Tip To use LAN3 to 10, a blade requires a LAN mezzanine card.



Interface connector to server blade

10 Gb LAN pass-through module

Notes on use

⚠ DANGER

Do not look directly into the laser beam. Do not look into the laser beam using an optical instrument. Small form-factor pluggable plus (SFP+) optical transceiver uses a laser beam that is colorless, transparent, and invisible and can damage your eyes.

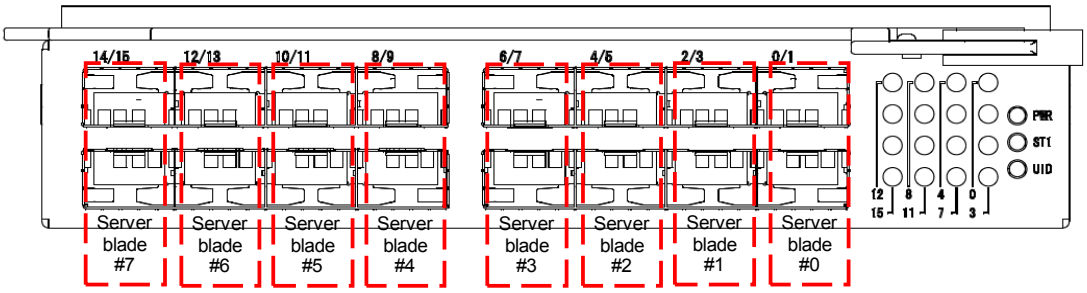
⚠ CAUTION

Make sure to purchase and use the optional SFP+ transceiver. If not, proper behavior and safety cannot be guaranteed. Consult your reseller for details.

Connection with server blades

Slot number of server blade	Mezzanine card number	10 Gb LAN port number on server blade		Slot number: 10 Gb LAN pass through module installed	Line number of 10 Gb LAN pass through module
0	0	NIC0-0	Blade Engine3	2	Line0
		NIC0-1		3	Line0
		NIC1-0	Blade Engine3	2	Line1
		NIC1-1		3	Line1
	1	NIC0-0	Blade Engine3	4	Line0
		NIC0-1		5	Line0
		NIC1-0	Blade Engine3	4	Line1
		NIC1-1		5	Line1
1	0	NIC0-0	Blade Engine3	2	Line2
		NIC0-1		3	Line2
		NIC1-0	Blade Engine3	2	Line3
		NIC1-1		3	Line3
	1	NIC0-0	Blade Engine3	4	Line2
		NIC0-1		5	Line2
		NIC1-0	Blade Engine3	4	Line3
		NIC1-1		5	Line3
2	0	NIC0-0	Blade Engine3	2	Line4
		NIC0-1		3	Line4
		NIC1-0	Blade Engine3	2	Line5
		NIC1-1		3	Line5
	1	NIC0-0	Blade Engine3	4	Line4
		NIC0-1		5	Line4
		NIC1-0	Blade Engine3	4	Line5
		NIC1-1		5	Line5
3	0	NIC0-0	Blade Engine3	2	Line6
		NIC0-1		3	Line6
		NIC1-0	Blade Engine3	2	Line7
		NIC1-1		3	Line7
	1	NIC0-0	Blade Engine3	4	Line6
		NIC0-1		5	Line6
		NIC1-0	Blade Engine3	4	Line7
		NIC1-1		5	Line7
4	0	NIC0-0	Blade Engine3	2	Line8
		NIC0-1		3	Line8
		NIC1-0	Blade Engine3	2	Line9
		NIC1-1		3	Line9
	1	NIC0-0	Blade	4	Line8

Slot number of server blade	Mezzanine card number	10 Gb LAN port number on server blade		Slot number: 10 Gb LAN pass through module installed	Line number of 10 Gb LAN pass through module
4	1	NIC0-1	Engine3	5	Line8
		NIC1-0	Blade Engine3	4	Line9
		NIC1-1		5	Line9
5	0	NIC0-0	Blade Engine3	2	Line10
		NIC0-1		3	Line10
		NIC1-0	Blade Engine3	2	Line11
		NIC1-1		3	Line11
	1	NIC0-0	Blade Engine3	4	Line10
		NIC0-1		5	Line10
		NIC1-0	Blade Engine3	4	Line11
		NIC1-1		5	Line11
6	0	NIC0-0	Blade Engine3	2	Line12
		NIC0-1		3	Line12
		NIC1-0	Blade Engine3	2	Line13
		NIC1-1		3	Line13
	1	NIC0-0	Blade Engine3	4	Line12
		NIC0-1		5	Line12
		NIC1-0	Blade Engine3	4	Line13
		NIC1-1		5	Line13
7	0	NIC0-0	Blade Engine3	2	Line14
		NIC0-1		3	Line14
		NIC1-0	Blade Engine3	2	Line15
		NIC1-1		3	Line15
	1	NIC0-0	Blade Engine3	4	Line14
		NIC0-1		5	Line14
		NIC1-0	Blade Engine3	4	Line15
		NIC1-1		5	Line15



Interface connector to server blade

10

Configuring the Fibre-channel switch module

This chapter provides information about the module operation as well as how to connect the system and how to set the system administrator's password.

For the details about the operation of the Fibre-channel switch module, see the user’s guide in the Hitachi Compute Blade Fibre Channel Switch Accessory DVD (EN) that came with the Fibre-channel switch module.

Notes on use 858
Connection to setup terminal 859
Initial installation operation overview 862
Connection with server blades 863
Backup and restore of module information 867

Notes on use

DANGER!

- Do not look directly into inside of the fibre channel port in operation. The optical module equipped with this equipment uses laser beam. If you do, the laser beam can damage your eyes.
- Make sure to attach a port protector to any optical modules to which a fibre cable is not connected.

See the following manuals in the “Hitachi Compute Blade Fibre Channel Switch Accessory DVD (EN)” attached to the device.

- Access Gateway Administrator’s Guide
- Fabric Watch Administrator’s Guide
- Fabric OS Administrator’s Guide
- Fabric OS Command Reference
- Fabric OS Message Reference
- Fabric OS MIB Reference
- Web Tools Administrator’s Guide

❑ Accessories

The following accessories are attached to the built-in Fibre-channel switch.

- Short-wave SFP+ module

  8 Gbps short-wave small form-factor pluggable plus (SFP+) modules are installed in the module.

  Each built-in Fibre-channel switch contains two or four modules. When using more modules than those installed in each Fibre-channel switch, purchase optional SFP+ modules.

- DVD: Hitachi Compute Blade 2000 Fibre-channel Switch Accessory DVD (EN)

  The attached DVD contains the manuals, MIB file, and data for maintenance.

  For details, see the “Readme.txt” in the DVD.

❑ Powering on and off

When AC power is supplied to the Compute Blade 2000, the built-in Fibre-channel switch is automatically turned on.

You can turn on and off each switch separately using the management module system console command or system Web console.

Connection to setup terminal

A setup terminal connected via a local area network (LAN) or serial cable is initially required.
This section describes how to connect a terminal to the module in each method.

LAN interface connection

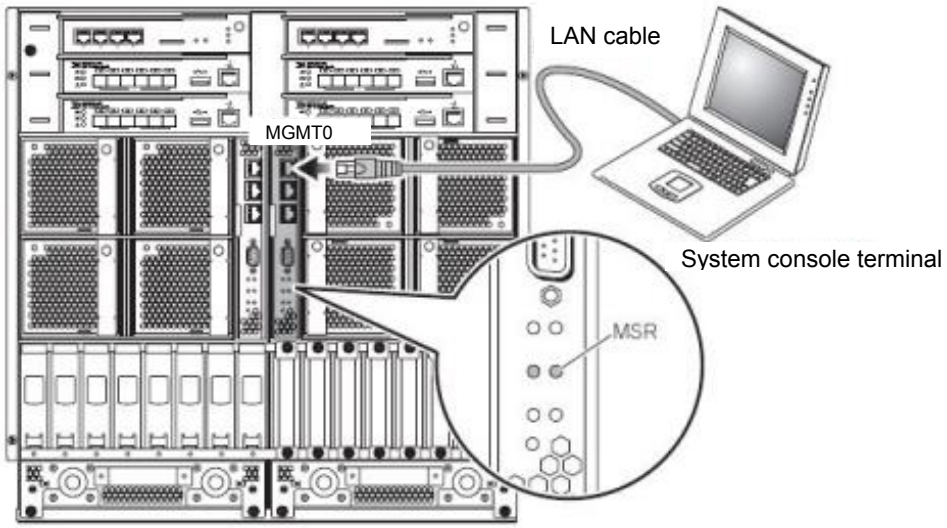
You can access the built-in Fibre-channel switch through the LAN port of the management module or the LAN port of the built-in Fibre-channel switch for managing the built-in Fibre-channel switch. You can determine which LAN port to use and set it by using the LAN configuration (LC) command, a system console command of the management module.

Network connection specifications (default value set during shipment)

Item	Setting value
IP address	switch module2: 192.168.253.37 switch module3: 192.168.253.38 switch module4: 192.168.253.39 switch module5: 192.168.253.40
Subnet mask	255.255.255.240
Connection type	Dedicated to the management module

- Via LAN port of the management module

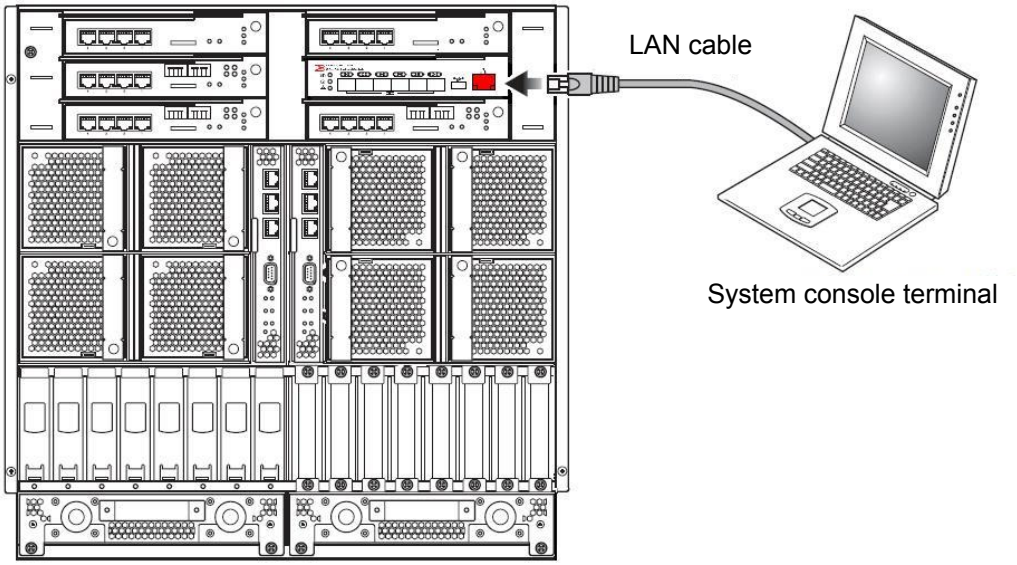
  When the connection setting is dedicated to the management module, you can access the switch module via the management module. You can also access directly to the switch module through a management module port, MGMT0 or MGMT1. These settings can be changed using the management module system console command or Web console.



Connect your system console terminal to the MGMT0 port of the management module at the rear of the system via the LAN cable. When two management modules are installed, connect the system console with the MSR LED that lights solid green. Prepare the LAN cable for connection.

- Via LAN port of the built-in Fibre-channel switch

  When connecting to the LAN port of the built-in Fibre-channel switch, you can change the connection setting using the system console command of the management module.

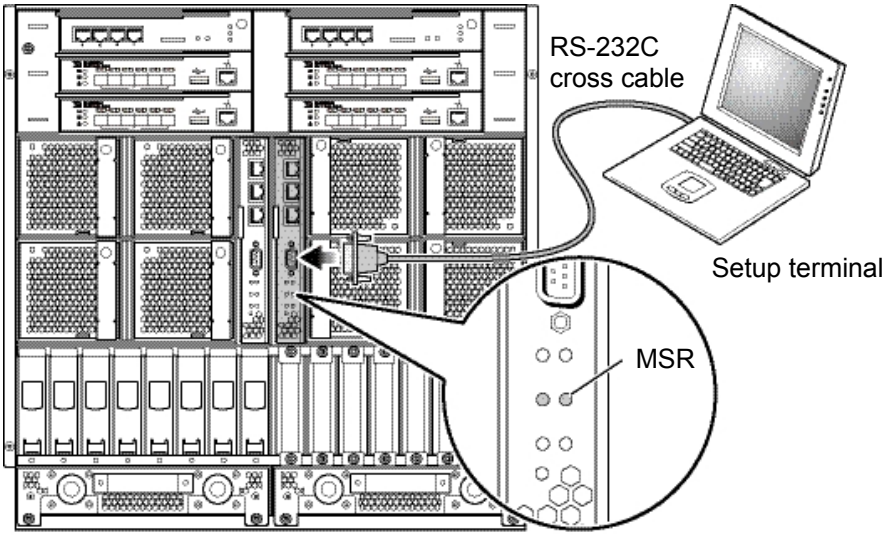


Serial interface connection

Select a built-in Fibre-channel switch module to connect using the SCO command described in Chapter 6. Then connect your setup terminal to the serial port on the management module installed in the system equipment using the RS-232C cross cable.

When two management modules are installed, connect to the management module with the Master (MSR) light emitting diode (LED) that lights solid green.

Prepare the RS-232C cross cable for connection.



Requirements for the setup terminal

Item		Specification
Communication port		RS-232C port
Communication software		Any of the following communications software products or its equivalent communication software - Hyper terminal attached to Windows 2000 or Windows XP - Tera Term Pro (Version 2.3)
Communication setting	Communication protocol	ZMODEM protocol
	Communication parameter	8 bits, 1 stop bit, no parity
	Communication rate *1	9600 bits/s

*1 In settings of this system at the time of shipment, the communication speed of the CONSOLE port is set in 9600 bits/s. Do not use a communication rate other than 9600 bits/s.

Initial installation operation overview

For details about how to log in via the LAN or serial connection, and for operation during the initial installation, see the user's guide in the Hitachi Compute Blade 2000 Fibre Channel Switch Accessory CD (EN) that came with the device.

❑ Port number

Port numbers of the built-in Fibre-channel switch are assigned as follows:

Server blade slot 0	6	Built-in fiber channel switch	0	External port
Server blade slot 1	7		1	External port
Server blade slot 2	8		2	External port
Server blade slot 3	9		3	External port
Server blade slot 4	10		4	External port
Server blade slot 5	11		5	External port
Server blade slot 6	12			
Server blade slot 7	13			
(Unconnected)	14			
(Unconnected)	15			
Server blade slot 0	16			
Server blade slot 1	17			
Server blade slot 2	18			
Server blade slot 3	19			
Server blade slot 4	20			
Server blade slot 5	21			
Server blade slot 6	22			
Server blade slot 7	23			
(Unconnected)	24			
(Unconnected)	25			

❑ Active port setting

You can use 12 or 22 ports out of 26 ports of a built-in Fibre-channel switch, and also change ports available in the setting. For information about how to set available ports, see the user's guide in the Hitachi Compute Blade 2000 Fibre Channel Switch Accessory CD (EN)" that came with the device.

Model name	Total number of active ports	Number of active port
GVX-BE2FSW1X1/ GV-BE2FSW1X1-Y	12	0-3, 6-13
GVX-BE2FSW2X1	22	0-5, 6-13, 16-23

Connection with server blades

Connection between server blades and built-in Fibre-channel switches is described in the table below:

With 2-port Fibre-channel mezzanine cards installed:

Slot number of server blade	Port number on server blade		Fibre-channel switch module	
	Number of mezzanine card	Port number of Fibre-channel	Slot number	Port number
0	0	0	2	6
		1	3	6
	1	0	4	6
		1	5	6
1	0	0	2	7
		1	3	7
	1	0	4	7
		1	5	7
. . . . . .				
7	0	0	2	13
		1	3	13
	1	0	4	13
		1	5	13
Unconnected			2-5	14-25

With 4-port Fibre-channel mezzanine card installed:

Slot number of server blade	Port number on server blade		Fibre-channel switch module	
	Number of mezzanine card	Port number of Fibre-channel	Slot number	Port number
0	0	0	2	6
		1		16
		2	3	6
		3		16
	1	0	4	6
		1		16
		2	5	6
		3		16
1	0	0	2	7
		1		17
		2	3	7
		3		17
	1	0	4	7
		1		17
		2	5	7
		3		17
. . . . . .				
7	0	0	2	13
		1		23
		2	3	13
		3		23
	1	0	4	13
		1		23
		2	5	13
		3		23
Unconnected			2-5	14-15, 24-25

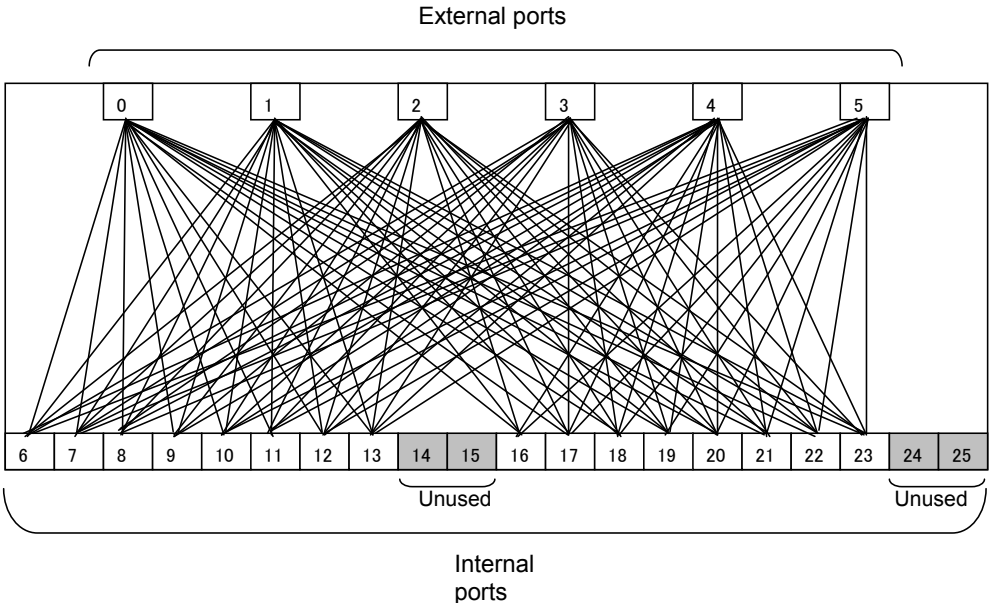
❑ Zone setting at shipment

A built-in Fibre-channel switch contains zone settings set by default at the time of shipment. The default values of the settings are shown in the table below.



If you have asked Hitachi for setting the built-in Fibre-channel switch using our service menu, the settings are different from those shown in the table below. For details about zone setting, contact a Hitachi sales representative.

Name of zone configu-ration	Assigned zone name	Port #	Name of zone configu-ration	Assigned zone name	Port #	Name of zone configu-ration	Assigned zone name	Port #
FCSW1	zone0006	0, 6	FCSW1	zone0206	2, 6	FCSW1	zone0406	4, 6
	zone0007	0, 7		zone0207	2, 7		zone0407	4, 7
	zone0008	0, 8		zone0208	2, 8		zone0408	4, 8
	zone0009	0, 9		zone0209	2, 9		zone0409	4, 9
	zone0010	0, 10		zone0210	2, 10		zone0410	4, 10
	zone0011	0, 11		zone0211	2, 11		zone0411	4, 11
	zone0012	0, 12		zone0212	2, 12		zone0412	4, 12
	zone0013	0, 13		zone0213	2, 13		zone0413	4, 13
	zone0016	0, 16		zone0216	2, 16		zone0416	4, 16
	zone0017	0, 17		zone0217	2, 17		zone0417	4, 17
	zone0018	0, 18		zone0218	2, 18		zone0418	4, 18
	zone0019	0, 19		zone0219	2, 19		zone0419	4, 19
	zone0020	0, 20		zone0220	2, 20		zone0420	4, 20
	zone0021	0, 21		zone0221	2, 21		zone0421	4, 21
	zone0022	0, 22		zone0222	2, 22		zone0422	4, 22
	zone0023	0, 23		zone0223	2, 23		zone0423	4, 23
	zone0106	1, 6		zone0306	3, 6		zone0506	5, 6
	zone0107	1, 7		zone0307	3, 7		zone0507	5, 7
	zone0108	1, 8		zone0308	3, 8		zone0508	5, 8
	zone0109	1, 9		zone0309	3, 9		zone0509	5, 9
	zone0110	1, 10		zone0310	3, 10		zone0510	5, 10
	zone0111	1, 11		zone0311	3, 11		zone0511	5, 11
	zone0112	1, 12		zone0312	3, 12		zone0512	5, 12
	zone0113	1, 13		zone0313	3, 13		zone0513	5, 13
	zone0116	1, 16		zone0316	3, 16		zone0516	5, 16
	zone0117	1, 17		zone0317	3, 17		zone0517	5, 17
	zone0118	1, 18		zone0318	3, 18		zone0518	5, 18
	zone0119	1, 19		zone0319	3, 19		zone0519	5, 19
	zone0120	1, 20		zone0320	3, 20		zone0520	5, 20
	zone0121	1, 21		zone0321	3, 21		zone0521	5, 21
	zone0122	1, 22		zone0322	3, 22		zone0522	5, 22
	zone0123	1, 23		zone0323	3, 23		zone0523	5, 23



❑ Unused internal ports: disabled

Built-in Fibre-channel switches can save energy consumption by disabling unused ports. Unused ports are automatically disabled under the following conditions in Compute Blade 2000.

<Requirements for internal ports to be automatically disabled>

- Internal ports to the slot of a server blade that is not installed or power is not supplied to.
- Internal ports not connected to any Fibre-channel mezzanine card.

```
<Example>  :  Displays switchshow command of a built-in fibre channel switch

BR5460:admin> switchshow

----- <omitted in the middle> -----

Area Port Media Speed State Proto
====================================
  0   0   id   N8   No_Light
----- <omitted in the middle> -----

  6   6   cu   N    No_Sync   Disabled (Persistent)
  7   7   cu   N8   Online    F-Port   50:00:08:70:00:57:31:78

----- <omitted in the middle> -----
 25  25   cu   N8   Online
```

Automatically disabled.

Internal ports

Backup and restore of module information

For information about how to backup and restore Fibre-channel switch modules see the user's guide in the Hitachi Compute Blade 2000 Fibre Channel Switch Accessory CD (EN) that came with the device.

11

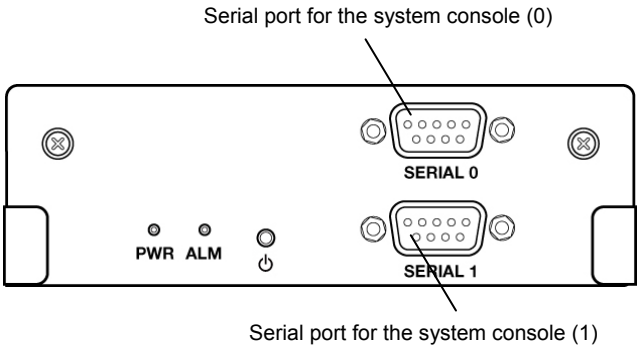
I/O slot expansion unit

This chapter describes how to set the I/O slot expansion unit.

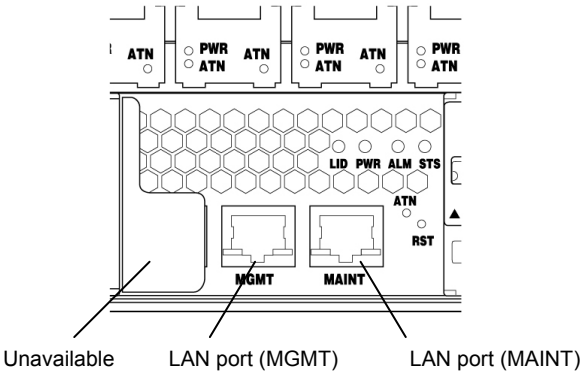
External interface for the I/O slot expansion unit 870
Cable connection to the I/O slot expansion unit 872
Initial settings of the I/O slot expansion unit 874
Backup and restore the settings 876
Account 879
Privilege and role 881
System console command reference 882
Alert log message 989

External interface for the I/O slot expansion unit

❑ Front panel



❑ Rear panel



Port number	Description
LAN port (MGMT)	Port for connecting to the management network: Connect this port during the initial setting.
LAN port (MAINT)	Dedicated port for maintenance. Only maintenance personnel can use this port. Any user cannot use this.
Serial Port	Serial port for the system console: used for maintenance when a local area network (LAN) port is not available. Serial port for the system console (0): used for connection to I/O module 0. Serial port for the system console (1): used for connection to I/O module 1.

Tip

Prepare the following items for connection via the LAN port:

- A terminal for the system console
- Unshielded twisted pair (UTP) cable: UTP-5 or above
- Client software: Telnet or Secure SHell (SSH)

When you connect an I/O module via Telnet or SSH, refer to the following table about the default setting of the I/O module at the time of shipment:

Item	Setting at the shipment
IP address	192.168.0.65
Subnet mask	255.255.255.0
SSH	Enabled
Telnet	Enabled

■ Prepare the following items for connection via the serial port.

- A terminal for the system console
- A connecting cable for the serial port (RS-232C cross cable D-SUB9 pin female-female connector)
- Terminal software such as Hyper Terminal: available for VT100 emulation

When you connect to the serial port of an I/O module, refer to the following table about communication parameter settings to the terminal software.

Communication parameter	Setting
Communication rate	9600 bps
Data	8 bits
Parity	None
Stopbit	1 bit
Flow control	None

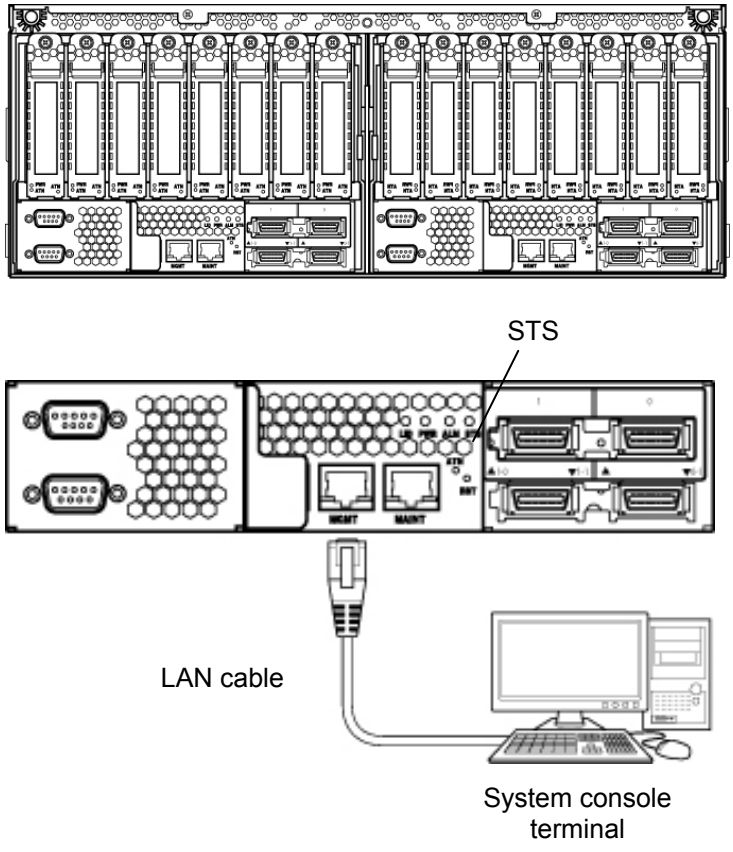
Cable connection to the I/O slot expansion unit

Connection with LAN cable

Note

Failure occurs in an I/O slot expansion unit connected to a network, if a device with the same IP address as that of the I/O slot expansion unit exists on the network. Configure the network settings of the I/O slot expansion unit before connecting the unit to the network.

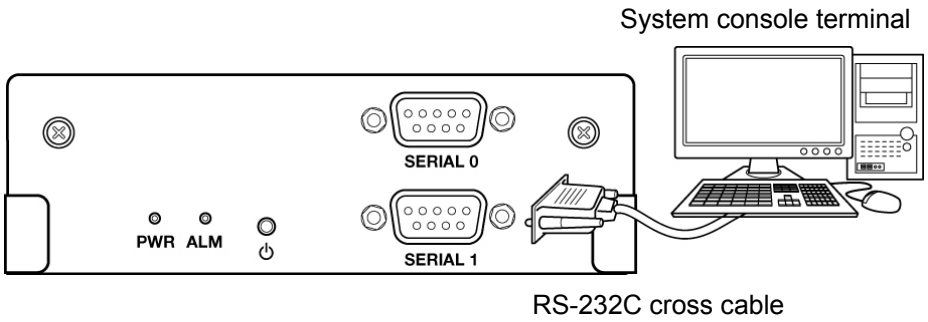
Both straight cable or cross cable are available for the LAN port for the system console. 10/100 Mbps is automatically selected as the communication rate.



Connect the MGMT0 port of the I/O module in the back of the I/O slot expansion unit to your system console terminal using a LAN cable. Since two I/O modules are installed, connect to the I/O module with the status LED (STS) that lights solid orange. Prepare a LAN cable to connect to the terminal.

Connection with serial cable

Use a RS-232C cross cable (D-SUB9 pin female-female) for the serial port of the system console. Communication rate setting at the time of shipment is 9600 bps.



Connect the serial port in the front panel of the I/O slot expansion unit to your system console terminal using a RS-232C cross cable. Since two I/O modules are installed, connect to the I/O module with the STS that lights solid orange. Prepare the RS-232C cross cable to connect to the terminal.

Initial settings of the I/O slot expansion unit

The I/O slot expansion unit must be initialized for your environment.

This section describes how to initialize the I/O slot expansion unit.

The following data needs to be initialized:

- Password for the administrator account
- Setting of device identification information
- Setting of network information such as IP addresses

To set items above, use the console functions.

Initial settings via system console

(1) First login

1 Boot the client software, such as Telnet or Serial terminal software, of the system console.

2 Specify `192.168.0.65` to connect the client software, which is not required for serial connection, and start the connection.

3 Fixed user account and password are set to Administrator account for the system console at the time of shipment. Type the following user account and password to login.

Item	Setting at the shipment
User account	administrator
Password	password

4 When login is successful, you can type a command to perform.

```
Compute Blade 2000 I/O slot expansion unit I/O Module
ALL RIGHTS RESERVED,COPYRIGHT (C), 2010, HITACHI,LTD.
Chassis ID        : 5713RF0 00108
Firmware Revision : A0100-Z-919

Use EX Command to logout.
Use HE Command to get a list of available commands.

5713RF0 00108(0)IOEU>
```

(2) Password change in Administrator account

See “SO Command” in Chapter 6.



It is recommended that the Administrator account password be changed.

(3) Device identifier setting

See “CI Command” in Chapter 6.

(4) Network information setting, such as IP address

See “LC command” in Chapter 6.

(5) Logout

Execute the EX command at prompt to logout.

```
5713RF0 00108(0)IOEU> EX (Enter)
[Clear the screen.]
[Disconnected.]
```

Backup and restore the settings

The following setting can be saved and restored from the I/O slot expansion unit.

Item	Operation available
I/O slot expansion unit setting	Backup and Restore

Backup the I/O slot expansion unit settings

1 Log in to the system console as Administrator.

2 Type `UBR`, and press **Enter**.

```
Compute Blade 2000 I/O slot expansion unit I/O Module
ALL RIGHTS RESERVED,COPYRIGHT (C), 2010, HITACHI,LTD.
Chassis ID        : 5713RF0 00108
Firmware Revision : A0100-Z-919

Use EX Command to logout.
Use HE Command to get a list of available commands.

5713RF0 00108(0)IOEU>UBR (Enter)

<< UBR - Backup and restore setting. >>

-- Backup and restore setting menu --
    B. Backup.
    R. Restore.
    Q. Quit.
(B,R,[Q]):
```

3 Type `B` in the menu and press **Enter**. A message asks you to input a backup file name.

```
(B,R,[Q]):B (Enter)

Input backup file name ([Quit]):
```

4 When you type a file name string, a confirmation message is displayed and the prompt is ready. Type `Y` and press **Enter**. A file with the setting is created. To cancel the setting backup, type `N` and press **Enter** after the confirmation message. When the file has been created, the file name is displayed and the prompt is ready. Press **Enter**, and the screen returns to the menu.

```
Input backup file name ([Quit]):conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is io-conf.backup.
Hit enter key. (Enter)
```

5 You can take the created file with FTP or SFTP, which is stored in the user directory of the I/O slot expansion unit. The account name and password is the same as those used in logging into the console.

Restore the I/O slot expansion unit settings

1 Transfer the file with the settings to the I/O slot expansion unit with File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP). Log into FTP or SFTP using the same account name and password as those used in logging into the console Log into the Web console as Administrator.

2 Log in to the console as Administrator.

3 Type `UBR` at prompt, and press **Enter**.

```
Compute Blade 2000 I/O slot expansion unit I/O Module
ALL RIGHTS RESERVED,COPYRIGHT (C), 2010, HITACHI,LTD.
Chassis ID        : 5713RF0 00108
Firmware Revision : A0100-Z-919

Use EX Command to logout.
Use HE Command to get a list of available commands.

5713RF0 00108(0)IOEU>UBR (Enter)

<< UBR - Backup and restore setting. >>

-- Backup and restore setting menu --
    B. Backup.
    R. Restore.
    Q. Quit.
(B,R,[Q]):
```

4 Type R in the menu and press **Enter**. The file list with settings stored in the user directory is displayed.

```
(B,R,[Q]):R (Enter)

-- Backup file list --
<File0>
io-conf.backup

Select backup file (0,[Q=Quit]):
```

5 Check the file name, type a number to specify the file, and press **Enter**. A warning message indicating that the session will be disconnected for restarting the I/O slot expansion unit is displayed. A confirmation message is displayed and the prompt is ready.

```
Select backup file (0,[Q=Quit]) : 0 (Enter)

WARNING : If confirm, this connect is lost.

Confirm? (Y,[N]):
```

6 Type Y and press **Enter**, and the setting restoration starts. The I/O slot expansion unit will restart after the setting restoration. To cancel the setting restoration, type N and press **Enter,** or just press Enter.

```
Confirm? (Y,[N]): Y (Enter)
-   <I/O module0> Restarting
-   [Disconnected.]
```

Account

Account overview

❑ Purpose of account

You need to set accounts for the following purposes.

(1) To log in to the console

When logging in to the console, you can view the state of a device or change settings. For login, an account should be specified and authentication for the account should be required. With accounts, people who can access the device can be specified. Available functions can be limited using a combination of accounts and role definition.

(2) To transfer files via FTP or SFTP

Files can be transferred between the user directory in an I/O slot expansion unit and a terminal connected using LAN via FTP or SFTP. You need to specify an account for the unit, and the account should be authenticated before transferring files.

❑ Account specifications

The following table shows the account specifications to be registered in the I/O slot expansion unit. You need to set the following items at or after the account setting.

#	Item	Description
1	Account name	- An account name It can contain up to 32 characters with the following conditions: First character: Alphabetic character Second and subsequent characters: Alphanumeric characters, hyphens (-), underscores (_), and periods (.).
2	Status	Indicates whether an account is enabled or disabled. With Enabled, the account is available.
3	Role	Role names to be assigned to an account. See Privilege and role for the details of Role.
4	Type of prompt	Type of a prompt displayed Select one from “IOEU>” fixed and “chassis ID (a slot number of the I/O module slot number) IOEU>”.
5	Timeout minutes	Time to wait until an automatic logout occurs. The wait time can be set in minutes from 0 to 1440 for the console. If 0 is set, however, the automatic logout function is disabled.
6	Password	A password required for authentication It can contain at least one and up to 32 printable American Standard Code for Information Interchange (ASCII) characters from character codes 0x20 to 0x7e. Keep your password in a safe place because no password string is displayed on the screen.
7	SSH public key	Public keys, used for SSH authentication, can be registered per account. Up to five public keys can be registered to one account. The key algorithm supports RSA (the first-described public-key cryptosystem) and digital signature algorithm (DSA). It is recommended that the key length should be 1024 bits or over.

❑ Account setting

You can use the console to set accounts. For procedures, see “SO command”.

Privilege and role

Privilege, role, and account

Using the I/O slot expansion unit console function, you can define a role with specified privileges by adding or removing each privilege for your user management. The following table describes privileges that can be set to a role.

Privilege list

#	Privilege	Description
1	Chassis	Can set and operate a chassis.
2	Network	Can set a network.
3	Account	Can add and delete accounts or roles.

The following role account is set at the shipment.

Defined roles at the shipment

#	Role name	Privilege		
		Account	Chassis	Network
1	Administrator	Permitted	Permitted	Permitted

Defined account at shipment

#	Account name	Default password	Assigned role	Description
1	administrator	password	Administrator	Unit manager with all privileges

System console command reference

Command list

1 Basic operation

Command	Description	See page:
EX	Finishes the system console.	884
HE	Help	885
SCO	Console setting	886
WHO	Session information	887

2 Chassis management

Command	Description	See page:
CI	Chassis ID setting	888
SD	Time setting	889
SDN	Shutdown the unit	891
PES	Sets PCI express expander.	892
PS	Displays status of all modules.	895
DF	Displays modules installed in the unit.	897
DH	Displays riser boards and I/O adapter module.	900
WWN	Displays WorldWideName.	903
PSM	Displays status of power modules and sets those modules.	905
IOC	Operates the I/O module.	906
FAN	Displays the FAN module status.	909
DL	Log	910
DEL	Deletes files in the user directory of the I/O module.	924
FW	Displays the firmware version and updates the dictionary.	925
LM	Sets a language to use onscreen.	927

3 Network management

Command	Description	See page:
LC	Management network setting	929
LFT	Redundant setting for LAN	931
LS	Displays MAC address.	933
XD	Network diagnosis	934
MLC	Reference for maintenance network setting	935
ILC	Internal LAN setting	936

4 External server connection management

Command	Description	See page:
BSM	SC/BSM linkage setting	937
SNM	SNMP setting	942
MI	E-mail setting	950
LDAP	Directory service connection setting	963

5 Security management

Command	Description	See page:
CER	Operates SSH public keys.	969
SEC	Service setting	971
SO	Role and account setting	974

6 Backup and restore the configuration

Command	Description	See page:
DC	Restores to the default setting at the shipment	985
UBR	Backups and restores I/O module configuration.	986

Basic operation

- Press **Enter** at the prompt to input the I/O module.
- When an option in parentheses is displayed, characters in parentheses can be entered.
- [Q] means that the screen goes to the prompt or returns to the previous menu.
- [Unchange] means that you do not change it.
- Characters in brackets mean that you can enter the value by pressing **Enter**.
- Prompt is displayed in the following composition.

  [Chassis ID] ([the slot number of the I/O module that currently logs in]) IOEU>

  Ex) the slot number is 0 of the I/O module that logs in with Chassis ID 5713RF0 NNNNN:

```
5713RF0 NNNNN(0)IOEU>
```

❑ EX command

This command finishes the system console and executes disconnection. For disconnection, type `EX` at prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> EX (Enter)
[Disconnected]
```

❑ HE command

You can show a command list in this session. Type HE at the prompt, and press **Enter**. Displayed commands depend on the privilege assigned to a role. The following figure is an example, which might differ from the actual screen.

```
5713RF0 NNNNN(0)IOEU> HE (Enter)

<<HE - Help.>>

BSM  - SC/SBM setting.
CER  - Public key.
CI   - Chassis ID.
DC   - Restore factory setting.
DEL  - Delete copy of log.
DF   - Show field replaceable unit information.
DH   - Show riser board and PCI Express adapter information.
DL   - Log.
EX   - Exit.
FAN  - FAN module.
FW   - Update I/O module firmware.
HE   - Help.
ILC  - Internal LAN setting.
IOC  - I/O module control.
LC   - LAN configuration.
LDAP - Directory service setting.
LFT  - Link Fault Tolerance setting.
LM   - Language Mode.
LS   - LAN controller discriminating information.
MI   - E-mail notification.
MLC  - Maintenance LAN setting.
PES  - PCI Express expander.
PS   - Show power and other sensors.
PSM  - Power supply module.
SCO  - Setting console.
SD   - Edit local time, time zone and NTP.
SDN  - System shutdown.
SEC  - Service setting.
SNM  - SMNP setting.
SO   - Security setting.
UBR  - Backup and restore setting.
WHO  - Show who is logged on.
WWN  - World wide name.
XD   - Execute diagnostics.

5713RF0 NNNNN(0)IOEU>
```

❑ SCO command

You can show and set the inactivity timer and serial connection. Type `SCO` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SCO (Enter)

<<SCO -Setting console.>>

-- Current session setting --
Inactivity timer (min): 10

-- Serial console setting --
Baud rate (bps)        : 9600

-- Console setting menu --
   I. Set inactivity timer.
   B. Set baud rate.
   Q. Quit.
(I, B, [Q]):
```

Select a menu item from the following list to execute it.

Menu		Description
I.	Set inactivity timer	Sets the inactivity timeout period.
B.	Set baud rate.	Sets the baud rate of a serial port.
Q.	Quit	Quits the SCO command.

The current setting, the session information that you currently log in, is shown in the following list.

Item	Description of item	Value	Description of value
Inactivity timer	Monitoring timer for inactivity	0 to 1440	Integers from 0 to 1440 can be specified. Unit: minute Setting “0” cancels the timer, and timeout for inactivity is not executed.

The serial console setting is shown in the following list.

Item	Description of item	Value	Description of value
Baud rate	The baud rate of the serial console for the I/O module	9600	Can select a baud rate among the three: 9600 bps, 38400 bps, and 115200 bps.
		38400	
		115200	

❑ WHO command

The following figure shows information about a user who is currently logged in. Type WHO at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> WHO (Enter)

<<WHO - Show who is logged on.>>

No. Name            Role  Login              Access    IP address
-- ---------------- ----- ---------------- -------- ----------
0   administrator   0     2009-03-02 10:37:30 SSH   192.168.0.200
1   MailServerAdmin 1     2009-03-02 10:20:12 SSH   192.168.0.210

-- Session menu --
D. Disconnect user.
Q. Quit.
(D,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
D.	Disconnect User.	Disconnects a user who currently logs in.
Q.	Quit	Quits the WHO command.

The information about the user currently logged in is shown in the following list.

Item	Description of item	Value	Description of value
No.	Serial number of sessions during the user login	integer	Serial number of sessions: from 0 to 6
Name	Account name	Character string in ASCII	Comprised of up to 32 characters.
		MAINTENANCE	Maintenance personnel
Role	Role ID	Integer	Role ID: from 0 to 23
		MNT	Maintenance personnel
		GST	Guest
Login	Login time	YYYY-MM-DD hh:mm:ss	YYYY: A. D.; MM: month; DD: day; hh: hour; mm: minute; ss: second
Access	Type of connection	Serial	Serial connection
		Telnet	Telnet connection
		SSH	SSH connection
IP address	A user IP address	Type of IP address	A user IP address has been connected via LAN
		----------	Connected from a serial port.

Chassis management

❑ CI command

You can display and set a chassis ID with this command. Type `CI` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> CI (Enter)

<<CI - Chassis ID.>>

Chassis ID : 5713RF0 NNNNN

-- Chassis ID menu --
   C. Edit chassis ID.
   Q. Quit.
(C,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Edit chassis ID.	Sets a chassis ID.
Q.	Quit	Quits the CI command.

The following table describes the displayed item.

Item	Description of item	Value	Description of value
Chassis ID	Chassis ID	Up to 20 characters in ASCII	Identifier for a chassis. The default value is the chassis serial number.

❑ SD command

You can display and set time. Type SD at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SD (Enter)

<<SD - Edit local time, time zone and NTP.>>

-- Local time --
Date : 2009-03-02
Time : 09:37:50

-- Time zone and Daylight Saving Time --
Time zone      : +09:00
DST            : Disable
DST start time : -------
DST end time   : -------

-- Time synchronization --
NTP : Disable

-- NTP server --
<NTP0>
Hostname : ------
Status   : Not connect
<NTP1>
Hostname : ------
Status   : Not connect
<NTP2>
Hostname : ------
Status   : Not connect
<NTP3>
Hostname : ------
Status   : Not connect

-- Time setting menu --
   L. Edit local time.
   Z. Edit time zone and Daylight Saving Time.
   S. Edit synchronization setting.
   N. Edit NTP server setting.
   R. Restart NTP service.
   Q. Quit.
(L,Z,S,N,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
L.	Edit local time.	Sets time of day.
Z.	Edit time zone and Daylight Saving Time.	Sets a time zone and Daylight Saving Time.
S.	Edit synchronization setting.	Sets automatic time adjustment.
N.	Edit NTP server setting	Sets Network Time Protocol (NTP) server.
R.	Restart NTP service.	Restarts NTP service.
Q.	Quit	Quits the SD command.

Local time information on the I/O module is described in the table below.

Item	Description of item	Value	Description of value
Date	Local date	YYYY-MM-DD	YYYY: AD year; MM: month; DD:day
Time	Local time	hh:mm:ss	hh: hour; mm:minute; ss: second

Time zone and DST information on the I/O module is described in the table below.

Item	Description of item	Value	Description of value
Time zone	-	from –2:00 to +14:00	Time difference from Coordinated Universal Time (UTC)
DST	Daylight Saving Time (DST)	Enable	The daylight saving time setting is enabled.
		Disable	The daylight saving time setting is disabled.
DST start time	When DST starts.	MMM ZZZZZ hh:mm	The time to start DST MMM: the first 3 characters of a month (ex. Apr, Oct) ZZZZZ: start date (hh: hour; mm: minute)
		-------	DST is disabled.
DST end time	When DST finishes.	MMM ZZZZZ hh:mm	The time to finish DST MMM: the first 3 characters of a month (ex. Apr; April; Oct: October) ZZZZZ: end date (hh: hour; mm: minute)
		-------	DST is disabled.

Details of DST are described in the following list.

Item	Description of value
Y	The day in the month.
lastXXX	The last day of a week in the month: XXX is 3 characters to show a day of a week. (For example: Sun, Mon, Tue, etc.)
XXX>=Y	The first XXX after the Y in the month: XXX is 3 characters to show a day of a week. (For example: Sun, Mon, Tue, etc.)
XXX<=Y	The last XXX before the Y in the month: XXX is 3 characters to show a day of a week. (For example: Sun, Mon, Tue, etc.)

Time synchronization information by NTP is described in the table below.

Item	Description of item	Value	Description of value
NTP	Time synchronization by NTP	Enable	The setting of time synchronization by NTP enabled.
		Disable	The setting of time synchronization by NTP disabled.

NTP server information is described in the table below.

Item	Description of item	Value	Description of value
No.	NTP server number	NTP0 to NTP3	Up to 4 NTP servers can be registered.
Hostname	NTP server address	Domain name	FQDN for NTP servers: displays up to 127 characters as ASCII code.
		IP address	IP address for NTP servers
		-------	No NTP server is set.
Status	Connection status to NTP server	Not connect	Connection is unavailable.
		Connect	Connection is available but the NTP server is not synchronized: a server with higher priority exists.
		Sync	Connection is available and the NTP server is synchronized.
		Unknown	Connection status is unknown.
		-------	No NTP server is set.



With the following conditions, time synchronization is not available:

- NTP server address is specified as the domain name.
- The I/O module with time synchronization by NTP enabled cannot be connected to the domain name system (DNS) server.

❑ SDN command

You can shutdown the system. Type `SDN` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SDN (Enter)

<< SDN - System shutdown. >>

-- Shutdown menu --
  S. Shutdown system.
  Q. Quit.
(S,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
S.	Shutdown system.	Shuts down the I/O slot expansion unit.
Q.	Quit	Quits the SDN command.

❑ PES command

Status of the peripheral components interconnect (PCI) express expander such as power operation, setting, and cables is displayed. Type `PES` at the prompt, and press

```
5713RF0 NNNNN(0)IOEU> PES(Enter)

<< PES - PCI Express expander. >>

-- PCI Express expander status --
# Power Condition
- ----- ---------
0 On    Normal
1 ---   -------

-- PCI Express expander setting --
# Current Config
- ------- ------
0 1:8     1:8
1  -----  1:8

-- PCI Express expander menu --
  D. Show detail cable information.
  Q. Quit.
(D,[Q]) :
```

Enter.

Select a menu item from the following list to execute it.

Menu		Description
D.	Show detail cable information.	Displays cable status.
Q.	Quit	Quits the PES command.

Status of PCI Express expander is described in the table below.

Item	Description of item	Value	Description of value
#	I/O module slot number with a PCI express expander installed	0.1	-
Power	Power status	-------	PCI express expander: Not installed in the I/O module.
		On	Power is On.
		Off	Power is Off.
Condition	Failure status	-------	PCI express expander: Not installed in the I/O module.
		Normal	Normal condition
		Fail	Failed status

PCI Express expander setting is described in the table below.

Item	Description of item	Value	Description of value
#	I/O module slot number with a PCI express expander installed	0.1	-
Current	The currently applied VS configuration	-------	PCI express expander: the power is Off or Not installed in the I/O module.
		1:8	1:8 mode
		1:4	1:4 mode
Config	VS configuration that can be applied when the PCI express expander is On.	1:8	1:8 mode
		1:4	1:4 mode

To display the cable status, type `D` at the prompt, and press `Enter`. The display may be different depending on your configuration.

```
- Control signal cable status --
-- I/O module0 --
# Presence      Server status
- ------------- -------------
0 Connected     On
1 Connected     On

-- I/O module1 --
# Presence      Server status
- ------------- -------------
0 Not connected  -----------
1 Not connected  -----------

-- I/O slot expansion unit connect cable status --
-- I/O module0 --
#   Presence      Link status Type
--- ------------- ----------- -------
0-0 Connected     Up          Metal
0-1 Connected     Up          Metal
1-0 Connected     Up          Metal
1-1 Connected     Up          Metal

-- I/O module1 --
#   Presence      Link status Type
--- ------------- ----------- -------
0-0 Not connected  ---------   -----
0-1 Not connected  ---------   -----
1-0 Not connected  ---------   -----
1-1 Not connected  ---------   -----

-- Control signal setting --
# Control signal
- --------------
0 Enable
1 Enable

-- Cable menu --
    Q. Quit.
```

```
([Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
Q.	Quit	Returns to the previous menu.

Control signal cable status is described in the table below.

Item	Description of item	Value	Description of value
#	Number of slots used for cable connection	0.1	0: control port0 1: control port1
Presence	Connection status	-------	I/O module: Not installed
		Connected	Currently connected.
		Not connected	Currently not connected.
Server status	Server power status	-------	Control signal cable: not connected.
		On	Power is on.
		Off	Power is off.

I/O slot expansion unit connect cable status is described in the table below.

Item	Description of item	Value	Description of value
#	Number of slots used for cable connection	0-0, 0-1, 1-0, 1-1	Ports for connection to server chassis 0-0: Port0 (upper port) 0-1: Port0 (lower port) 1-0: Port1 (upper port) 1-1: Port1 (lower port)
Presence	Connection status	-------	I/O module: Not installed
		Connected	Currently connected.
		Not connected	Currently not connected.
Link status	-	-------	I/O slot expansion unit cable: not connected.
		Up	Linkup
		Down	Linkdown
Type	Cable type	-------	I/O slot expansion unit cable: not connected.
		Metal	Metal cable for I/O slot expansion connection
		Optical	Optical cable for I/O slot expansion connection

Control signal setting status is described in the table below.

Item	Description of item	Value	Description of value
#	I/O module slot number with a PCI express expander installed	0.1	-
Control signal	Synchronization setting	Disable	The setting is Off.
		Enable	The setting is On.

❑ PS command

Status of all modules is displayed. Type `PS` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> PS (Enter)

<< PS - Show power and other sensors. >>

-- Sensor menu --
   C. Show information of server chassis.
   I. Show sensors of I/O module.
   PS. Show sensors of power supply module.
   F. Show sensors of fan module.
Q. Quit.
(C,I,PS,F,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Show information of I/O slot expansion unit chassis.	Displays the chassis information.
I.	Show sensors of I/O module.	Displays sensors of the I/O module.
PS.	Show sensors of power supply module.	Displays sensors of the power supply module.
F.	Show sensors of fan module.	Displays sensors of the fan module.
Q.	Quit	Quits the PS command.

If you type `C` in the PS command menu and press `Enter`, the chassis information is displayed. The screen display may be different depending on your configuration.

```
-- Current data of I/O slot expansion unit chassis --
Name                  : GV0EDW11-224N11N
Nameplate Power       : 176(W)
Present AC Power      : 93(W)
Present DC Power      : 32(W)
Average AC Power      : 99(W)
Maximum AC Power      : 105(W)
Minimum AC Power      : 81(W)
Average DC Power      : 32(W)
Maximum DC Power      : 32(W)
Minimum DC Power      : 32(W)
Airflow Volume        : 14.00(m3/min)
```

If you type [I] in the PS command menu and press **Enter**, the I/O module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of I/O module0 --
-- Temperature --
Intake                : 32.00(degrees C)
Exaust                : 31.00(degrees C)
Riser                 : 31.00(degrees C)

-- Voltage --
hotswap sub           : 5.01(V)
hotswap main          : 11.94(V)
sub 3.3V              : 3.27(V)
sub 1.8V              : 1.78(V)
sub 1.2V              : 1.19(V)
main 12V              : 11.91(V)
main 3.3V             : 0.00(V)
main 1.2V             : 0.00(V)
main 1.0V             : 0.00(V)
riser sub 3.3V        : 3.27(V)
riser main 3.3V01     : 0.00(V)
riser main 3.3V02     : 3.34(V)
riser main 3.3V03     : 3.34(V)
riser main 12V        : 11.99(V)

-- Current --
hotswap sub           : 1.03(A)
hotswap main          : 0.22(A)

-- Current data of I/O module0 --
Name                  : GV-BE2MNG1N1
Slot                  : 0
Nameplate Power       : 250(W)
Present Sub Power     : 5(W)
Present Main Power    : 2(W)
Average Sub Power     : 4(W)
Maximum Sub Power     : 5(W)
Minimum Sub Power     : 4(W)
Average Main Power    : 1(W)
Maximum Main Power    : 3(W)
Minimum Main Power    : 1(W)
```

If you type PS in the PS command menu and press **Enter**, the power supply module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Power supply module1 --
Main 12V             : 1.50(A)
Input                : 0.50(A)

-- Current data of Power supply module1 --
Name                 :
Slot                 : 1
Total Power          : 1000(W)
AC Input Power       : 50(W)
DC Output Power      : 16(W)
```

If you type F in the PS command menu and press **Enter**, the fan module information is displayed. The screen display may be different depending on your configuration.

```
-- Sensors of Fan module0 --
FAN0                 : 1929(rpm)
FAN1                 : 1917(rpm)

-- Current data of Fan module0 --
Slot                 : 0
Nameplate Power      : 38(W)
```

❑ DF command

Information on internal modules is displayed. Type DF at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> DF (Enter)

<< DF - Show field replaceable unit information. >>

-- Detail field replaceable unit information menu --
    C. I/O slot expansion unit chassis.
    M. I/O module main board.
    R. I/O module riser board.
   PS. Power supply module.
    T. Show mass of modules.
    A. All module.
    Q. Quit.
(C,M,R,PS,T,A,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	I/O slot expansion unit chassis	Displays chassis information.
M.	I/O module main board	Displays I/O module main board information.
R.	I/O module riser board	Displays I/O module riser board information.
PS.	Power supply module	Displays power supply module main board information.
T.	Show mass of modules	Displays information on module mass.
A.	All module	Displays information on all modules.
Q.	Quit	Quits the DF command.

If you type C in the DF command menu and press **Enter**, the chassis information is displayed. The screen display may be different depending on your configuration.

```
--- I/O slot expansion unit chassis ---
Part/Model Number : GV0EDW11-224N11N
Serial Number     : 5713RF0 00108
Midplane ID       : 00
Chassis ID        : BS2000-7
```

If you type M in the DF command menu and press **Enter**, the I/O module main board information is displayed. The screen display may be different depending on your configuration.

```
--- I/O module main board ---
Slot          : 0

-- Board information --
Manufacturer  : HITACHI
Product Name  : HBS23-YA
Serial Number : 851590

-- Product information --
Manufacturer          : HITACHI
Product Name          : I/O Module
Part/Model Number     : GV0EDW11-224N11N
Serial Number         : 851590

-- MultiRecord information --
Manufacturer ID       : 000074
Module Type1          : 40
Module Type2          : 00
Model ID              : Compute Blade 2000 I/O Slot expansion unit (00)
```

If you type R in the DF command menu and press **Enter**, the I/O module riser board information is displayed. The screen display may be different depending on your configuration.

```
--- I/O module riser board ---
Slot          : 0

-- Board information --
Manufacturer  : HITACHI
Product Name  : HBS24-YB
Serial Number : 987654
```

If you type PS in the DF command menu and press **Enter**, the power supply module information is displayed. The screen display may be different depending on your configuration.

```
-- Power supply module -
Slot          : 1

-- Product information -
Manufacturer          : DELTA
Product Name          : DPS-1000FB B
Part/Model Number     :
Product Version       : S0F
Serial Number         : CKYD0919S00024
```

If you type T in the DF command menu and press **Enter**, the mass information is displayed. The screen display may be different depending on your configuration.

```
-- I/O slot expansion unit chassis -
Total : 40.96(kg)
```

If you type A in the DF command menu and press **Enter**, information on each module and mass is displayed. The screen display may be different depending on your configuration.

```
--- I/O slot expansion unit chassis ---
Part/Model Number : GV0EDW11-224N11N
Serial Number     : 5713RF0 00108
Midplane ID       : 00
Chassis ID        : BS2000-7

(omitted in the middle.)

-- I/O slot expansion unit chassis -
Total : 40.96(kg)
```

❑ DH command

Status of riser boards and I/O adapter modules is displayed. Type DH at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> DH (Enter)

<< DH - Show riser board and PCI Express adapter information. >>

-- Riser board status -
# Presence      Power Condition
- ------------- ----- ---------
0 Installed     On     Normal
1  -----------   ---   -------

-- PCI Express adapter status -
# P  Presence      Power Condition Type
- -- ------------- ----- --------- ----------------------------------------
0  0 Installed     On    Normal     1000BASE-T 2-port LAN adapter
0  1 Installed     On    FAIL       1000BASE-T 2-port LAN adapter
0  2 Installed     On    Normal     1000BASE-T 2-port LAN adapter
0  3 Not Installed  ---   -------   ----------------------------------------
0  4 Installed     Off    -------   Unknown
0  5 Not Installed  ---   -------   ----------------------------------------
0  6 Installed     On    Normal     Hitachi 8Gb 2-port fibre channel adapter
0  7 Installed     On    Normal     Unknown
1  8  -----------   ---   -------   ----------------------------------------
1  9  -----------   ---   -------   ----------------------------------------
1 10  -----------   ---   -------   ----------------------------------------
1 11  -----------   ---   -------   ----------------------------------------
1 12  -----------   ---   -------   ----------------------------------------
1 13  -----------   ---   -------   ----------------------------------------
1 14  -----------   ---   -------   ----------------------------------------
1 15  -----------   ---   -------   ----------------------------------------

-- Riser board and PCI Express adapter menu -
    Q. Quit.
([Q]) :
```

Select a menu item from the table below to execute it.

Menu		Description
Q.	Quit	Quits the DH command.

Riser board status is described in the table below.

Item	Description of item	Value	Description of value
#	Slot number of the I/O module with a riser board installed.	0, 1	-
Presence	Status of the riser board	-------	I/O module: Not installed.
		Installed	-
		Not installed	-

Item	Description of item	Value	Description of value
Power	Power status	-------	Riser board: Not installed.
		On	Power is on.
		Off	Power is off.
Condition	Failure status	-------	No riser board is installed, or power is off.
		Normal	-
		Fail	-

PCI express adapter status is described in the table below: correspondence between I/O adapter status and riser boards.

Item	Description of item	Value	Description of value
#	Slot number of the I/O module with a riser board installed.	0, 1	-
P	Slot number of the I/O board	0 to 15	-
Presence	Status of the I/O board	-------	I/O module: Not installed.
		Installed	-
		Not installed	-
Power	Power status	-------	Riser board: Not installed.
		On	Power is on.
		Off	Power is off.
Condition	Failure status	-------	No riser board is installed, or power is off.
		Normal	-
		Fail	-
Type	Type of I/O adapters	-------	No I/O adapter is installed, or power is off.
		Unknown	-
		1000BASE-T 2-port LAN adapter	-
		1000BASE-T 4-port LAN adapter	
		10 GB 1-port LAN adapter	
		Hitachi 8 Gb 1-port Fibre-channel adapter	

Item	Description of item	Value	Description of value
Type	Type of I/O adapters	Hitachi 8 Gb 2-port Fibre-channel adapter	
		Emulex 8 Gb 2-port Fibre-channel adapter	
		Hitachi 16Gb 1-port fibre channel adapter	
		Hitachi 16Gb 2-port fibre channel adapter	
		Emulex 16Gb 2-port fibre channel adapter	
		3 Gb 1-port SAS adapter	
		10 Gb 2-port LAN adapter	
		I/O adapter name	A name of the displayed I/O adapter may be different from a name of the installed I/O adapter.

❑ WWN command

You can display World Wide Name (WWN). Type `WWN` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> WWN (Enter)

<< WWN - World wide name. >>

-- World wide name menu --
    A. Show additional WWN.
    O. Show original WWN.
    Q. Quit.
(A, 0, [Q]):
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Show additional WWN	Displays information on Optional Physical WWN.
O.	Show original WWN	Displays information on the Default Physical WWN.
Q.	Quit	Quits the WWN command.

If you type `A` in the WWN command menu and press `Enter`, Optional Physical WWNs are displayed.

```
-- Optional Physical WWN --
P  Port World wide port name     World wide node name
-- ---- ----------------------- -----------------------
 0    0  01:23:45:67:89:AB:CD:EF  01:23:45:67:89:AB:CD:F0
 0    1  01:23:45:67:89:AB:CD:F1  01:23:45:67:89:AB:CD:F2
 0    2  01:23:45:67:89:AB:CD:F3  01:23:45:67:89:AB:CD:F4
 0    3  01:23:45:67:89:AB:CD:F5  01:23:45:67:89:AB:CD:F6
 1    0  01:23:45:67:89:AB:CD:F7  01:23:45:67:89:AB:CD:F8
 1    1  01:23:45:67:89:AB:CD:F9  01:23:45:67:89:AB:CD:FA
 1    2  01:23:45:67:89:AB:CD:FB  01:23:45:67:89:AB:CD:FC
 1    3  01:23:45:67:89:AB:CD:FD  01:23:45:67:89:AB:CD:FE
(Omitted in the middle.)
14    0  01:23:45:67:89:AB:CE:5F  01:23:45:67:89:AB:CE:60
14    1  01:23:45:67:89:AB:CE:61  01:23:45:67:89:AB:CE:62
14    2  01:23:45:67:89:AB:CE:63  01:23:45:67:89:AB:CE:64
14    3  01:23:45:67:89:AB:CE:65  01:23:45:67:89:AB:CE:66
15    0  01:23:45:67:89:AB:CE:67  01:23:45:67:89:AB:CE:68
15    1  01:23:45:67:89:AB:CE:69  01:23:45:67:89:AB:CE:6A
15    2  01:23:45:67:89:AB:CE:6B  01:23:45:67:89:AB:CE:6C
15    3  01:23:45:67:89:AB:CE:6D  01:23:45:67:89:AB:CE:6E
```

Information on the Optional Physical WWN is described in the table below.

Item	Description of item	Value	Description of value
P	I/O adapter slot number	0 to 15	-
Port	Port number	0 to 3	-

Item	Description of item	Value	Description of value
World wide port name	WWPN	XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN (WWPN): default value
World wide node name	WWNN	XX:XX:XX:XX:XX:XX:XX:XX	Optional Physical WWN (WWNN): default value

If you type o in the WWN command menu and press **Enter**, Default Physical WWNs are displayed.

```
-- Original WWN --
P  Port World wide port name     World wide node name
-- ---- ------------------------ ------------------------
 0    0  01:23:45:67:89:AB:CD:EF  01:23:45:67:89:AB:CD:F0
 0    1  01:23:45:67:89:AB:CD:F1  01:23:45:67:89:AB:CD:F2
 0    2  ----------------------    ----------------------
 0    3  ----------------------    ----------------------
 1    0  01:23:45:67:89:AB:CD:F7  01:23:45:67:89:AB:CD:F8
 1    1  ----------------------    ----------------------
 1    2  ----------------------    ----------------------
 1    3  ----------------------    ----------------------
(Omitted in the middle)
14    0  ----------------------    ----------------------
14    1  ----------------------    ----------------------
14    2  ----------------------    ----------------------
14    3  ----------------------    ----------------------
15    0  ----------------------    ----------------------
15    1  ----------------------    ----------------------
15    2  ----------------------    ----------------------
15    3  ----------------------    ----------------------
```

Information on the Default Physical WWN is described in the table below.

Item	Description of item	Value	Description of value
P	I/O adapter slot number	0 to 15	-
Port	Port number	0 to 3	-
World wide port name	WWPN	-------	Not installed; No applicable port; I/O adapter without WWN installed; Not collected information on the I/O adapter.
		XX:XX:XX:XX:XX:XX:XX:XX	Default Physical WWN (WWPN)
		*XX:XX:XX:XX:XX:XX:XX:XX	Displayed Default Physical WWN (WWPN) may be different from Default Physical WWN (WWPN) of the I/O adapter.

Item	Description of item	Value	Description of value
World wide node name	WWNN	-------	Not installed; No applicable port; I/O adapter without WWN installed; Not collected information on the I/O adapter.
		XX:XX:XX:XX:XX:XX:XX:XX	Default Physical WWN (WWNN)
		*XX:XX:XX:XX:XX:XX:XX:XX	Displayed Default Physical WWN (WWPN) may be different from Default Physical WWN (WWPN) of the I/O adapter.

❑ PSM command

You can set a power supply module and display the status. Type `PSM` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> PSM (Enter)

<< PSM - Power supply module. >>

-- Power supply module status --
PS Power                Condition AC input
-- -------------------- --------- --------
 0 On                   Normal    Normal
 1 On                   Normal    Normal

-- AC input voltage setting --
Voltage      : 200

-- Power supply module menu --
    Q. Quit.
([Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
Q.	Quit	Quits the PSM command.

Items of the power supply module status are described in the table below.

Item	Description of item	Value	Description of value
PS	Power supply slot number	0 to 1	-
Power	Power status	-------	No power supply module is installed.
		On	The power is on.
		Off	The power is off.

Condition	Status: failure status	-------	No power supply module is installed.
		Normal	No problem
		FAIL	The power supply fails.
AC input	AC input status	-------	No power supply module is installed.
		Normal	AC input exists.
		None	No AC input.

AC input voltage setting is described in the table below.

Item	Description of item	Value	Description of value
Voltage	AC input voltage setting of the power supply	100	AC input voltage: 100 V (Not supported)
		200	AC input voltage: 200 V
		Unknown	The setting value is unknown.

❑ IOC command

You can display I/O module status and operate the module. Type `IOC` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> IOC (Enter)

<< IOC - I/O module control. >>

-- I/O module status --
# Behavior Power Condition     LID lamp
- -------- ----- ------------- --------
0 Active   On    Normal        Off
1 Standby  On    Normal        Off

-- I/O module control menu --
    P. Power control.
    L. LID lamp control.
    Q. Quit.
(P,L,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
P.	Power control.	Executes the power operation of the I/O module.
L.	LID lamp control	Executes the identification light-emitting diode (LED) of the I/O module.
Q.	Quit	Quits the IOC command.

Items of I/O module status are described in the table below.

Item	Description of item	Value	Description of value

Item	Description of item	Value	Description of value
#	I/O module slot number	0 or 1	-
Behavior	I/O module performance	-------	No I/O module is installed. "Active" undecided Boot is disabled.
		Active	Unit management master
		Standby	Not unit management master
Power	Power supply status	-------	No I/O module is installed.
		On	The I/O module is powered on.
		Off	The I/O module is powered off.
Condition	Status: Whether or not available for the user operation; FAIL status	-------	No I/O module is installed.
		Normal	-
		Booting	Booting now
		Shutting down	Shutting down now
		Boot disable	Boot is disabled.
		FAIL	The module fails.
LID Lamp	Status of the identification LED	-------	No I/O module installed; Boot is disabled; Boot of the other module is disabled; In failure; the other module in failure.
		On	LED lights solid.
		Off	LED is off.

Type `P` in the IOC command menu and press **Enter.** The Power control menu is displayed.

```
(P,L,[Q]) : P (Enter)
-- I/O module status --
# Behavior Power Condition     LID lamp
- -------- ----- ------------- --------
0  ------   ---   -----------   ------
1 Active   On    Normal        Off

-- Power control menu --
    S. Shutdown.
    R. Restart.
   SW. Switch active/standby.
    Q. Quit.
(S,R,SW,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
S.	Shutdown	Shuts down the I/O module.
R.	Restart	Restarts the I/O module.
SW.	Switch active/standby	Switches the unit management masters of the I/O module.
Q.	Quit	Returns to the previous menu.

If you type `L` in the IOC command menu and press **Enter**, the identification LED menu is displayed.

```
(P,L,[Q]) : L (Enter)
-- I/O module status --
# Behavior Power Condition     LID lamp
- -------- ----- ------------- --------
0  ------   ---   -----------   ------
1 Active   On    Normal        Off

-- LID lamp control menu --
    T. Turn on
    F. Turn off
    Q. Quit.
(T,F,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
T.	Turn on	Turns on the identification LED of the I/O module.
F.	Turn off	Turns off the identification LED of the I/O module.
Q.	Quit	Returns to the previous menu.

❑ FAN command

You can display the fan module status. Type `FAN` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> FAN (Enter)

<< FAN - FAN module. >>


-- FAN module status --
F Power                Condition Unit1(rpm) Unit2(rpm)
- -------------------- --------- ---------- ----------
0 On                   Normal          3000       3000
1 On                   Normal          3000       3000
2 On                   Normal          3000       3000
3 On                   Normal          3000       3000

-- FAN module menu --
    Q. Quit.
([Q]) :
```

Select a menu item from the following table to execute it.

Menu		Description
Q.	Quit	Quits the FAN command.

Items of the fan module status are described in the table below.

Item	Description of item	Value	Description of value
F	Fan module slot number	0 to 3	-
Power	Power supply status	-------	No fan module is installed.
		On	Power is supplied to the fan module.
		Processing power off	Power is being turned down.
		Off	No power is supplied to the fan module.
		Processing power on	Power is being supplied to the fan module.
Condition	Status: FAIL status	-------	No fan module is installed.
		Normal	-
		FAIL	The module fails.
Unit1 (rpm)	Fan 1	-------	No fan module is installed.
		Integer	Revolution per minute of Fan 1 (Unit: rpm)
Unit2 (rpm)	Fan 2	-------	No fan module is installed.
		Integer	Revolution per minute of Fan 2 (Unit: rpm)

❑ DL command

You can display logs. Type DL at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> DL (Enter)

<< DL - Log. >>

-- Log menu --
    S. Show alert log.
    E. Show system event log.
    D. Dump log to file.
    P. Show power monitoring log.
    M. Show environment monitoring log.
    A. Show console access log.
    F. Create error log file.
    I. Show MARLOG.
    C. Show RC list.
    Q. Quit.
(S,E,D,P,M,A,F,I,C,[Q]) :
```

Select a menu item from the following table to execute it.

Menu		Description
S.	Show alert log.	Views alert logs.
E.	Show system event log.	Views system event logs.
D.	Dump log to file.	Creates a log file for a probe to the current system equipment, and saves the file to the user directory in the I/O module. The file can be downloaded via FTP or SFTP.
P.	Show power monitoring log.	Views power monitoring logs.
M.	Show environment monitoring log.	Views environment monitoring logs.
A.	Show console access log.	Views console access logs.
F.	Create error log file.	Views and creates error logs.
I.	Show MARLOG.	Views MAR logs.
C.	Show RC list.	Views the RC list.
Q.	Quit	Quits the DL command.

If you type S in the DL command menu and press **Enter**, alert logs are displayed.

```
-- SVP log --
Timestamp           ID   Level   Message
------------------- ---- ------- ------------------------------------
--------
2009-12-25 04:10:12 1890 Info     Module <Power Supply module 0> was
installed.
(SEL=000002243B344B61000408506FA00000,SID=,PAR=XX,MTY=05,SLT=00)
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:12 1890 Info     Module <Power Supply module 1> was
installed.
(SEL=000002243B344B61000408506FA00001,SID=,PAR=XX,MTY=05,SLT=01)
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:12 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:15 18E4 Info     Module information update alert is
sent.
2009-12-25 04:10:15 18E4 Info     Module information update alert is
sent.

Hit enter key.
```

Items of the alert log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (Local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
ID	Log ID (Alert ID)	NNNN	Alert message ID: a character string in hex (4 characters)
Level		Info	Information
		WARNING	-
		FAIL	-
Message	Event message	Character string	Displayed in ASCII.

If you type E in the DL command menu and press **Enter**, system event logs are displayed.

```
-- System event log --
Timestamp                          Module  Level       System  event  log
Message
------------------- ------ ------- ----------------------------
2009-12-25 04:10:12 PS0    Info    001D 02 6100 04 0850 6FA00000 Power
Supply module#z: installed
2009-12-25 04:10:12 PS1    Info    001E 02 6100 04 0850 6FA00001 Power
Supply module#z: installed
2009-12-25 04:10:12 PS0    Info    001F 02 6100 04 F2F8 07A82000 Power
Supply module#z: Power On
2009-12-25 04:10:12 PS1    Info    0020 02 6100 04 F2F9 07A82001 Power
Supply module#z: Power On
2009-12-25 04:10:16 IO0     Info     0021 02 6100 04 F2F8 07A80A60 I/O
module#z: Control signal cable installed
2009-12-25 04:10:16 IO0     Info     0022 02 6100 04 F2F8 07A80A61 I/O
module#z: Control signal cable installed

Hit enter key.
```

Items of the system event log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Module	Where the event occurs	IOX	I/O module
		IOAX	I/O adapter
		PSX	Power supply module
		FANX	Fan module
		ETC	Others including “Unknown”
Level		Info	Information
		Caution	-
		WARNING	-
		FAIL	-
System event log	Event data	IIII RR gggg ee ssSS ee11223344	IIII: Record ID RR: Record type gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3
Message	Event message	Character string	Displayed in ASCII.

If you type D in the DL command menu and press **Enter**, a message appears to confirm the data collection. At the prompt, type Y and press **Enter**, and the log file data for a probe is created. To cancel creating the data file for a probe, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
WARNING : If confirm, it will take few minutes to dump log to file.

Confirm? (Y,[N]) : Y (Enter)

--- Dumping log to file progress ---
I/O module0 process:Collecting Log is completed.
0% ------ 20% ----- 40% ----- 60% ----- 80% ---- 100%
|.................................................| [100]%
- Dumping log to file was completed.
- File name is "io-20090303-184046.dmp".
Hit enter key.
```

It takes a few minutes to create a log data file for a probe. When it is completed, the file name is displayed. At the prompt, press **Enter**, and the screen returns to the DL command menu.

If you type P in the DL command menu and press **Enter**, power monitoring logs are displayed. The I/O module and chassis display different items in the screen.

- I/O module

```
Select target (0-1,C=chassis,A=All,[Q=Quit]) : 0 (Enter)
Select trend data(0=last 24 hours,1=yesterday,[Q=Quit]) : 0 (Enter)

-- I/O module0 power monitoring log --
                    Main Power consumption[W]    Sub Power consumption[W]
Timestamp           Ave     Max     Min          Ave     Max     Min
------------------- ------- ------- -------      ------- ------- -------
YYYY-MM-DD hh:mm:ss    7600    7800    7500         7600    7800    7500
(Omitted in the middle)
YYYY-MM-DD hh:mm:ss    7600    7800    7500         7600    7800    7500

Hit enter key.
```

Items of the I/O module power consumption monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Ave	Average power consumption value	Integer	Average power consumption value by the I/O module. (Unit: watt)
Max	Maximum power consumption value	Integer	Maximum power consumption value by the I/O module. (Unit: watt)

Item	Description of item	Value	Description of value
Min	Minimum power consumption value	Integer	Minimum power consumption value by the I/O module. (Unit: watt)

■ Chassis

```
Select target (0-1,C=chassis,A=All,[Q=Quit]) : C (Enter)
Select trend data(0=last 24 hours,1=yesterday,[Q=Quit]) : 0 (Enter)

-- Chassis power monitoring log --
                    AC Power consumption[W]      DC Power consumption[W]
Timestamp           Ave     Max     Min          Ave     Max     Min
------------------- ------- ------- -------      ------- ------- -------
YYYY-MM-DD hh:mm:ss    7600    7800    7500         7600    7800    7500
(Omitted in the middle)
YYYY-MM-DD hh:mm:ss    7600    7800    7500         7600    7800    7500

Hit enter key.
```

Items of the chassis power monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Timestamp	When a log is created. (local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Ave	Average power consumption value	Integer	Average power consumption value by the chassis. (Unit: watt)
Max	Maximum power consumption value	Integer	Maximum power consumption value by the chassis. Unit: watt)
Min	Minimum power consumption value	Integer	Minimum power consumption value by the chassis. (Unit: watt)

If you type M in the DL command menu and press **Enter**, the environment log menu is displayed. Type S and press **Enter**, and the environment monitoring logs of the I/O module are displayed.

```
-- Environment monitoring log menu --
    S. Show log in recent days.
    Q. Quit.
(S,[Q]) : S (Enter)
Select I/O module (0-1,[Q=Quit]) : 0 (Enter)
Select I/O module parts (M=Main board,R=Riser board,[Q=Quit]) : M (Enter)

-- I/O module0 (Main board) environment monitoring log --

   Date   |                      intake temperature[C]                      |
          |-----------------------------------------------------------------|
          | avg | min | max |  00  01  02  03  04  05  06  07  08  09  10  11|
          |     |     |     |  12  13  14  15  16  17  18  19  20  21  22  23|
----------+-----+-----+-----+-----------------------------------------------|
```

```
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  --  --  --  --  --|
          |     |     |     |  --  --  --  --  --  --  --  --  --  --  --  --|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|

   Date   |                     exhaust temprature[C]                         |
          |---------------------------------------------------------------|
          | avg | min | max |  00  01  02  03  04  05  06  07  08  09  10  11|
          |     |     |     |  12  13  14  15  16  17  18  19  20  21  22  23|
----------+-----+-----+-----+-----------------------------------------------|
          |---------------------------------------------------------------|
          | avg | min | max |  00  01  02  03  04  05  06  07  08  09  10  11|
          |     |     |     |  12  13  14  15  16  17  18  19  20  21  22  23|
----------+-----+-----+-----+-----------------------------------------------|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  --  --  --  --  --|
          |     |     |     |  --  --  --  --  --  --  --  --  --  --  --  --|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
 YY-MM-DD |  aa |  bb |  cc |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|
          |     |     |     |  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX  XX|

Hit enter key.
```

Items of the I/O module environment monitoring log are described in the table below.

Item	Description of item	Value	Description of value
Date		YY-MM-DD	YY: Last 2 digits of AD year; MM: month; DD: day
		-------	Date is invalid.
avg	Average value of the temperature sensor in a specific day	Integer	Average value of the temperature sensor. (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day

Item	Description of item	Value	Description of value
min	Minimum value of the temperature sensor in a specific day	Integer	The minimum value of the temperature sensor (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day.
max	Maximum value of the temperature sensor in a specific day	Integer	The maximum value of the temperature sensor (Unit: °C)
		--	Values of the temperature sensor are all invalid in a specific day.
00-23	Temperature sensor value by the hour	Integer	Average value of the temperature sensor by the hour (Unit: °C)
		--	Temperature sensor values are invalid.

Note: When R-Riser board is selected, “Riser board” is displayed in the title instead of (Main board). “exhaust” for Riser board is always displayed as “=No logs” due to no temperature sensor.

If you type A in the DL command menu and press **Enter**, the access log menu is displayed.

```
-- Console access log menu --
    C. Create log file.
    A. Show all log.
    P. Show log for a period of time.
    Q. Quit.
(C,A,P,[Q]) :
```

Menu		Description
C.	Create log file	Outputs access logs as a CSV file to the user directory in the I/O module. You can download the file via FTP or SFTP.
A.	Show all log	Displays access logs.
P.	Show log for a period of time	Displays access logs for a specific period.
Q.	Quit	Returns to the previous menu.

If you type C in the access log menu and press **Enter**, the access log file is created.

```
Confirm? (Y,[N]) : Y (Enter)
- Creating console access log file was completed.
- File name is “acs-20090303-150957.csv”.
Hit enter key. (Enter)
```

If you type A in the access log menu and press **Enter**, the access log list is displayed.

```
(C,A,P,[Q]) : A (Enter)

Full period     : 2009-02-21 13:37:15 - 2009-03-09 04:47:27

-- Console access log --
No. Name                            Host            Login
--- ------------------------------- --------------- -------------------
  0 00003_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  1 00002_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  2 00001_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  3 00000_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  4 00019_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  5 00018_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  6 00017_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  7 00016_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  8 00015_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  9 00014_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 10 00013_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 11 00012_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 12 00011_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 13 00010_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 14 00009_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 15 00008_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38

(0-15,Q=Quit,[N=Next]) :
```

Items of the I/O module console access log are described in the table below.

Item	Description of item	Value	Description of value
No.	Log number	Integer	From 0 up to 15
Name	Account name	Character string in ASCII	Account name: consists of up to 32 characters.
		MAINTENANCE	Maintenance personnel
		SPECIALIST	Factory specialist
Host	Connection source IP address	IP address	Source IP address for the user connected via LAN
		--	Connected from a serial port.
Login	Login time	YYYY-MM-DD hh:mm:ss	Login date: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second

Select a log number from the access log list, and the access log details are displayed.

```
(0-15,Q=Quit,[N=Next]) : 1 (Enter)
-- Console access log detail --
Name     : 00002_ABCDEFGHIJKLMNOPQRSTUVWXY
Role     : 2
Host     : 192.168.  0.  1
Access   : SSH
Login    : 2009-02-21 13:47:59
Logout   : 2009-02-21 13:47:59
Behavior : Active
Slot     : 0

Hit enter key.
```

Items of the I/O module access log details are described in the table below.

Item	Description of item	Value	Description of value
Name	Account name	Character string in ASCII	Account name: consists of up to 32 characters.
		MAINTENANCE	Maintenance personnel
		SPECIALIST	Factory specialist
Role		Integer	Role ID: from 0 up to 23
		Maintenance	Maintenance personnel
		Specialist	Factory specialist
		Guest	-
Host	Connection source IP address	IP address	Source IP address for the user connected via LAN
		--	Connected from a serial port.
Access	Connection type	Serial	Connected via serial.
		Telnet	Connected via Telnet.
		SSH	Connected via SSH.
Login	Login time	YYYY-MM-DD hh:mm:ss	Login date and time: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Logout	Logout time	YYYY-MM-DD hh:mm:ss	Logout date and time: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Behavior	I/O module type	Active	Unit management master
		Standby	Not unit management master
Slot	I/O module slot number	0 or 1	Slot number of the I/O module that you log in.

If you type P in the access log menu and press **Enter**, you can specify a time period for the access logs to display.

```
(C,A,P,[Q]) : P (Enter)

Full period     : 2009-02-21 13:37:15 - 2009-03-09 04:47:27

Start Date([Quit]) : 2009-02-21 (Enter)
Start Time([Quit]) : 00:00:00 (Enter)
Set current date and time as end of period? (Y,[N]) : N (Enter)
End Date([Quit])   : 2009-02-28 (Enter)
End Time([Quit])   : 00:00:00 (Enter)

Selected period : 2009-02-21 00:00:00 - 2009-02-28 00:00:00

-- Console access log --
No. Name                              Host            Login
--- ------------------------------- --------------- -------------------
  0 00003_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  1 00002_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  2 00001_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  3 00000_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:47:59
  4 00019_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  5 00018_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  6 00017_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  7 00016_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  8 00015_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
  9 00014_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 10 00013_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 11 00012_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 12 00011_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 13 00010_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 14 00009_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38
 15 00008_ABCDEFGHIJKLMNOPQRSTUVWXY 192.168.  0.  1 2009-02-21 13:45:38

(0-15,Q=Quit,[N=Next]) :
```

If you type F in the access log menu and press **Enter**, the error log list is displayed.

```
-- Error log notification history --
NO. Timestamp           System event log      Message
--- ------------------- ---------------------
  0 2009-12-25 05:43:09 6100 04 F2F8 07A10800 I/O module#z: Failure(I2C error)
  1 2009-12-25 05:43:13 6100 04 F2F8 07A10800 I/O module#z: Failure(I2C error)
  2 2009-12-25 05:43:14 6100 04 F2F8 07A10800 I/O module#z: Failure(I2C error)
  3 2009-12-25 05:43:15 6100 04 F2F8 07A10800 I/O module#z: Failure(I2C error)
  4 2009-12-25 05:43:15 6100 04 F2F8 07A10800 I/O module#z: Failure(I2C error)

Select No. (0-4,[Q=Quit]) :
```

Items of the error log notification history are described in the table below.

Item	Description of item	Value	Description of value
No.	E-mail notification history number	Integer	From 0 to 31: up to 32 records
Timestamp	When the event that triggered the notification happened	YYYY-MM-DD hh:mm:ss	Date and time when the event that triggered the e-mail notification happened: YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
System Event Log		IIII RR gggg ee ssSS ee11223344	IIII: Record ID RR: Record type gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3
Message	Event message	Character string	Message in ASCII

Specify an e-mail notification history number, and the log data file to probe the system in failure is created and saved in the user directory in the I/O module. You can download it via FTP or SFTP.

If you type [l] in the DL command menu and press **Enter**, the MAR log list is displayed.

```
-- MARLOG INDEX --
No. Timestamp           Assist Reason
--- ------------------- ------ ------------------------------------------------
  0 2009-03-09 10:13:39   OK   IOA detected failure
  1 2009-03-09 10:13:48   OK   no redundancy
  2 2009-03-09 10:13:29   OK   PCI Slot/IOA failure/Fault Status asserted
  3 2009-03-09 10:07:40   OK   IOA detected failure
  4 2009-03-09 10:07:34   OK   IOA detected failure
  5 2009-03-09 10:07:40   OK   PCI Slot/IOA failure/Fault Status asserted
  6 2009-03-09 09:38:54   OK   PCI Slot/IOA failure/Fault Status asserted
  7 2009-03-09 09:38:56   OK   PCI Slot/IOA failure/Fault Status asserted
  8 2009-03-09 09:38:50   OK   IOA detected failure
  9 2009-03-09 09:33:23   OK   PCI Slot/IOA failure/Fault Status asserted
 10 2009-03-09 09:28:52   NG   IOA detected failure
 11 2009-03-09 09:29:00   OK   PCI Slot/IOA failure/Fault Status asserted
 12 2009-03-09 06:25:29   OK   Power module failure
 13 2009-03-09 06:25:05   OK   Voltage abnormal

Select MARLOG (0-13,[Q=Quit]) :
```

Item	Description of item	Value	Description of value
No.	Log number	from 0 to 31	Used to select a log.
Timestamp	Recorded local time and date	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Assist	Assist notification result	-	Notification is not sent or will be retried.
		OK	Notification is successful.
		NG	Notification fails.
Reason	Message to show a cause	Character string	Available in English and Japanese according to the language mode.

Select a maintenance action report (MAR) log from the MAR log list, and the MAR log details are displayed.

```
+------------------------------+
| MARLOG (2009-03-09 10:13:39) |
+------------------------------+
-- CALL FACTOR INFORMATION --
 Reason         : 21
 Impact         : UU
 Partition No   : -
 BMC-ID         : -

-- RC INFORMATION --
 EVENT          : 0000 02 19584F4B 6100 04 2139 6FA00000
 RC             : 10 6000 40 21390000 6FA00000
 RC NAME        : IOA1 STATUS
 COMMENT        : I/O module#1: Failure
(1) Replace the I/O module


Hit enter key. (Enter)
-- FRU INFORMATION --
-- --------------- ------------------- ----------------- --------------
 0 | UNIT         : SYS                 | FRU MNEMONIC   : IOA1
   | PARTS NAME   :  -                  | REV            :  -
   | ACTION       : RPL                 | WEIGHT         : 100
   | DRAWING_NO   :  -                  | SERIAL NO      :  -
-- --------------- ------------------- ----------------- --------------
-- End of data --
Hit enter key.
```

Items of the detailed MAR log are described in the table below:

Item	Description of item	Value	Description of value
Timestamp	Recorded time and date (Local time)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
Reason	Message to show a reason	XX	XX: Reason code

Item	Description of item	Value	Description of value
Impact	Connection trigger	UU	Emergency: fix it quickly
		UE	Non-emergency: fix it the next day
		US	Non-emergency: fix it within a week
		UC	Non-emergency: the redundant component work
		PR	Protective maintenance request
Partition No	Number of a failed partition	-	Invalid for I/O slot expansion units
BMC-ID	Primary BMC ID	-	Invalid for I/O slot expansion units
EVENT	Event code	Hexadecimal string	-
RC	RC	Hexadecimal string	-
RC NAME	RC name	Character string	Displayed in ASCII
COMMENT		Character string	RC comment in ASCII

Items of field replaceable unit (FRU) information are described in the list below: FRU information to MAR logs

Item	Description of item	Value	Description of value
UNIT	Unit name	See UNIT and FRU mnemonic shown below:	
PARTS NAME	Component name	Character string in ASCII	-
ACTION	Action code	RPL	Replace
		CHK	Check
		ADJ	Adjust
		CRT	Correct
		CLN	Clean
		CKE	Check externally.
		RTM	Execute TMP.
		RPE	Replace externally.
		RMD	Execute MD.
		CSP	Call maintenance personnel.
		ADD	Add
		REM	Remove
DRAWING NO	Part number	Character string in ASCII	-
FRU MNEMONIC	FRU mnemonic	See UNIT and FRU mnemonic shown below:	
REV	Revision	Character string in ASCII	-
WEIGHT	Ratio of potentially failed components	Integer	Ratio in % of potentially failed component(s) to one error (100%).
SERIAL NO	Serial number	Character string in ASCII	-

Details of UNIT and FRU mnemonic are described in the list below:

UNIT	FRU mnemonic	Major item	Description
SYS	BKPL	Server chassis	Backplane
	FANx (x: 0 to 7)		FAN module
	PANEL		Front panel
	PSx (x: 0 to 3)		Power supply module
	ACINx (x: 0 to 1)		AC power input module
	IOAx (x: 0 to 1)		I/O module
	PCIBMx (x: 0 to 15)		I/O adapter
	SYSVOL		Check the voltage value with a tool.
IOA (x: 0 to 1)	CF	I/O module	CF card
	BAT		Lithium battery
OTHER	AIRCON	Others	Check the room temperature.
	BUNDEN		Check the distribution panel.
	USBDEV		USB device

If you type C in the DL command menu and press **Enter**, the RC list is displayed. Then select an RC, and the detailed information is displayed.

```
-- RC list --
No.  Timestamp            RE UID  EC Failure  Additional
---- -------------------- -- ---- -- -------- ----------
   0 2010-01-18 13:55:29  10 6000 40 21390000 6FA00000
   1 2010-01-18 13:09:07  10 6000 40 21390000 6FA00000
   2 2010-01-18 10:40:42  10 6001 40 21190000 6FA00000
   3 2010-01-18 10:26:24  10 6001 40 21190000 6FA00000
   4 2010-01-18 10:26:24  10 6601 40 F2F90000 07A30B04
   5 2010-01-14 17:44:57  10 6000 40 21390000 6FA00000
   6 2010-01-14 17:32:34  10 6001 40 21190000 6FA00000
   7 2010-01-14 17:32:34  10 6601 40 F2F90000 07A30B04
   8 2010-01-14 14:20:34  10 6200 40 1E510000 07A30000
   9 2010-01-14 14:20:34  10 6200 70 08500000 6FA30000
  10 2010-01-14 14:20:34  10 6200 40 08500000 6FA10000
  11 2010-01-14 14:20:34  10 6000 70 0B400000 0BA30000
  12 2010-01-14 14:20:34  10 6000 40 0C3B0000 6FA10000
  13 2010-01-14 14:20:34  10 6000 40 0C3A0000 6FA10000
  14 2010-01-14 14:20:33  10 6000 40 21390000 6FA00000
  15 2010-01-14 14:20:33  10 6000 40 1E370000 07A30000
-- more (Q:Quit) --
Select No. (0-15) : 2 (Enter)
-- RC INFORMATION --
 RC            : 10 6001 40 21190000 6FA00000
 RC NAME       : IOA0 STATUS
 COMMENT       : I/O module#0 : Failure
(1) Replace the I/O module


Hit enter key. (Enter)
```

Items of the RC list are described in the table below:

Item	Description of item	Value	Description of value
No.	Log number	0 to 15	-
Timestamp	Recorded time and date (Local)	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
RE	RC type enhanced bit	XX	2 digits in hex
UID	Unit ID	XXXX	4 digits in hex
EC	Event code	XX	2 digits in hex
Failure	Failure code	XXXXXXXX	8 digits in hex
Additional	Additional code	XXXXXXXX	8 digits in hex

Items of the RC information are described in the table below:

Item	Description of item	Value	Description of value
RC	Reference code	Hexadecimal string	Consists of RE, UID, EC, Failure, and Additional in the RC list.
RC NAME	RC name	Character string	Displayed in ASCII.
COMMENT	-	Character string	RC comment in ASCII.

❑ DEL command

You can delete files from the user directory of the I/O module. Type `DL` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> DEL (Enter)

<< DEL - Delete copy of log. >>

-- Log menu --
    D. Delete file.
    Q. Quit.
(D,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
D.	Delete file.	-
Q.	Quit	Quits the DEL command.

Type D in the Delete menu of the user directory and press Enter, and the file name list in the user directory is displayed. You are required to select a file to delete. Type the number to specify the file, and the confirmation message appears for deletion. At the prompt, to delete the file, type Y and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(D,[Q]) : D (Enter)

-- File list --
<File0>
io-conf.backup

Select file (0,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <io-conf.backup> Deleting file was completed.
Hit enter key. (Enter)
```

❑ FW command

You can display the firmware version of an I/O module. Type FW at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> FW (Enter)

<< FW - Update I/O module firmware. >>

-- I/O module firmware --
# Behavior Revision
- -------- --------------------------------
0 Active   A0101-A-3138
1 Standby  A0101-A-3138

-- Dictionary --
Revision : 00053

-- I/O module firmware menu -
    U. Update firmware
    Q. Quit.
(U, [Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
U.	Update firmware.	Updates the dictionary.
Q.	Quit	Quits the FW command.

Items of the I/O module firmware are described in the table below: I/O module firmware information.

Item	Description of item	Value	Description of value
#	I/O module slot number	0, 1	-
Behavior	I/O module mode	-------	Not installed; undecided mode; BootDisable
		Active	Unit management master
		Standby	Not unit management master
Revision	General version of I/O slot expansion unit controller firmware	-------	Not installed.
		XXXXXXXXXXXXXXX	General version of I/O slot expansion unit controller firmware: 32 characters

Dictionary is described in the table below: Dictionary information.

Item	Description of item	Value	Description of value
Revision	Dictionary file version	XXXXX	Dictionary version: 5 characters

You can update the dictionary by typing `U` in the FW command menu and pressing **Enter**. The dictionary to be updated and then a confirmation message are displayed. At the prompt, if you type `Y` and press **Enter**, the dictionary will be updated. To cancel the update, type `N` after the confirmation message and press **Enter**, or just press **Enter**.

```
-- Update file information --
File name                        File size(byte)
-------------------------------- ---------------
dict.00059.update                         280310

Confirm? (Y,[N]) : Y (Enter)
--- Update I/O module firmware progress ---
I/O module0 process:Completed.
0% ------ 20% ----- 40% ----- 60% ----- 80% ---- 100%
|.................................................| [100]%

I/O module1 process:Completed.
0% ------ 20% ----- 40% ----- 60% ----- 80% ---- 100%
|.................................................| [100]%

- Update firmware was completed.
Hit enter key. (Enter)
```

- Be sure not to downgrade the current dictionary to any earlier version.
- Locate the currently installed dictionary version in the window displayed immediately after the FW command is performed.
- Check your dictionary version with the dictionary file name as follows:

  Naming rules: dict.xxxxx.update
  xxxxx: Dictionary version

You need to transfer the dictionary to the user directory in the I/O slot expansion unit via FTP or SFTP before updating it. For access via FTP or SFTP, use the same account name and password as those for login.

❑ LM command

You can display and set a language. Type `LM` at the prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> LM (Enter)

<< LM - Language Mode. >>

-- Language mode --
Language      : Japanese

-- Language mode setting menu --
    L. Set language mode.
    Q. Quit.
(L,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
L.	Set language mode.	
Q.	Quit	Quits the LM command.

Items of the language mode are described in the table below:

Item	Description of item	Value	Description of value
Language	Language used on screen	English	-
		Japanese	-

If you type L in the LM command menu and press **Enter**, you can set a language. The current setting value and specifiable values are displayed. At the prompt, press **Enter**, or input a setting value and press **Enter**, and the new setting value is displayed. A confirmation message appears. At the prompt, press Y and press **Enter**, and the language value will become effective. To cancel the setting value, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
Language      : Japanese
(0=English,1=Japanese,[Unchange]) : 1 (Enter)

-- Language mode --
Language      : Japanese

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

Network management

❑ LC command

You can display and set the network information with this command. Type `LC` at prompt, and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> LC (Enter)

<< LC - LAN configuration. >>

-- I/O module LAN interface setting --
IP address      Subnetmask      Default gateway
--------------- --------------- ---------------
192.168.  0. 65 255.255.255.  0   0.  0.  0.  0

-- I/O module DNS setting --
D IP address
- ---------------
0   0.  0.  0.  0
1   0.  0.  0.  0
2   0.  0.  0.  0

-- Management LAN setting menu --
    E. Edit I/O module setting.
    Q. Quit
(E,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
M.	Edit I/O module setting	Edits network setting for the I/O module.
Q.	Quit	Quits the LC command.

If you type `E` in the LC command menu and press **Enter**, the current values appear in numerical order as shown in the following table. At the prompt, press **Enter**, or enter a setting value and press **Enter**, and the screen will go to the next setting.

Menu	Description
1	IP address of the I/O module
2	Subnetmask of the I/O module
3	Default gateway of the I/O module
4	IP address of the DNS server 0
5	IP address of the DNS server 1
6	IP address of the DNS server 2

If you enter the IP address of DNS server 2, the value after the change is displayed. A warning indicating that the connection to the I/O module may be disconnected after the setting is applied is displayed. A message to confirm the change is displayed. At the prompt, type Y and press **Enter**. The network setting is reflected on the I/O module. When the IP address of the I/O module is changed, the session connected using the former IP address is disconnected. To cancel the network setting in the I/O module, type N and press **Enter**, or just press **Enter** to confirm the new setting value.

```
(E,[Q]) : L (Enter)
IP address       : 192.168.  0. 65
([Unchange]) : 192.168.0.10 (Enter)
Subnetmask       : 255.255.255.  0
([Unchange]) : 255.255.254.0 (Enter)
Default gateway  :   0.  0.  0.  0
([Unchange]) : (Enter)
DNS0             :   0.  0.  0.  0
([Unchange]) : (Enter)
DNS1             :   0.  0.  0.  0
([Unchange]) : (Enter)
DNS2             :   0.  0.  0.  0
([Unchange]) :
-- I/O module LAN interface setting --
IP address      Subnetmask      Default gateway
--------------- --------------- ---------------
192.168.  0. 10 255.255.254.  0   0.  0.  0.  0

-- I/O module DNS setting --
D IP address
- ---------------
0   0.  0.  0.  0
1   0.  0.  0.  0
2   0.  0.  0.  0

WARNING : Session may be disconnected when setting saved.

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

❑ LFT command

You can set redundancy to LAN ports. Type `LFT` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> LFT (Enter)

<< LFT - Link Fault Tolerance setting. >>

-- Link Fault Tolerance setting --
Ext port I/O module        LFT     Down(s) Up(s)
-------- ----------------- ------- ------- -----
MGMT     Active            Enable        3   180
MNT      Active            Enable        3   180

-- Link Fault Tolerance setting menu --
    G. Edit management port setting.
    Q. Quit.
(G,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
G.	Edit management port setting	Edit redundancy setting on MGMT port of the I/O module.
Q.	Quit	Quits the LFT command.

Items on the screen are described in the table below.

Menu	Description
Ext port	External output port MGMT: MGMT port; MNT: MAINT port
I/O module	I/O module with open ports Active: unit management master Standby: non-unit management master
LFT	Redundancy status of the management LAN port: Enable or Disable
Down(s)	How many seconds takes to ascertain that the external output port is linkdown: 1 to 3600 seconds can be set.
Up(s)	How many seconds takes to ascertain that the external output port is linkup: 1 to 3600 seconds can be set.

If you type G in the LFT command menu and press **Enter**, the current redundancy setting in the MGMT port of the management LAN port appears. At the prompt, enter a redundancy setting value of the management LAN port. The required time to ascertain linkdown is displayed in seconds. Next, enter a time to ascertain linkdown in seconds. A time required to ascertain the current linkup status is displayed. Enter a setting in seconds to ascertain linkup. The changed setting value is displayed. A confirmation message appears. Type Y and press **Enter**, and the management LAN redundancy setting is saved. To cancel the setting change, type N and press **Enter**, or just press **Enter**.

```
(G,[Q]) : G (Enter)
LFT     : Enable
(0=Disable,1=Enable,[Unchange]) : 0 (Enter)
Down(s) :     3
(1-3600,[Unchange]) : 10 (Enter)
Up(s) :   180
(1-3600,[Unchange]) : 1800 (Enter)

-- Link Fault Tolerance setting --
Ext port I/O module        LFT     Down(s) Up(s)
-------- ----------------- ------- ------- -----
MGMT     Active            Disable      10  1800
MNT      Active            Enable        3   180

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

For the MAINT port, you can only display the setting.

❑ LS command

You can display the MAC address of the I/O module. Type `LS` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> LS (Enter)

<< LS - LAN controller discriminating information. >>

-- MAC addresses on I/O module --
# controller0        controller1
- ------------------ ------------------
0 00:00:87:12:5B:B0  00:00:87:12:5B:B1
1 00:00:87:12:5B:4C  00:00:87:12:5B:4D

-- LAN controller information menu --
    Q. Quit.
([Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
Q.	Quit	Quits the LS command.

Items on the screen are described in the table below.

Menu	Description
#	I/O module slot number
controller0	MAC address to the network interface controller0
controller1	MAC address to the network interface controller1

❑ XD command

You can execute the diagnostics. Type XD at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> XD (Enter)

<< XD - Execute diagnostics. >>

-- Diagnostics menu --
    I. ICMP Ping.
    Q. Quit.
(I,[Q]) :
```

Select a menu item from the following table to execute it.

Menu		Description
I.	ICMP Ping	Check the network connection using the ICMP Ping.
Q.	Quit	Quits the XD command.

If you type [I] in the XD command menu and press **Enter**, the prompt is ready for an IP address. When pressing **Enter** during the prompt for IP address, the screen goes back to the XD command menu. Enter the IP address at the prompt. A message to confirm executing diagnostics appears. At the prompt, type Y and press **Enter**, diagnostics is executed and the result is displayed. To cancel diagnostics, type N and press the **Enter**, or just press **Enter**.

```
(I,[Q]) : I (Enter)
Input IP address ([Q=Quit]) : 192.168.0.253 (Enter)

Confirm? (Y,[N]) : Y(Enter)

PING 192.168.0.253 (192.168.0.253): 56 data bytes
64 bytes from 192.168.0.253: icmp_seq=0 ttl=64 time=3.2 ms
64 bytes from 192.168.0.253: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 192.168.0.253: icmp_seq=2 ttl=64 time=0.2 ms

--- 192.168.0.253 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/1.2/3.2 ms

Hit enter key. (Enter)
```

❑ MLC command

You can display the network setting for maintenance. Type `MLC` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> MLC (Enter)

<< MLC - Maintenance LAN setting. >>

-- I/O module --
# IP address      Subnetmask
- --------------- ---------------
0 192.168.254.  1 255.255.255.  0
1 192.168.254.  2 255.255.255.  0

-- static route --
Network address   :   0.  0.  0.  0
Subnetmask        :   0.  0.  0.  0
Router IP address :   0.  0.  0.  0

-- Maintenance LAN setting menu --
    Q. Quit.
([Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
Q.	Quit	Quits the MLC command.

Items per I/O module on the screen are described in the table below.

Menu	Description
IP address	IP address of the interface for the maintenance network of the I/O module
Subnetmask	Subnetmask of the interface for the maintenance network of the I/O module

Items of the static route are described in the table below.

Menu	Description
Network address	Network address of a network targeted for static routing
Subnetmask	Subnetmask of a network targeted for static routing
Router IP address	IP address of a router transferring to targeted network for static routing

❑ ILC command

You can set the internal network setting. Type `ILC` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> ILC (Enter)

<< ILC - Internal LAN setting. >>

-- Internal network --
Network address : 192.168.253.  0
Subnetmask      : 255.255.255.  0

-- Internal network menu --
    E. Edit setting.
    Q. Quit.
(E,[Q]) :
```

Select a menu item from the following table to execute it.

Menu		Description
E.	Edit setting.	Sets the internal network.
Q.	Quit	Quits the ILC command.

Items displayed on the screen are described in the table below.

Item	Description
Network address	Network address of internal network Default value: 192.168.253.0
Subnetmask	Subnetmask of internal network Default value: 255.255.255.0

If you type `E` in the ILC command menu and press **Enter**, the current setting is displayed. At the prompt, enter an internal network address, and the changed setting value is displayed. A warning message appears indicating that the I/O module will restart after the setting change is displayed. A confirmation message appears. Type `Y` and press **Enter**. The internal network setting is saved. Then the I/O module will restart. To cancel the setting, type `N` and press **Enter**, or just press **Enter**.

```
(E,[Q]) : E(Enter)
Network address : 192.168.253.  0
([Unchange]) : 192.168.200.0(Enter)

-- Internal network --
Network address : 192.168.200.  0
Subnetmask      : 255.255.255.  0

WARNING : If confirm, I/O module restart and this connect is lost.

Confirm? (Y,[N]) : Y(Enter)
- <I/O module0> Restarting
(Disconnected.)
```

External server connection manager

❑ BSM command

You can display and set connection setting to ServerConductor (SC)/ Blade Server Manager (BSM). Type `BSM` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> BSM (Enter)

<< BSM - SC/BSM setting. >>

-- Manager setting --
No. Name            IP address      Alert level
--- --------------- --------------- -----------
  0 BSM_0           192.168.  0.254 All
  1  -------------   -------------   ---------
  2  -------------   -------------   ---------
  3  -------------   -------------   ---------

-- SC/BSM setting menu --
    M. Edit manager setting.
    D. Delete manager setting.
   DB. Show/Edit basis detail setting.
   DM. Show/Edit manager detail setting.
    Q. Quit.
(M,D,DB,DM,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
M.	Edit manager setting	Edits SC/BSM connection setting.
D.	Delete manager setting	Deletes SC/BSM connection setting.
DB.	Show/Edit basis detail setting.	Shows and edits the processing details about accepting requests from SC/BSM.
DM.	Show/Edit manager detail setting.	Shows and edits details about SC/BSM connection setting.
Q.	Quit	Quits the BSM command.

Items displayed on the screen are described in the table below.

Item	Description
No.	SC/BSM connection setting number
Name	SC/BSM name
IP address	IP address of SC/BSM
Alert level	Alert level notified to SC/BSM All: all alerts are notified. Alert: alerts in the error level are notified. Information: alerts in the information level are notified. Disable: no alert is notified.

If you type [M] in the BSM command menu and press **Enter**, you are asked to select a SC/BSM connection setting. At the prompt, enter a SC/BSM connection setting number. The current setting is displayed in the numerical order as shown in the table below, or the recommended value is displayed. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	SC/BSM name
2	SC/BSM IP address
3	Alert level to notify SC/BSM

If you enter an alert level, the changed setting value is displayed. A confirmation message appears. At the prompt, type Y and press **Enter**. The edited SC/BSM connection setting is applied. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(M,D,DB,DM,T,[Q]) : M (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
Name                 : BSM_1
([Unchange]) : (Enter)
IP address           :   0.  0.  0.  0
([Unchange]) : 192.168.0.253 (Enter)
Alert level          : All
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : 1 (Enter)

-- Manager setting --
No. Name            IP address      Alert level
--- --------------- --------------- -----------
  0 BSM_0           192.168.  0.254 All
  1 BSM_1           192.168.  0.253 Alert
  2  -------------   -------------   ---------
  3  -------------   -------------   ---------

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type D in the BSM command menu and press **Enter**, you are asked to select a SC/BSM connection setting. At the prompt, enter a SC/BSM connection setting number, and the changed setting is displayed. A confirmation message appears. Type Y and press **Enter**, and the deleted SC/BSM connection setting is saved. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(M,D,DB,DM,T,[Q]) : D (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
-- Manager setting --
No. Name            IP address      Alert level
--- --------------- --------------- -----------
  0 BSM_0           192.168.  0.254 All
  1  -------------   -------------   ---------
  2  -------------   -------------   ---------
  3  -------------   -------------   ---------

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type DB in the BSM command menu and press **Enter**, the current setting is displayed.

```
(M,D,DB,DM,T,[Q]) : DB (Enter)
-- Basis detail setting --
Command port         : 21001

-- Basis setting menu --
    S. Edit setting.
    Q. Quit.
(S,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
S.	Edit setting	Edits SC/BSM setting related to command requests.
Q.	Quit	Returns to the previous menu.

If you type S in the BSM command menu and press **Enter**, the current port number setting that receives requests from SC/BSM is displayed. At the prompt, press **Enter**, or enter a port number and press **Enter**. The changed setting value is displayed. A confirmation message appears. Type Y and press **Enter**, and the port number setting is saved. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(S,[Q]) : S (Enter)
Command port         : 21001
(1-65535,[Unchange]) : 21002 (Enter)

-- Basis detail setting --
Command port         : 21002

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type DM in the BSM command menu and press **Enter**, you are asked to select a SC/BSM connection setting. At the prompt, enter an SC/BSM connection setting number, and the current setting of the specified number is displayed.

```
(M,D,DB,DM,T,[Q]) : DM (Enter)
Select manager (0-3,[Q=Quit]) : 1 (Enter)
-- Manager detail setting --
No.                   : 1
Name                  : BSM_1
IP address            : 192.168.  0.253
Alert port            : 20079
Alert level           : Alert
Retry interval (sec) : 5
Retry duration (min) : 10

-- Manager setting menu --
    S. Edit setting.
    Q. Quit.
(S,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
S.	Edit setting.	Edits details of SC/BSM connection setting.
Q.	Quit	Returns to the previous menu.

If you type S in the BSM command menu and press **Enter**, the current setting is displayed in the numerical order as shown in the table below. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	SC/BSM name
2	SC/BSM IP address
3	SC/BSM alert report number
4	Alert level to notify SC/BSM
5	Intervals between connection retries: 5 to 50 seconds
6	Interval duration: 4 to 20 minutes

If you enter a duration period for connection retries, the changed setting is displayed. A confirmation message appears. At the prompt, type `Y` and press **Enter**, and SC/BSM connection setting is saved. To cancel the setting, type `N` and press **Enter**, or just press **Enter**.

```
(S,[Q]) : S (Enter)
Name                  : BSM_1
([Unchange]) : BSM_01 (Enter)
IP address            : 192.168.  0.253
([Unchange]) : 192.168.0.254 (Enter)
Alert port            : 20079
(1-65535,[Unchange]) : 20078 (Enter)
Alert level           : Alert
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : 0 (Enter)
Retry interval (sec) : 5
(5-50,[Unchange]) : 6 (Enter)
Retry duration (min) : 10
(4-20,[Unchange]) : 5 (Enter)

-- Manager detail setting --
No.                   : 1
Name                  : BSM_01
IP address            : 192.168.  0.254
Alert port            : 20078
Alert level           : All
Retry interval (sec) : 6
Retry duration (min) : 5

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

❑ SNM command

You can set Simple Network Management Protocol (SNMP) of the I/O module. Type `SNM` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SNM (Enter)

<< SNM - SNMP setting. >>

-- SNMP agent setting --
Agent            : Enable
Contact name     : contact
Location         : location
Port number      : 161
Trap level       : All
SNMP version     : v1/v2c/v3
Engine ID string : engineid
Engine ID        : 8000007404656E67696E656964

-- SNMP manager setting --
<Manager0>
SNMP version            : v1/v2c
Hostname                : 0.0.0.0
Port number             : 162
Community name          : ---

<Manager1>
SNMP version            : v3
Hostname                : 0.0.0.0
Port number             : 162
User name               : User01
Access type             : noAuthnoPriv
Authentication password :  ---
Encryption type         :  ---
Encryption password     :  ---

<Manager2>
SNMP version            : v1/v2c
Hostname                : 0.0.0.0
Port number             : 162
Community name          : ---

<Manager3>
SNMP version            : v3
Hostname                : 192.168.0.22
Port number             : 162
User name               : User03
Access type             : AuthPriv
Authentication type     : MD5
Authentication password : *****
Encryption type         : DES
Encryption password     : *****

-- MIB information --
Version : 00-00

-- SNMP setting menu --
    A. Edit agent setting.
```

```
    M. Edit manager setting.
   DA. Delete agent setting.
   DM. Delete manager setting.
    T. SNMP trap test.
    C. Copy MIB file.
    Q. Quit.
(A,M,DA,DM,T,C,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Edit agent setting	Sets SNMP agents.
M.	Edit manager setting	Configures the setting necessary for SNMP manager connection.
DA.	Delete agent setting	Deletes SNMP agent settings.
DM.	Delete manager setting	Deletes settings required for SNMP manager connection.
T.	SNMP trap test	Transmits the SNMP trap for tests.
C.	Copy MIB file	Copies management information base (MIB) files.
Q.	Quit	Quits the SNM command.

SNMP agent setting items are described in the table below: SNMP agent setting.

Item	Description of item	Value	Description of value
Agent	SNMP agent function	Enable	Valid
		Disable	Invalid
Contact name	System contact name (System administrator name)	Character string in ASCII	Up to 60 characters in ASCII
Location	System location: installation site	Character string in ASCII	Up to 60 characters in ASCII
Port number	Port number for SNMP agent to use	Integer	Integer between 1 and 65535: However, the value162 is not available.
Trap level	Levels notified in SNMP trap	Disable	Nothing notified
		Alert	Notifies reports in non-recoverable and serious level.
		Information	Notifies reports in information level.
		All	All levels are notified.
SNMP version	SNMP version	v1/v2c	SNMP version used by agents Value: v1/v2c
		v1/v2c/v3	SNMP version used by agents Value: v1/v2c/v3
Engine ID string	A string forming an engine ID	-------	SNMP version v1/v2c is used, or no setting
		Character string in ASCII	1 and up to 27 character string in ASCII
Engine ID	Engine ID	-------	SNMP version v1/v2c is used, or no setting

Item	Description of item	Value	Description of value
		Character string in ASCII	1 and up to 27 character string in ASCII

SNMP manager setting items are described in the table below: SNMP manager setting.

Item	Description of item	Value	Description of value
SNMP version	SNMP version	v1/v2c	SNMP version v1/v2c is used.
		v3	SNMP version v3 is used.
Host name	SNMP manager address	-	Up to 4 addresses of the SNMP manager can be registered.
		Domain name	FQDN for SNMP manager: Up to 255 character string with printable ASCII code is displayed.
		IP address	IP addresses of the SNMP manager
		-------	No setting
Port number	Port number of the SNMP manager	Integer	Integer between 1 to 65535. However, 161 is not available.

With SNMP version v1/v2c, the following setting is displayed.

Item	Description of item	Value	Description of value
Community name	Community name for SNMP manager	Character string in ASCII	Up to 60 character string in ASCII

With SNMP version v3, the following settings are displayed.

Item	Description of item	Value	Description of value
User Name	User name	Character string in ASCII	Character string in ASCII: at least 1; up to 32 characters
Access type	Access type	noAuthnoPriv	No authentication and encryption
		AuthnoPriv	With authentication but no encryption
		AuthPriv	With authentication and encryption
Authentication type	Authentication type	-------	No authentication
		MD5	Type: MD5
		SHA	Type: SHA
Authentication password	Authentication password	-------	No authentication or no setting
		Character string in ASCII	String comprised of 8 to 64 characters in ASCII With a setting, 5 asterisks "*****" is always displayed.
Encryption	Encryption type	-------	No encryption

Item	Description of item	Value	Description of value
type		DES	Type: DES
		AES	Type: AES
Encryption password	Encryption password	-------	No encryption or no setting
		Character string in ASCII	String comprised of 8 to 64 characters in ASCII With a setting, 5 asterisks "*****" is always displayed.

MIB information is displayed.

Item	Description of item	Value	Description of value
Version	MIB file version	Character string in ASCII	-

If you type A in the SNM command menu and press **Enter**, you can set the SNMP agent setting.

The current setting is displayed in numerical order as shown in the following table. To proceed to the next setting, press **Enter,** or enter a setting value and press **Enter**.

Menu	Description
1	SNMP agent : Enable or Disable
2	System contact name: administrator name
3	System location
4	Port number used by SNMP agents
5	SNMP trap notification level
6	SNMP version to be used
7	Type a character string for the engine ID (when SNMP version v1/v2/v3 is selected).

When you type a notification level with SNMP trap or a character string for ID, the changed setting value is displayed. A confirmation message appears. Type Y and press **Enter**, and the SNMP agent setting is applied. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM.T,C,[Q]) : A (Enter)

Agent             : Enable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Contact name      :
([Unchange]) : user01 (Enter)
Location          :
([Unchange]) : A3F (Enter)
Port number       : 161
(1-65535,[Unchange]) : (Enter)
Trap level        : All
(0=All,1=Alert,2=Information,3=Disable,[Unchange]) : (Enter)
SNMP version      : v1/v2c
(0=v1/v2c,1= v1/v2c/v3,[Unchange]) : 1 (Enter)
Engine ID string : zzzzzzzzzzz
([Unchange]) : xxxxxxxxxxxxx (Enter)
```

```
-- SNMP agent setting --
Agent            : Enable
Contact name     : user01
Location         : A3F
Port number      : 161
Trap level       : All
SNMP version     : v1/v2c/v3
Engine ID string : xxxxxxxxxxxxx
Engine ID        : yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

The screen for engine ID strings is displayed only when version v1/v2/v3 is selected. Be sure to configure a string for engine ID. If no string is configured for engine ID, "([Unchange]) is not displayed.

If you type M in the SNM command menu and press the [Enter] key, you can set the SNMP manager connection. You are asked to select a SNMP manager. When you type a SNMP manager number, the current setting is displayed in the following numerical order. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

With SNMP version v1/v2c:

Menu	Description
1	Address for SNMP manager
2	Port number for SNMP manager
3	Community Name for SNMP manager

When you type a community manager of the SNMP manager, the changed setting value is displayed. A confirmation message appears. Type Y and press **Enter**, and the SNMP manager connection setting is applied. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : M (Enter)
Select manager (0-3,[Q=Quit]) : 0 (Enter)
SNMP version   : v1/v2c
(0=v1/v2c,1=v3,[Unchange]) : 0 (Enter)
Hostname       : 0.0.0.0
([Unchange]) : 192.168.100.200 (Enter)
Port number    : 162
(1-65535,[Unchange]) : (Enter)
Community name : Community
([Unchange]) : com01 (Enter)

-- SNMP manager setting --
<Manager0>
SNMP version            : v1/v2c
Hostname                : 192.168.100.200
Port number             : 162
Community name          : com01
```

```
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

Be sure to configure a community name. If not configured, “([Unchange]) is not displayed.

With SNMP version v3:

Menu	Description
1	Address for SNMP manager
2	Port number for SNMP manager
3	User name
4	Access type
5	Authentication type when a type of access other than noAuthnoPriv is selected.
6	Authentication password when a type of access other than noAuthnoPriv is selected.
7	Encryption type when a type of access AuthPriv is selected.
8	Encryption password when a type of access AuthPriv is selected.

When you type an encryption password, the changed setting value is displayed. A confirmation message appears. Type `Y` and press **Enter**, and the SNMP manager connection setting is applied. To cancel the setting, type `N` and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : M (Enter)
Select manager (0-3,[Q=Quit]) : 0 (Enter)
SNMP version   : v1/v2c
(0=v1/v2c,1=v3,[Unchange]) : 1 (Enter)
Hostname       : 0.0.0.0
([Unchange]) : 192.168.0.22 (Enter)
Port number    : 162
(1-65535,[Unchange]) : (Enter)
User name      : xxxxxx
([Unchange]) : UserName : (Enter)
Access type    : noAuthnoPriv
(0=noAuthnoPriv,1=AuthnoPriv,2=AuthPriv,[Unchange]) : 2  (Enter)
Authentication type : MD5
(0=MD5,1=SHA,[Unchange]) : 1 (Enter)
Authentication password : *****
([Unchange]) :        (Enter)
Encryption type : DES
(0=DES,1=AES,[Unchange]) : 1 (Enter)
Encryption password : *****
([Unchange]) :        (Enter)

-- SNMP manager setting --
<Manager0>
SNMP version           : v3
```

```
Hostname                : 192.168.0.22
Port number             : 162
User name               : UserName
Access type             : AuthPriv
Authentication type     : SHA
Authentication password : *****
Encryption type         : AES
Encryption password     : *****

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

Be sure to configure a user name. If not configured, “([Unchange]) is not displayed.

The screen for authentication type is displayed when an access type other than noAuthnoPriv is selected.

Be sure to configure an authentication password. If not configured, “([Unchange]) is not displayed. When a password is configured, 5 asterisks “*****” are displayed.

The screen for encryption type is displayed when AuthPriv as an access type is selected.

Be sure to configure an encryption password. If not configured, “([Unchange]) is not displayed. When a password is configured, 5 asterisks “*****” are displayed.

If you type DA in the SNM command menu and press **Enter**, you can delete SNMP agent settings. Type Y and press **Enter**, and the SNMP agent is deleted. To cancel the deletion, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : DA (Enter)

-- SNMP agent setting --
Agent            : Disable
Contact name     :
Location         :
Port number      : 161
Trap level       : All
SNMP version     : v1/v2c
Engine ID string :  ---
Engine ID        :  ---

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type DM in the SNM command menu and press **Enter**, you can delete SNMP manager settings. Select a manager number to delete and the settings after deletion and a confirmation message are displayed. At the prompt, type Y and press **Enter**, and the SNMP manager setting is deleted. To cancel the deletion, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : DM (Enter)

Select manager (0-3,[Q=Quit]) : 0 (Enter)

-- SNMP manager setting --
<Manager0>
SNMP version            : v1/v2c
Hostname                : 0.0.0.0
Port number             : 162
Community name          :  ---

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type T in the SNM command menu and press **Enter**, an SNMP trap for test is sent. Type Y in the message to confirm the test transmission and press **Enter.** The SNMP trap for test is transmitted. To cancel the test SNMP trap transmission, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : T (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Sending SNMP trap was completed.
Hit enter key. (Enter)
```

If you type C in the SNM command menu and press **Enter**, a copy of the MIB file is mirrored into the user directory. Type Y in the message to confirm the copy execution and press **Enter** to copy it. To cancel the copy process, type N and press **Enter**, or just press **Enter**.

```
(A,M,DA,DM,T,C,[Q]) : C (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Copying MIB file was completed.
Hit enter key. (Enter)
```

❑ MI command

You can set e-mail notification settings. Type `MI` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> MI (Enter)

<< MI - E-mail notification. >>

-- E-mail setting menu --
    C. Show e-mail setting.
    E. Edit e-mail notification setting.
    A. Edit e-mail address.
    M. Send e-mail notification.
    Q. Quit.
(C,E,A,M,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Show e-mail setting.	Displays the e-mail notification settings.
E.	Edit e-mail notification setting.	Sets the e-mail notification setting.
A.	Edit e-mail address.	-
M.	Send e-mail notification.	-
Q.	Quit.	Quits the MI command.

If you type C in the MI command menu and press **Enter**, you can display the e-mail notification setting.

```
(C,E,A,M,[Q]) : C (Enter)
-- E-mail notification setting --
Notification : Enable
Address      : dish@hitachi.com
Host (FQDN)  : bs2kfw.com
Comment      : test
SMTP server  : 192.168.0.76
Port number  : 25

-- E-mail authentication setting --
Authentication : Enable
Name           : auth
Method         : PLAIN

-- E-mail encryption setting --
Encryption   : Disable
Protocol     : SSL

-- E-mail address --
<Address0>
Nickname  : user0
Address   : user0@one8647.com
Attach    : Yes
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Hit enter key. (Enter)
```

If you type E in the MI command menu and press **Enter**, you can display the email notification setting menu.

```
(C,E,A,M,[Q]) : E (Enter)
-- E-mail notification setting menu --
    E. Edit notification setting.
    R. Reset notification setting.
    Q. Quit.
(E,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
E	Edit notification setting.	-
R.	Reset notification setting.	-
Q.	Quit	Returns to the previous menu.

Items of e-mail notification setting are described in the table below.

Item	Description of item	Value	Description of value
Notification	Enable or Disable the email notification	Enable	Valid
		Disable	Invalid
Address	e-mail address of the system administrator	Character string in ASCII	Up to 64 character strings in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “ _”, “ ·”, “[”, “]”. Make sure to specify the system administrator’s e-mail address when the e-mail notification function is enabled.
Host (FQDN)	Host name (FQDN)	Character string in ASCII	Host name of the I/O module. Enter it as Qualified Domain Name. Up to 64 character string in ASCII Make sure to specify the host name when the e-mail notification function is enabled.
Comment	Comment for information to identify a customer	Character string in ASCII	Up to 32 characters in ASCII to specify a customer.
SMTP server	SMTP server	Character string in ASCII	IP address of the SMTP server or the SMTP server host name Up to 64 character string in ASCII Make sure to specify the SMTP server when the e-mail notification function is enabled.
Authentication	SMTP authentication	Enable	Valid
		Disable	Invalid
Name	Account name for SMTP authentication	Character string in ASCII	Account name registered in the SMTP server Up to 64 character string in ASCII Make sure to specify an account name for SMTP authentication when the SMTP authentication function is enabled.

Item	Description of item	Value	Description of value
Password	Password for SMTP authentication	Character string in ASCII	Password for the account registered in the SMTP server. Up to 64 character string in ASCII Make sure to specify a password for SMTP authentication when the SMTP authentication function is enabled.
Method	SMTP authentication method	PLAIN	Plain text method for authentication: The account name and password are sent together.
		LOGIN	Plain text method for authentication: The account name and password are sent separately.
		CRAM-MD5	Challenge-response method authentication mechanism: Uses MD5 when a message digest is created.
Encryption		Enable	Valid
		Disable	Invalid
Protocol	Protocol used when encryption is enabled	SSL	Secure Socket Layer
		TLS	Transport Layer Security
Port number	Port number of the SMTP server	Integer	-

If you type E and press **Enter** in the e-mail notification setting menu, you can change and delete the e-mail notification setting.

The current setting is displayed in numerical order as shown in the table below. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	Enable or Disable the e-mail notification.
2	e-mail address of the system administrator
3	Host name (FQDN)
4	Comment for information to identify a customer
5	SMTP server
6	Enable or Disable SMTP authentication.
7	Account name for SMTP authentication
8	Password for SMTP authentication
9	Method for SMTP authentication
10	Enable or Disable for encryption function.
11	Method for encryption
12	Port number for a SMTP server

When you disable the e-mail notification, no prompt is ready for menu 2 to 12 described in the table above.

When you disable SMTP authentication, no prompt is ready for menu 7 to 9 described in the table above.

When you disable encryption, no prompt is ready for menu 11 described in the table above.

After the input, the new setting value is displayed. When the notification retry is scheduled, a message appears showing that the notification will be processed with the latest setting. A confirmation message is displayed. Type `Y` and press **Enter**, and the e-mail notification setting is saved. To cancel the setting, type `N` and press **Enter**, or just press **Enter**.

```
(E,R,[Q]) : E (Enter)
Notification : Enable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Address      :
([Unchange]) : dish@hitachi.com (Enter)
Host (FQDN)  :
([Unchange]) : bs2kfw.com (Enter)
Comment      :
([Unchange]) : test (Enter)
SMTP server  :
([Unchange]) : 192.168.0.76 (Enter)
Authentication : Disable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Name         :
([Unchange]) : admin (Enter)
Password     : *****
([Unchange]) :
Method       : PLAIN
(0=PLAIN,1=LOGIN,2=CRAM-MD5,[Unchange]) : 2 (Enter)
Encryption   : Disable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
Protocol     : SSL
(0=SSL,1=TLS,[Unchange]) : 1 (Enter)
Set port number to 587? (Y,[N]) : N (Enter)
Port number  :
(1-65535,[Unchange]) : 25 (Enter)

-- E-mail notification setting --
Notification : Enable
Address      : dish@hitachi.com
Host (FQDN)  : bs2kfw.com
Comment      : test
SMTP server  : 192.168.0.76
Port number  : 25

-- E-mail authentication setting --
Authentication : Enable
Name           : admin
Method         : CRAM-MD5

-- E-mail encryption setting --
Encryption   : Enable
Protocol     : TLS

WARNING : If e-mail notification is scheduled to retry, the latest setting will
be in effect.
```

```
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type R and press **Enter** in the e-mail notification setting menu, you can initialize the e-mail notification setting.

A setting value and notification retry are scheduled, and a message appears to show that the notification will be processed with the latest setting. Type Y and press **Enter**, and the e-mail notification setting is saved. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(E,R,[Q]) : R (Enter)
-- E-mail notification setting --
Notification : Disable
Address      :
Host (FQDN)  :
Comment      :
SMTP server  :
Port number  : 25

-- E-mail authentication setting --
Authentication : Disable
Name           :
Method         : PLAIN

-- E-mail encryption setting --
Encryption   : Disable
Protocol     : SSL

WARNING : If e-mail notification is scheduled to retry, the latest setting will
be in effect.

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type A in the MI command menu and press **Enter**, the e-mail address setting menu is displayed.

```
(C,E,A,M,[Q]) : A (Enter)
-- E-mail address setting menu --
    E. Edit e-mail address.
    D. Delete e-mail address.
    Q. Quit.
(E,D,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
E.	Edit e-mail address.	-
D.	Delete e-mail address.	-
Q.	Quit	Returns to the previous menu.

E-mail address setting items are described in the table below.

Item	Description of item	Value	Description of value
Nickname	Nickname of the destination to send notification	Character string in ASCII	Nickname of the address: up to 15 character string in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “ _ ”, “ . ”, “[”, “]”.
Address	E-mail address of the destination to send notification	Character string in ASCII	Up to 64 character string in ASCII Signs available are as follows: “~”, “@”, “#”, “$”, “%”, “^”, “-“, “+”, “=”, “ _ ”, “ . ”, “[”, “]”.
Attach	With or Without a log file: notification to the destination	Yes	Notification with a log file to be sent to the destination
		No	Notification without a log file to be sent to the destination

If you type E in the e-mail notification menu and press **Enter**, you can edit the e-mail address.

The current address list is displayed. Enter an address number, and the current setting is displayed in numerical order as shown in the table below. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Menu	Description
1	Address name for notification to be sent to
2	e-mail address for notification to be sent to
3	With or without a log file: notification to the address

Type Yes or No for **Attach** to decide whether the e-mail is sent with or without a log file, and the changed value is displayed. Type Y and press **Enter**, and the setting is saved. To cancel the setting change, type N and press **Enter**, or just press **Enter**.

```
(E,D,[Q]) : E (Enter)
-- E-mail address --
<Address0>
Nickname  : user0
Address   : user0@one8647.com
Attach    : Yes
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Select address (0-3,[Q=Quit]) : 0 (Enter)

Nickname  : user0
([Unchange]) : USER0 (Enter)
Address   : user0@one8647.com
([Unchange]) : (Enter)
Attach    : Yes
(0=No,1=Yes,[Unchange]) : (Enter)

-- E-mail address --
<Address0>
Nickname  : USER0
Address   : user0@one8647.com
Attach    : Yes
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Confirm? (Y,[N]) : Y (Enter)
- <Address0> Writing setting was completed.
Hit enter key. (Enter)
```

If you type D in the e-mail address menu and press **Enter**, you can delete an e-mail address.

The list including the current addresses is displayed and the prompt is ready for an address number. Enter an address number. The list without the deleted address and then a message to confirm the setting is displayed. Type Y and press **Enter**, and the setting is saved: the selected address is deleted. To cancel the setting change, type N and press **Enter**, or just press **Enter**.

```
(E,D,[Q]) : D (Enter)
-- E-mail address --
<Address0>
Nickname  : user0
Address   : user0@one8647.com
Attach    : Yes
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Select address (0-3,[Q=Quit]) : 0 (Enter)


-- E-mail address --
<Address0>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address1>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Confirm? (Y,[N]) : Y (Enter)
- <Address0> Writing setting was completed.
Hit enter key. (Enter)
```

If you type M in the MI command menu and press **Enter**, the manual e-mail notification menu is displayed.

```
(C,E,A,M,[Q]) : M (Enter)
-- Manual e-mail notification menu --
    N. Send latest log data.
    H. Select from notification history.
    Q. Quit.
(N,H,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
N.	Send latest log data.	Collects the current log data and sends them via e-mail.
H.	Select from notification history.	Selects a log from the notification history and send e-mail notification.
Q.	Quit	Returns to the previous menu.

If you type N in the manual e-mail notification menu and press **Enter**, the address list including addresses currently registered is displayed. When you specify an address, a message indicating that it takes a few minutes to put out the log to the file is displayed. A message appears to confirm the e-mail transmission. At the prompt, type Y and press **Enter**, and the log is output to the file; the e-mail will be sent to the selected address. To cancel the e-mail transmission, type N and press **Enter**, or just press **Enter**.

```
(N,H,[Q]) : N (Enter)
-- E-mail address --
<Address0>
Nickname  : USER0
Address   : user0@mail.hitachi.com
Attach    : Yes
<Address1>
Nickname  : -----------
Address   : -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Select address (0-3,A=All,[Q=Quit]) : A (Enter)


WARNING : If confirm, it will take few minutes to dump log to file.

Confirm? (Y,[N]) : Y (Enter)

- <Address0> Sending e-mail notification was completed.

Hit enter key. (Enter)
```

If you type H in the manual e-mail notification menu and press **Enter**, the notification history is displayed: the prompt is ready for a notification history number. When you specify a number from the notification history, the e-mail text during the notification and the list including the currently registered addresses are displayed. The prompt is ready for you to select an address number. When you specify an address, a message appears to confirm the e-mail transmission. Type Y and press **Enter**, and the file containing the log corresponding to the notification history is output; the e-mail will be sent to the selected address. To cancel the e-mail transmission, type N and press **Enter**, or just press **Enter**.

```
(N,H,[Q]) : H (Enter)
-- Notification history --
                                                Result
No. Timestamp           System event log        0123
--- ------------------- ----------------------- ------
  0 2009-02-26 09:30:13 6100 04 0952 0BA5FFFF CCCC
  1 2009-02-26 09:33:01 6100 04 0205 01599988 CCCC
  2 2009-02-26 11:07:19 6100 04 0952 0BA5FFFF O---
  3 2009-02-26 11:24:11 6100 04 0952 0BA5FFFF X---
  4 2009-02-26 11:45:43 6100 04 0952 0BA5FFFF CCCC
  5 2009-02-26 11:52:19 6100 04 0952 0BA5FFFF CCCC
  6 2009-02-26 11:56:29 6100 04 0952 0BA5FFFF O---
  7 2009-02-26 12:54:51 6100 04 0952 0BA5FFFF X---
  8 2009-02-26 13:06:08 6100 04 0952 0BA5FFFF X---
  9 2009-02-26 13:14:47 6100 04 0952 0BA5FFFF X---
 10 2009-02-26 13:35:10 6100 04 0952 0BA5FFFF X---
 11 2009-02-26 14:04:42 6100 04 0952 0BA5FFFF X---
 12 2009-02-26 14:09:48 6100 04 0952 0BA5FFFF X---
 13 2009-02-26 14:20:11 6100 04 0952 0BA5FFFF X---
 14 2009-02-26 14:30:37 6100 04 0952 0BA5FFFF X---
 15 2009-02-27 09:25:39 6100 04 0952 0BA5FFFF X---
 16 2009-02-27 10:10:20 6100 04 0952 0BA5FFFF X---
 17 2009-02-27 10:44:17 6100 04 0952 0BA5FFFF X---
 18 2009-02-27 10:50:34 6100 04 0952 0BA5FFFF X---
 19 2009-02-27 13:51:38 6100 04 0952 0BA5FFFF X---
 20 2009-02-27 15:15:56 6100 04 0952 0BA5FFFF X---
 21 2009-02-27 16:16:36 6100 04 0952 0BA5FFFF X---
 22 2009-02-27 20:39:17 6100 04 0952 0BA5FFFF X---
 23 2009-03-02 14:02:02 6100 04 0952 0BA5FFFF X---
 24 2009-03-02 14:13:25 6100 04 0952 0BA5FFFF X---
 25 2009-03-02 14:25:35 6100 04 0952 0BA5FFFF X---
 26 2009-03-02 14:40:51 6100 04 0952 0BA5FFFF X---
 27 2009-03-02 15:48:02 6100 04 0952 0BA5FFFF X---
 28 2009-03-02 16:46:08 6100 04 0952 0BA5FFFF X---
 29 2009-03-02 17:44:30 6100 04 0952 0BA5FFFF X---
 30 2009-03-02 18:02:52 6100 04 0952 0BA5FFFF X---
 31 2009-03-02 18:15:40 6100 04 0952 0BA5FFFF X---


Select No. (0-31,[Q=Quit]) : 31 (Enter)

The trouble occurred by the following device.

--- I/O slot expansion unit chassis ---
Part/Model Number : GV0EDW11-224N11N
Serial Number     : 5713RF0 NNNNN
Midplane ID       : 00
Chassis ID        : 5713RF0 NNNNN
```

```
+------------------------------+
| MARLOG (2009-03-02 18:15:40) |
+------------------------------+
-- CALL FACTOR INFORMATION --
Reason : 09
Impact : UU
Partition No  : -
BMC-ID        : -

-- RC INFORMATION --
EVENT         : 0000 02 5F90104A 6100 04 0952 0BA5FFFF
RC            : 10 6201 10 09520000 0BA5FFFF
RC NAME       : PSM REDUNDANCY
COMMENT       : Power Supply module#z: Operated without Redundancy (<N)
(1) Check the AC input, (2) Check the Power Supply configuration, (3) Replace
Power Supply module which is determined from previous SEL.

-- FRU INFORMATION --
+---+-------------------------------------------------------------------+
| 1 | UNIT         : OTHER              FRU MNEMONIC : BUNDEN           |
|   | PARTS NAME   :  -                 REV          :  -               |
|   | ACTION       : CHK                WEIGHT       : 50               |
|   | DRAWING NO   : MAP_CHECK          SERIAL NO    :  -               |
+---+-------------------------------------------------------------------+
| 2 | UNIT         : SYS                FRU MNEMONIC : PSALL            |
|   | PARTS NAME   :  -                 REV          :  -               |
|   | ACTION       : CHK                WEIGHT       : 50               |
|   | DRAWING NO   : MAP_CHECK          SERIAL NO    :  -               |
+---+-------------------------------------------------------------------+


-- E-mail address --
<Address0>
Nickname  : USER0
Address   : user0@mail.hitachi.com
Attach    : Yes
<Address1>
Nickname  : -----------
Address   : -----------
Attach    : No
<Address2>
Nickname  :  -----------
Address   :  -----------
Attach    : No
<Address3>
Nickname  :  -----------
Address   :  -----------
Attach    : No

Select address (0-3,A=All,[Q=Quit]) : A (Enter)

Confirm? (Y,[N]) : Y (Enter)
- <Address0> Sending e-mail notification was completed.
Hit enter key. (Enter)
```

Items of notification history are described in the table below.

Item	Description of item	Value	Description of value
No.	Notification history number	Integer	Serial number: 0 up to 31
Timestamp	When the event to trigger e-mail notification happened.	YYYY-MM-DD hh:mm:ss	YYYY: AD year; MM: month; DD: day; hh: hour; mm: minute; ss: second
System Event Log		gggg ee ssSS ee11223344	gggg: Generator ID ee: evn revision ss: Sensor type SS: Sensor number ee: Event trigger 11: Event data 1 22: Event data 2 33: Event data 3
Result	e-mail notification result	-	Not targeted
		O	Notification is successful.
		X	Notification fails.
		R	Notification fails: Wait for a retry.
		C	Just collecting logs.

❑ LDAP command

You can display and configure I/O module directory service connection. Enter `LDAP` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> LDAP (Enter)

<< LDAP - Directory service setting. >>

-- Directory service setting menu --
    D. Show directory service setting.
    C. Edit connection setting.
    S. Edit directory search setting.
    A. Edit group authentication setting.
    R. Reset directory service setting.
    Q. Quit.
(D,C,S,A,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
D.	Show directory service setting.	-
C.	Edit connection setting.	Configures required settings for Lightweight Directory Access Protocol (LDAP) server connection.
S.	Edit directory search setting.	-
A.	Edit group authentication setting.	^
R.	Reset directory service setting.	Initializes directory service settings.
Q.	Quit	Quits the LDAP command.

If you type `D` in the LDAP command menu and press **Enter**, the current directory service settings are displayed.

```
(D,C,S,A,R,[Q]) : D (Enter)

-- connection setting --
LDAP          : Enable
LDAP server 0 : 192.168.1.100
LDAP server 1 : 192.168.1.200
LDAP server 2 :
Port number   : 636
Bind DN       : bind

-- directory search setting --
Base DN            : testname
Login ID attribute : loginid_attribute
Role attribute     : role_attribute

-- group authentication setting --
Group member attribute : member_attribute
Group DN 0             : GDN0
Group DN 1             : GDN1
```

```
Group DN 2              : GDN2
Group DN 3              :
Group DN 4              :

Hit enter key. (Enter)
```

Connection setting for the LDAP server is shown in the table below.

Item	Description
LDAP	LDAP feature: Enable or Disable
LDAP server 0 to LDAP server 2	LDAP server address: fully qualified domain name (FQDN) or IP address A string consisting of up to 127 characters: both uppercase and lowercase alphanumeric characters, and signs: “-“, “.” are available.
Port number	LDAP server port number
Bind DN	Up to 256 character string in ASCII: A blank space is not available at the head and end of a string.

Directory search setting is shown in the table below.

Item	Description
Base DN	Up to 256 character string in ASCII: A blank space is not available at the head and end of a string.
Login ID attribute	Up to 64 character string: Uppercase and lower case alphabet is available for the first character of a string. Both uppercase and lowercase alphanumeric characters are available for the second or later characters of a string. A blank space is not available at the head and end of a string.
Role attribute	Up to 64 character string: Uppercase and lower case alphabet is available for the first character of a string. Both uppercase and lowercase alphanumeric characters are available for the second or later characters of a string. A blank space is not available at the head and end of a string.

Group authentication setting is shown in the table below.

Item	Description
Group member attribute	Up to 64 character string: Uppercase and lower case alphabet is available for the first character of a string. Both uppercase and lowercase alphanumeric characters are available for the second or later characters of a string. A blank space is not available at the head and end of a string.
Group DN 0 to Group DN 4	Distinguished Name (DN) for a group with permission to log in. Up to 256 character string in ASCII: A blank space is not available at the head and end of a string.

If you type C in the LDAP command menu and press **Enter**, you can edit the LDAP server connection setting.

The current LDAP server connection setting list is displayed. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Order	Description
1	Enable or Disable the LDAP feature
2	Address for LDAP server 0
3	Address for LDAP server 1
4	Address for LDAP server 2
5	Port number
6	Bind DN
7	Bind password: up to 32 character string in ASCII

When you type the bind password, the changed setting values are displayed. A confirmation message appears. To apply the LDAP server connection setting, type `Y` and press **Enter**. To cancel the setting, type `N` after the confirmation message and press **Enter**, or just press **Enter**.

```
(D,C,S,A,R,[Q]) : C (Enter)
LDAP          : Enable
(0=Disable,1=Enable,[Unchange]) : 1 (Enter)
LDAP server 0 : 192.168.1.100
([Unchange]) : 192.168.1.101 (Enter)
LDAP server 1 : 192.168.1.200
([Unchange]) : 192.168.1.201 (Enter)
LDAP server 2 :
([Unchange]) : (Enter)
Set port number to 636? (Y,[N]) : N (Enter)
Port number   : 636
(1-65535,[Unchange]) : (Enter)
Set Bind DN to Anonymous? (Y,[N]) : N (Enter)
Bind DN       : bind
([Unchange]) : (Enter)
Set Password? ([Y],N) : Y (Enter)
Password           : *****
([Unchange]) :          (Enter)
Retype password    :           (Enter)

-- connection setting --
LDAP          : Enable
LDAP server 0 : 192.168.1.101
LDAP server 1 : 192.168.1.201
LDAP server 2 :
Port number   : 636
Bind DN       : bind

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

When a bind password is configured, 5 asterisks "*****" are displayed.



When a bind password is set to be Anonymous, no setting is required for the bind password.

If you type S in the LDAP command menu and press **Enter**, you can edit the directory search setting.

The current directory search setting list is displayed. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Order	Description
1	Base DN
2	Attribute to show a login ID
3	Attribute to show a role

When you type the attribute to show a role, the changed setting values are displayed. A confirmation message appears. To apply the LDAP server setting, type Y and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(D,C,S,A,R,[Q]) : S (Enter)
Bind DN             : testname
([Unchange]) : testdn (Enter)
Login ID attribute : loginid_attribute
([Unchange]) : (Enter)
Role attribute      : role_attribute
([Unchange]) : (Enter)

-- directory search setting --
Bind DN             : testdn
Login ID attribute : loginid_attribute
Role attribute      : role_attribute

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type A in the LDAP command menu and press **Enter**, you can edit the group authentication setting.

The current group authentication setting list is displayed. To proceed to the next setting, press **Enter**, or enter a setting value and press **Enter**.

Order	Description
1	Attribute to show group members
2	DN0 for a group that is allowed to log in
3	DN1 for a group that is allowed to log in
4	DN2 for a group that is allowed to log in
5	DN3 for a group that is allowed to log in
6	DN4 for a group that is allowed to log in

When you type DN4 for a group that is allowed to log in, the changed setting values are displayed. To apply the LDAP server setting, type Y and press **Enter**. To cancel the setting, type N after the confirmation message and press Enter, or just press **Enter**.

```
(D,C,S,A,R,[Q]) : A (Enter)
Set Group member attribute to unuse? (Y,[N]) : N (Enter)
Group member attribute : member_attribute
([Unchange]) : gm_attribute (Enter)
Group DN 0             : GDN0
([Unchange]) : (Enter)
Group DN 1             : GDN1
([Unchange]) : (Enter)
Group DN 2             : GDN2
([Unchange]) : (Enter)
Group DN 3             :
([Unchange]) : (Enter)
Group DN 4             :
([Unchange]) : (Enter)

-- group authentication setting --
Group member attribute : gm_attribute
Group DN 0             : GDN0
Group DN 1             : GDN1
Group DN 2             : GDN2
Group DN 3             :
Group DN 4             :

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type C in the LDAP command menu and press **Enter**, the reset directory service setting menu is displayed.

```
(D,C,S,A,R,[Q]) : R (Enter)

--- Reset directory service setting menu ---
    C. Connection setting.
    D. Directory search setting.
    G. Group authentication setting.
    A. All LDAP setting.
    Q. Quit.
(C,D,G,A,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
C.	Connection setting.	Resets the LDAP server connection setting.
D.	Directory search setting.	Resets the directory search setting.
G.	Group authentication setting.	Resets the group authentication setting.
A.	All LDAP setting	Resets the entire directory service setting.
Q.	Quit	Returns to the previous menu.

When you type C in the reset directory service setting menu and press **Enter**, you can reset the LDAP server connection setting. To reset the setting, type Y to the confirmation message and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(C,D,G,A,[Q]) : C (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

When you type D in the reset directory service setting menu and press **Enter**, you can reset the directory search setting. To reset the setting, type Y at the confirmation message and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(C,D,G,A,[Q]) : D (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

When you type G in the reset directory service setting menu and press **Enter**, you can reset the group authentication setting. To reset the setting, type Y at the confirmation message and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(C,D,G,A,[Q]) : G (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

When you type A in the reset directory service setting menu and press **Enter**, you can reset the entire directory service setting. To reset the setting, type Y to the confirmation message and press **Enter**. To cancel the setting, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(C,D,G,A,[Q]) : A (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

Managing security

❑ CER command

You can operate public keys. Enter `CER` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> CER (Enter)

<< CER - Public key. >>

-- Public key menu --
    S. SSH host key.
    Q. Quit.
(S,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
S.	SSH host key	Operates the host key pairs of the SSH server.
Q.	Quit	Quits the CER command.

If you type `S` in the CER command menu and press **Enter**, the following menu screen is displayed.

```
(S,[Q]) : S (Enter)

-- SSH host key menu --
    G. Generate host key.
    H. Show host key information.
    B. Backup.
    R. Restore.
    Q. Quit.
(G,H,B,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
G.	Generate host key	Generates host key pairs for the SSH server
H.	Show host key information	Display information about the host key of the SSH server.
B.	Backup	Back up the host key pairs of the SSH server.
R.	Restore	Restore the host key pairs of the SSH server.
Q.	Quit	Return to the previous menu.

If you type G in the SSH host key menu and press **Enter**, you can generate a host key pair of the SSH server. To generate the host key pair, type Y and press **Enter**. To cancel the host key pair, type N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : G (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Generating host key was completed.
Hit enter key. (Enter)
```

If you type H in the SSH host key menu and press **Enter**, the host key information on the SSH server is displayed.

```
(G,H,B,R,[Q]) : H (Enter)

-- Host key information --
Key length  : 1024
Fingerprint : b6:16:6f:15:74:d6:89:95:86:76:b3:82:ba:89:be:b7

Hit enter key. (Enter)
```

Items of the host key information are described in the table below.

Item	Description of item	Value	Description of value
Key length	Host key length	Integer	Unit: bit
Fingerprint	Host key fingerprint	XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX	"XX" stands for two hexagonal figures. Alphabets from 'a' to 'f' is shown in lower case.

If you type B in the SSH host key menu and press **Enter**, you can save the host key pair of the SSH server. You are prompted to enter characters used for a file name to be generated when saving. Enter the characters for the file name, and a message appears to confirm the setting. To save the host key pair, type Y and press **Enter**. To cancel the save, type N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : B (Enter)

Input backup file name ([Quit]) : key_000000 (Enter)
Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is pub-key_000000.backup.
Hit enter key. (Enter)
```

When you have saved the host key, the host key of the SSH server is saved in the user directory in the I/O module. The host key name is displayed after saving. Press **Enter**, and the screen returns to the SSH host key menu. You can take out the host key file via FTP or SFTP.

If you type R in the SSH host key menu and press **Enter**, you can restore the host key of the SSH server. The host key list stored in the user directory is displayed. You are prompted to select a file to be restored. To restore the host key, type Y and press **Enter**. To cancel the restoring, type N and press **Enter**, or just press **Enter**.

```
(G,H,B,R,[Q]) : R (Enter)

-- Backup file list --
<File0>
pub-key_000000.backup
<File1>
pub-test.backup

Select backup file (0-1,[Q=Quit]) : 0 (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Restoring backup data was completed.
Hit enter key. (Enter)
```

❑ SEC command

You can set the network service. Enter SEC at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SEC (Enter)

<< SEC - Service setting. >>

-- Service setting menu --
    F. FTP setting.
    S. SSH setting.
    E. Telnet setting.
    H. Connection allowed network setting for all of above protocols.
    A. Show all service setting.
    Q. Quit.
(F,S,E,H,A,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
F.	FTP setting.	Sets the FTP server.
S.	SSH setting.	Sets the SSH server.
E.	Telnet setting.	Sets the Telnet server.
H.	Connection allowed network setting for all of above protocols.	Sets the range of permission for network connection to all three protocols (FTP, SSH, and Telnet).
A.	Show all service setting.	Displays the current values of all settings set by the SEC command.

Menu		Description
Q.	Quit	Quits the SEC command.

If you type F in the SEC command menu, and then press **Enter**, you can set the permissible network settings for connecting a FTP server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask. When you enter a setting, the new setting and a confirmation message appear. To save the permissible setting for the network, type Y and press **Enter**. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(F,S,E,H,A,[Q]) : F (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N]) : N (Enter)
Network address :   192.  0.  0.  0
([Unchange]) : (Enter)
Subnetmask      :   255.  0.  0.  0
([Unchange]) : (Enter)

-- FTP setting --
Allow           : Allow
Network address : 192.  0.  0.  0
Subnetmask      : 255.  0.  0.  0

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type S in the SEC command menu, and then press **Enter**, you can set the permissible network settings for connecting an SSH server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask. When you enter a setting, the new setting and a confirmation message appear. To save the permissible setting for the network, type Y and press **Enter**. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(F,S,E,H,A,[Q]) : S (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N]) : N (Enter)
Network address :   0.  0.  0.  0
([Unchange]) : (Enter)

-- SSH setting --
Allow           : Allow
Network address : ALL
Subnetmask      :  -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type E in the SEC command menu and press **Enter**, you can set the permissible network settings for connecting a Telnet server. You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask.

When you enter a setting, the new setting and a confirmation message appear. To save the permissible setting for the network, type Y and press **Enter**. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(F,S,E,H,A,[Q]) : E (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N]) : N (Enter)
Network address :   0.  0.  0.  0
([Unchange]) : (Enter)

-- Telnet setting --
Allow           : Allow
Network address : ALL
Subnetmask      :  -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type H in the SEC command menu, and then press **Enter**, you can set the same permissible network settings for connecting to all three protocol servers (FTP, SSH, and Telnet). You can choose to allow or deny all access, or allow access only from an address range defined by a particular network address and subnet mask.

When you enter a setting, the new setting and confirmation message appear. To save the permissible setting for three protocols: FTP, SSH, and Telnet, type Y and press **Enter**. To cancel the setting, type N and press **Enter**, or just press **Enter**.

```
(F,S,E,H,A,[Q]) : H (Enter)

Allow all? (Y,[N]) : N (Enter)
Deny all? (Y,[N]) : N (Enter)
Input Network address : 0.0.0.0 (Enter)

-- Allowed network setting  --
Allow           : Allow
Network address : ALL
Subnetmask      :  -----

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type A in the SEC command menu, and then press **Enter**, you can display all the current setting values set by the SEC command.

```
(F,S,E,H,A,[Q]) : A (Enter)

-- FTP setting --
Allow           : Allow
Network address : 192.  0.  0.  0
Subnetmask      : 255.  0.  0.  0

-- SSH setting --
Allow           : Allow
Network address : ALL
Subnetmask      :  -----

-- Telnet setting --
Allow           : Allow
Network address : ALL
Subnetmask      :  -----

Hit enter key. (Enter)
```

❑ SO command

You can display and set account and role information. Type SO at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> SO (Enter)

<< SO - Security setting. >>

-- Security setting menu --
    A. Account setting.
    R. Role setting.
    Q. Quit.
(A,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Account setting	Sets accounts.
R.	Role setting	Sets roles
Q.	Quit	Quits the SO command.

If you type A in the SO command menu and press **Enter**, the current account setting information is displayed.

```
(A,R,[Q]) : A (Enter)

-- Account setting --
ID Name                             Status  Role
-- -------------------------------- ------- ---------------
 0 administrator                    Enable  Administrator
 1 -----                            -----   -----
 2 -----                            -----   -----
 3 -----                            -----   -----
 4 -----                            -----   -----
 5 -----                            -----   -----
 6 -----                            -----   -----
 7 -----                            -----   -----
 8 -----                            -----   -----
 9 -----                            -----   -----
10 -----                            -----   -----
11 -----                            -----   -----
12 -----                            -----   -----
13 -----                            -----   -----
14 -----                            -----   -----
15 -----                            -----   -----
16 -----                            -----   -----
17 -----                            -----   -----
18 -----                            -----   -----
19 -----                            -----   -----
20 -----                            -----   -----
21 -----                            -----   -----
22 -----                            -----   -----
23 -----                            -----   -----

-- Account menu --
    A. Add account.
    D. Delete account.
    E. Edit account detail information.
    Q. Quit.
(A,D,E,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Add account.	-
D.	Delete account.	-
E.	Edit account detail information	-
Q.	Quit	Returns to the previous menu.

If you type A at the account menu and press **Enter**, you are prompted to enter an account name, password, account status, and role settings. When you have done so, the list of accounts is updated to include the account you intend to add, and a message appears prompting you to confirm the new account. To add the account, type Y and then press **Enter**. To cancel the operation, type N and then press **Enter**, or simply press **Enter**.

```
(A,D,E,[Q]) : A (Enter)
Enter account name ([Quit]) : iod (Enter)
Enter account password : (Password string: not displayed.)(Enter)
Select account status (0=Disable,1=Enable,[Q=Quit]) : 1 (Enter)

-- Role list --
ID Name
-- ---------------
 0 Administrator
 1 -----
 2 -----
 3 -----
 4 -----
 5 -----
 6 -----
 7 -----
 8 -----
 9 -----
10 -----
11 -----
12 -----
13 -----
14 -----
15 -----
16 -----
17 -----
18 -----
19 -----
20 -----
21 -----
22 -----
23 -----

Select role (0-23,[Q=Quit]) : 0 (Enter)

-- Account setting --
ID Name                             Status  Role
-- -------------------------------- ------- ---------------
 0 administrator                    Enable  Administrator
 1 iod                              Enable  Administrator
 2 -----                            -----   -----
 3 -----                            -----   -----
 4 -----                            -----   -----
 5 -----                            -----   -----
 6 -----                            -----   -----
 7 -----                            -----   -----
 8 -----                            -----   -----
 9 -----                            -----   -----
10 -----                            -----   -----
11 -----                            -----   -----
12 -----                            -----   -----
13 -----                            -----   -----
14 -----                            -----   -----
15 -----                            -----   -----
16 -----                            -----   -----
17 -----                            -----   -----
18 -----                            -----   -----
```

```
19 -----                              -----   -----
20 -----                              -----   -----
21 -----                              -----   -----
22 -----                              -----   -----
23 -----                              -----   -----

Confirm? (Y,[N]) : Y(Enter)
- Writing setting was completed.
Hit enter key.(Enter)
```



Account names reserved by the system cannot be registered.

Reserved account names are as follows:

bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, ntp, Recovery, ResetPassword, RecoveryCe, ResetPasswordCe, RecoveryPt, ResetPasswordPt, ceconsl.

If you type D at the account menu and press **Enter**, you are prompted to enter an account number. When you have done so, the account settings are displayed without the account you intend to delete, and a message appears prompting you to confirm deletion of the account. To delete the account, type Y and then press Enter. To cancel the operation, type N and then press **Enter**, or simply press **Enter**.

```
(A,D,E,[Q]) : D (Enter)
Select account (0-23,[Q=Quit]) : 1 (Enter)

-- Account setting --
ID Name                              Status  Role
-- --------------------------------- ------- ----------------
 0 administrator                     Enable  Administrator
 1 -----                             -----   -----
 2 -----                             -----   -----
 3 -----                             -----   -----
 4 -----                             -----   -----
 5 -----                             -----   -----
 6 -----                             -----   -----
 7 -----                             -----   -----
 8 -----                             -----   -----
 9 -----                             -----   -----
10 -----                             -----   -----
11 -----                             -----   -----
12 -----                             -----   -----
13 -----                             -----   -----
14 -----                             -----   -----
15 -----                             -----   -----
16 -----                             -----   -----
17 -----                             -----   -----
18 -----                             -----   -----
19 -----                             -----   -----
20 -----                             -----   -----
21 -----                             -----   -----
```

```
22 -----                              -----   -----
23 -----                              -----   -----

Confirm? (Y,[N]) : Y(Enter)
- Writing setting was completed.
Hit enter key.(Enter)
```

If you type E at the account menu and press **Enter** key, you are prompted to enter an account number. When you enter an account number, detailed information about the account is displayed, and the menu from which you can perform detailed account settings appears.

```
(A,D,E,[Q]) : E (Enter)

Select account (0-23,[Q=Quit]) : 1 (Enter)

-- Specified account setting --
ID                     : 1
Name                   : user0
Status                 : Enable
Role                   : Administrator
Key                    : Not installed
Inactivity timer(min) : 10
Prompt                 : Chassis ID and Slot Number

-- Account detail setting menu --
    N. Edit account name.
    S. Edit account status.
    R. Edit account role.
    P. Edit account password.
    K. Edit account public key.
    I. Edit account inactivity timer.
    M. Edit account prompt.
    Q. Quit.
(N,S,R,P,K,I,M,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
N.	Edit account name.	
S.	Edit account status.	
R.	Edit account role.	
P.	Edit account password.	
K.	Edit account public key.	
I.	Edit account inactivity timer.	Edit the inactivity timer settings for the account.
M.	Edit account prompt.	Edit the prompt setting for the account.
Q.	Quit	Returns to the previous menu.

If you type N at the account detail setting menu and press **Enter**, you can change the account name. You cannot change the account name if a user is logged in to the account.



Account names reserved by the system cannot be registered.

Reserved account names are as follows:

bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, ntp, Recovery, ResetPassword, RecoveryCe, ResetPasswordCe, RecoveryPt, ResetPasswordPt, ceconsl.

If you type S at the account detail setting menu and press **Enter**, you can change the account status. You cannot change the account status if a user is logged in to the account.

If you type R at the account detail setting menu and press **Enter**, you can change the role assigned to the account. You cannot change the role if a user is logged in to the account.

If you type P at the account detail setting menu and press **Enter**, you can change the password to the account. When changing the password of the currently logged-in account, you must enter the old and new passwords. If your account with permission for editing accounts attempts to edit an account other then yourself, type the new password.

If you type K at the account detail setting menu and press **Enter**, you can set public keys for the account password.

```
(N,S,R,P,K,I,M,[Q]) : K (Enter)

-- Public key status --
Key                  : Not installed

-- Account public key menu --
    I. Install public key.
    U. Uninstall public key.
    Q. Quit.
(I,U,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
I.	Install public key.	
U.	Uninstall public key.	
Q.	Quit	Returns to the previous menu.

If you type I and press **Enter**, you can install the public key for the account. The file list stored in the user directory is displayed. You are prompted to select a file from the list. When you specify the number of a file, the public key algorithm, key length, and fingerprint are displayed. To start installing the public key, type Y and press **Enter**. To cancel the installation, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(I,U,[Q]) : I(Enter)

-- File list --
<File0>
id_dsa.pub
<File1>
id_rsa.pub

Select file (0-1,[Q=Quit]) : 0(Enter)
-- Public key information --
<Public key0>
Algorithm   : DSA
Key length  : 1024
Fingerprint : 1f:90:2d:5e:16:a5:72:90:d8:b0:93:54:48:2b:2f:4e


Confirm? (Y,[N]) : Y (Enter)
- Installing public key was completed.
Hit enter key. (Enter)
```



- Only OpenSSH public key file is supported.
- Up to five public keys can be installed in one account.
- RSA (the first-described public-key cryptosystem) and digital signature algorithm (DSA) are supported. A public key with SSH version 1 is not supported.



- Check the fingerprint of the public key and confirm that the fingerprint is identical to the fingerprint displayed before installation.
- Back up the public key beforehand by yourself.

If you type U in the account public key menu and press **Enter**, you can uninstall the account public key. A message to confirm the uninstallation appears. To start uninstalling the public key, type Y and press **Enter**. To cancel the installation, type N after the confirmation message and press **Enter**, or just press **Enter**.

```
(I,U,[Q]) : U (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Uninstalling public key was completed.
Hit enter key. (Enter)
```

If you type `I` at the account detail setting menu and press **Enter**, you can change the inactivity timer setting for the account. Specify a value from 0 to 1440 (minutes). To disable the inactivity timer, specify 0. The new setting takes effect from the next time the user logs in to the account.

If you type `M` at the account detail setting menu and press **Enter**, you can change the account prompt settings. You can select from two formats: "chassis ID (I/O module slot number) IOEU>" (chassis ID and slot number)"; or "IOEU> (fixed)".

If you type `R` and press **Enter** at the prompt for the SO command menu, you can display the current role settings.

```
(A,R,[Q]) : R (Enter)

-- Role setting --
No. Name            Net Chassis Account
--- --------------- --- ------- -------
  0 Administrator   X   X       X
  1 -----           -   -       -
  2 -----           -   -       -
  3 -----           -   -       -
  4 -----           -   -       -
  5 -----           -   -       -
  6 -----           -   -       -
  7 -----           -   -       -
  8 -----           -   -       -
  9 -----           -   -       -
 10 -----           -   -       -
 11 -----           -   -       -
 12 -----           -   -       -
 13 -----           -   -       -
 14 -----           -   -       -
 15 -----           -   -       -
 16 -----           -   -       -
 17 -----           -   -       -
 18 -----           -   -       -
 19 -----           -   -       -
 20 -----           -   -       -
 21 -----           -   -       -
 22 -----           -   -       -
 23 -----           -   -       -

-- Role menu --
    A. Add role.
    D. Delete role.
    E. Edit role.
    Q. Quit.
(A,D,E,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
A.	Add role.	
D.	Delete role.	
E.	Edit role.	
Q.	Quit	Returns to the previous menu.

If you type A at the role menu and press **Enter**, the system awaits input of settings, in the order shown in the table below. To proceed to the next setting, press **Enter**, or enter a value and then press **Enter**. If you press the **Enter** at prompt for a role name, the screen returns to the role menu.

Order	Item
1	Role name
2	Network permission
3	Server chassis permission
4	Account permission

When you type a new account permission value, the list of role settings is updated to reflect the change, and a confirmation message appears. To apply the new settings, type Y and then press **Enter**. To cancel the operation, type **N** and then press **Enter**, or simply press Enter.

```
 (A,D,E,[Q]) : A (Enter)
Enter role name ([Quit]) : admin (Enter)
Add network authority? (Y,[N]) : Y (Enter)
Add chassis authority? (Y,[N]) : Y (Enter)
Add account authority? (Y,[N]) : Y (Enter)

-- Role setting --
No. Name            Net Chassis Account
--- --------------- --- ------- -------
  0 Administrator   X   X       X
  1 admin           X   X       X
  2 -----           -   -       -
  3 -----           -   -       -
  4 -----           -   -       -
  5 -----           -   -       -
  6 -----           -   -       -
  7 -----           -   -       -
  8 -----           -   -       -
  9 -----           -   -       -
 10 -----           -   -       -
 11 -----           -   -       -
 12 -----           -   -       -
 13 -----           -   -       -
 14 -----           -   -       -
 15 -----           -   -       -
 16 -----           -   -       -
 17 -----           -   -       -
 18 -----           -   -       -
 19 -----           -   -       -
 20 -----           -   -       -
 21 -----           -   -       -
 22 -----           -   -       -
 23 -----           -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type D at the role menu and press **Enter**, you are prompted to enter the number of the role to delete. When you have done so, the list of role settings is updated, and a message appears prompting you to confirm the deletion. To delete the role, type Y and then press **Enter**. To cancel the operation, enter N and then press **Enter**, or press **Enter**.

```
(A,D,E,[Q]) : D (Enter)
(0-23,[Q=Quit]) : 1 (Enter)

-- Role setting --
No. Name            Net Chassis Account
--- --------------- --- ------- -------
  0 Administrator   X   X       X
  1 -----           -   -       -
  2 -----           -   -       -
  3 -----           -   -       -
  4 -----           -   -       -
  5 -----           -   -       -
  6 -----           -   -       -
  7 -----           -   -       -
  8 -----           -   -       -
  9 -----           -   -       -
 10 -----           -   -       -
 11 -----           -   -       -
 12 -----           -   -       -
 13 -----           -   -       -
 14 -----           -   -       -
 15 -----           -   -       -
 16 -----           -   -       -
 17 -----           -   -       -
 18 -----           -   -       -
 19 -----           -   -       -
 20 -----           -   -       -
 21 -----           -   -       -
 22 -----           -   -       -
 23 -----           -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

If you type E at the role menu and press **Enter**, you are prompted to enter the number of the role to edit. When you have done so the current settings are displayed in the order shown in the table below, and the system awaits your input. To proceed to the next setting, press **Enter**, or enter a value and then press **Enter**.

Order	Item
1	Role name
2	Network permission
3	Server chassis permission
4	Account permission

If you enter a setting value of account permission, the role settings are updated to reflect the changes, and a confirmation message appears. To apply the changes, type Y and then press **Enter**. To cancel the operation, type N and then press **Enter**, or press **Enter**.

```
(A,D,E,[Q]) : E (Enter)
(0-23,[Q=Quit]) : 0 (Enter)
Role name      : Administrator
([Unchange]) : (Enter)
Network authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Chassis authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)
Account authority : Allow
(0=Deny,1=Allow,[Unchange]) : (Enter)

-- Role setting --
No. Name            Net Chassis Account
--- --------------- --- ------- -------
  0 Administrator   X   X       X
  1 -----           -   -       -
  2 -----           -   -       -
  3 -----           -   -       -
  4 -----           -   -       -
  5 -----           -   -       -
  6 -----           -   -       -
  7 -----           -   -       -
  8 -----           -   -       -
  9 -----           -   -       -
 10 -----           -   -       -
 11 -----           -   -       -
 12 -----           -   -       -
 13 -----           -   -       -
 14 -----           -   -       -
 15 -----           -   -       -
 16 -----           -   -       -
 17 -----           -   -       -
 18 -----           -   -       -
 19 -----           -   -       -
 20 -----           -   -       -
 21 -----           -   -       -
 22 -----           -   -       -
 23 -----           -   -       -

Confirm? (Y,[N]) : Y (Enter)
- Writing setting was completed.
Hit enter key. (Enter)
```

Backing up and restoring settings

❑ DC command

This command restores settings to factory defaults. Type DC at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> DC(Enter)

<< DC - Restore factory setting. >>

-- Restore setting menu --
    R. Restore factory setting.
    Q. Quit.
(R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
R.	Restore factory setting.	Restores the settings of the I/O module to the factory defaults.
Q.	Quit	Quits the DC command.

If you type R at the DC command menu and press **Enter**, a warning message appears indicating that if you proceed to reset the I/O module, the I/O module will restart to terminate the current session. To restore the I/O module to the defaults and restart, type Y at the confirmation prompt and press **Enter**. To cancel the operation, at the confirmation prompt, type N and then press **Enter**, or press **Enter**.

```
(R,[Q]) : R (Enter)

WARNING : If confirm, this connect is lost.

Confirm? (Y,[N]) : Y (Enter)
- <I/O module0> Restarting
(Disconnected.)
```

❑ UBR command

This command backs up, and restores configuration information. Type `UBR` at the prompt and press **Enter**.

```
5713RF0 NNNNN(0)IOEU> UBR(Enter)

<< UBR - Backup and restore setting. >>

-- Backup and restore setting menu --
    B. Backup.
    R. Restore.
    Q. Quit.
(B,R,[Q]) :
```

Select a menu item from the following list to execute it.

Menu		Description
B.	Backup	Backs up I/O module configuration information.
R.	Restore.	Restores I/O module configuration information.
Q.	Quit	Quits the UBR command.

If you type `B` at the UBR command menu and press the **Enter**, you are prompted to enter a character string used for the file name. Enter a file name, and a message appears to save the configuration information. To back up the configuration, type `Y` at the confirmation prompt and press **Enter**. To cancel the operation, type `N` at the confirmation prompt and press the **Enter**, or press **Enter**.

```
(B,R,[Q]) : B (Enter)

Input backup file name ([Q=Quit]) : conf (Enter)

Confirm? (Y,[N]) : Y (Enter)
- Creating backup file was completed.
- Backup file name is io-conf.backup.
Hit enter key. (Enter)
```

When the file finishes storing the configuration information, the file name is displayed and the prompt is ready. Press **Enter**, and the screen returns to the I/O module configuration menu. That file is stored in the user directory in the I/O module. You can take out the file via FTP or SFTP. The account name and password for connection via FTP or SFTP are the same as when you log in the system console.

If you type R at the Backup and restore setting menu and press **Enter**, a list appears of files containing the I/O module configuration that is stored in the user directory. You are prompted to select a file to be restored. When you enter a number to specify a file, a warning message indicating that the I/O module restarts after restoring the configuration is displayed. To restore the configuration, type Y at the confirmation prompt and press **Enter**. To cancel the operation, type N at the confirmation prompt and press **Enter**, or press **Enter**.

```
(B,R,[Q]) : R (Enter)

-- Backup file list --
<File0>
io-conf.backup

Select backup file (0,[Q=Quit]) : 0 (Enter)

WARNING : If confirm, this connect is lost.

Confirm? (Y,[N]) : Y (Enter)
- <I/O module0> Restarting
(Disconnected.)
```

Correspondence between commands and permissions

The following table shows the association between commands and the permissions required for command execution

	Command	Permission		
		Account	Chassis	Network
1	BSM		Yes	
2	CER	Yes		
3	CI		Yes	
4	DC		Yes	
5	DEL		Yes	
6	DF		Yes	
7	DH		Yes	
8	DL		Yes	
9	EX	None required		
10	FAN	None required		
11	FW		Yes	
12	HE	None required *1		
13	ILC			Yes
14	IOC (displays I/O module status.)	None required		
15	IOC (I/O module operation.)		Yes	
16	LC			Yes

	Command	Permission		
		Account	Chassis	Network
17	LDAP	Yes		
18	LFT			Yes
19	LM		Yes	
20	LS		Yes	
21	MI		Yes	
22	MLC			Yes
23	PES		Yes	
24	PS		Yes	
25	PSM (displays power supply module status.)	None required		
26	PSM (displays AC input power supply module voltage settings.)		Yes	
27	SCO (sets inactivity timer)	None required		
28	SCO (sets transfer rate of serial ports.)		Yes	
29	SD		Yes	
30	SDN		Yes	
31	SEC			Yes
32	SNM		Yes	
33	SO (edits your account)	None required *2		
34	SO (edits accounts other than yours.)	Yes		
35	UBR		Yes	
36	WHO (display a session)	None required		
37	WHO (forcibly terminates a session)	Yes		
38	WWN		Yes	
39	XD			Yes

Yes: Permission required for executing the command.

None required: Executable without any permission.

None required*1: Executable without any permission. Only the executable commands are displayed.

None required*2: Executable without any permission. Available operations include changing passwords, inactivity timer values, and prompt types; installing/uninstalling public keys.

Alert log message

(1) Overview of alert logs

Alert logs are notified directly to ServerConductor/Blade Server Manager (hereafter SC/BSM) by the I/O slot expansion unit and stored.

Alert logs can be viewed from the SC/ BSM console or “DL command” for the I/O slot expansion unit.

(2) Format of alert log messages (viewed from the I/O slot expansion unit console)

```
Timestamp           ID    Level   Message
------------------- ----  ------- --------------------
YYYY-MM-DD hh:mm:ss XXXX  XXXXXXX ********************
YYYY-MM-DD hh:mm:ss XXXX  XXXXXXX ********************
```

Timestamp

The date and time when the log message was generated, in the format YYYY (year) – MM (month) – DD (day) hh (hour) – mm (minutes) – ss (seconds)

ID

The message ID

Level

The level of the message: Info (information message), WARNING (warning message), or FAIL (error message)

Message

A message is shown. “%s” in a message stands for characters.

(3) List of messages

ID	Level	Message
Description		
1800	Info	On module <%s1>, the temperature <%s2> exceeded the normal level.
Meaning: The temperature at the part shown in %s2 of the module shown in %s1 is beyond the normal value but does not reach the warning level. Action: Nothing required. If this message frequently appears, check if something prevents the unit from cooling down		
1801	WARNING	On module <%s1>, the temperature <%s2> exceeded the warning level.
Meaning: The temperature at the part shown in %s2 of the module shown in %s1 is beyond the warning level. Action: Although the device can keep running, the high temperature can cause a fault. Thus, check if something prevents it from cooling down, such as failure in air conditioners or in fan modules of the unit, and inlet ports covered with dust.		
1802	FAIL	On module <%s1>, the temperature <%s2> rose too far above tolerable levels.
Meaning: The temperature at the part shown in %s2 of the module shown in %s1 is exceedingly high. Action: The module with a high temperature may stop working to protect hardware. Consult your reseller or maintenance personnel. Check if something prevents it from cooling down, such as failure in air conditioners or in fan modules of the unit, and inlet ports covered with dust.		
1803	WARNING	On module <%s1>, the temperature <%s2> fell below the warning level.
Meaning: The temperature at the part shown in %s2 of the module shown in %s1 is below the warning level. Action: Although the device can keep working, check if the temperature is proper where the device is installed.		
1805	Info	On module <%s1>, the temperature <%s2> has been restored to a tolerable level.
Meaning: The temperature at the part shown in %s2 of the module shown in %s1 is back to the normal level. Action: This shows just information. Nothing required.		
1810	WARNING	On module <%s1>, the voltage <%s2> exceeded the warning level.
Meaning: The voltage at the part shown in %s2 of the module shown in %s1 is beyond the warning level. Action: Although the device can keep working, the high voltage can cause a fault. Consult your reseller or maintenance personnel.		
1811	FAIL	On module <%s1>, the voltage <%s2> rose too far above tolerable levels.
Meaning: The voltage at the part shown in %s2 of the module shown in %s1 is exceedingly high. Action: The module with high voltage may stop working to protect hardware. Consult your reseller or maintenance personnel.		
1813	WARNING	On module <%s1>, the voltage <%s2> fell below the warning level.
Meaning: The voltage at the part shown in %s2 of the module shown in %s1 is below the warning level. Action: Although the device can keep working, the low voltage can cause a fault. Consult your reseller or maintenance personnel.		
1814	FAIL	On module <%s1>, the voltage <%s2> fell too far below tolerable

ID	Level	Message
Description		
		levels.
Meaning: The voltage at the part shown in %s2 of the module shown in %s1 is exceedingly low. Action: The module with extremely low voltage may stop working to protect the hardware. Consult your reseller or maintenance personnel.		
1815	Info	On module <%s1>, the voltage <%s2> has been restored to a normal level.
Meaning: The voltage at the part shown in %s2 of the module shown in %s1 is back to the normal level. Action: This shows just information. Nothing required.		
1821	FAIL	On module <%s1>, the current <%s2> rose too far above tolerable levels.
Meaning: The current at the part shown in %s2 of the module shown in %s1 is exceedingly high. Action: The module with extremely high current may stop working to protect hardware. Consult your reseller or maintenance personnel.		
1839	FAIL	On module <%s1>, a 2-bit error occurred in the memory.
Meaning: An unrecoverable error occurs in the memory of the module shown in %s. Action: Consult your reseller or maintenance personnel.		
183A	WARNING	On module <%s1>, the number of 1-bit error corrections exceeded the limit.
Meaning: Although a recoverable error, occurred in the memory of the module shown in %s, was fixed, the number of those errors that occurred is beyond the limit. Action: Although the device can keep working, this can change to an unrecoverable fault. Consult your reseller or maintenance personnel.		
183F	FAIL	On module <%s1>, an abnormal event occurred.
Meaning: Failure occurs in the module shown in %s. Action: Consult your reseller or maintenance personnel.		
1840	WARNING	On module <%s1>, an abnormal event occurred.
Meaning: Failure occurs in the module shown in %s. Action: Consult your reseller or maintenance personnel.		
1841	Info	On module <%s1>, the abnormal event was corrected.
Meaning: The module shown in %s is restored from failure Action: Nothing required.		
1842	WARNING	On module <%s1>, an AC input error occurred.
Meaning: An error occurs in the AC input to the module shown in %s. Action: Check if something wrong is in the power supply to devices, such as the breaker and socket outlet. If nothing wrong is detected, consult your reseller or maintenance personnel.		
1843	Info	On module <%s1>, the AC input error has been corrected.
Meaning: The AC input to the module shown in %s is restored. Action: Nothing required.		
1844	WARNING	On module <%s1>, the fan rotation speed is abnormally high or low.
Meaning: Failure occurs in the fan module shown in %s. Action: Consult your reseller or maintenance personnel.		
1845	Info	On module <%s1>, the fan rotation speed has been restored a normal level.
Meaning: The Fan module shown in %s is restored. Action: Nothing required.		

ID	Level	Message
Description		
1847	WARNING	On module <%s1>, an access error to <%s2> occurred.
Meaning: A communication error, shown in %s2 of the module shown in %s1, occurs. Action: When the message ID: 1848 is registered after this message to show the recovery due to the temporary error, nothing is required. If the message is not registered, consult your reseller or maintenance personnel.		
1890	Info	Module <%s1> was installed.
Meaning: A module shown in %s is inserted. Action: Nothing is required.		
1891	Info	Module <%s1> was removed.
Meaning: A module shown in %s is removed. Action: Nothing is required.		
1892	Info	Module <%s1> restored redundancy.
Meaning: A module shown in %s has redundancy. Action: Nothing is required.		
1893	WARNING	Module <%s1> lacks redundancy.
Meaning: A module shown in %s has no longer redundancy. Action: Although the device can keep working, redundancy is lost. Consult your reseller or maintenance personnel.		
1894	FAIL	The total number of modules <%s1> is insufficient.
Meaning: The number of modules shown in %s is not enough. If the number of power supply modules or fan module is not insufficient, the system halts. Action: Check if the module shown in %s is properly inserted. If they are properly inserted, consult your reseller or maintenance personnel.		
1899	FAIL	A system configuration error was found.
Meaning: A system configuration is improper. Action: If you changed the configuration before the message appeared, check if something is wrong in the configuration. If not, consult your reseller or maintenance personnel.		
18A0	WARNING	LAN port <%s1> lacks redundancy.
Meaning: The LAN port shown in %s1 has no longer redundancy. Action: Check if the LAN port is properly connected. Redundancy for LAN ports can be temporarily lost, but no problem when the message ID: 18A1 is registered after this message.		
18A1	Info	LAN port <%s1> redundancy was restored.
Meaning: Redundancy for the LAN port shown in %s is restored. Action: This shows just information. Nothing required.		
18A2	Info	LAN port <%s1> has switched to another port.
Meaning: The LAN port shown in %s has switched to another port when redundancy for the LAN port is enabled. Action: This message shows redundancy secured, but if the message ID: 18A0 appears with this message, check the LAN port connection.		
18A3	Info	LAN port <%s1> has recovered from an error.
Meaning: The switched LAN port as shown in the message ID: 18A2 has switched back to the former state. Action: This shows just information. Nothing required.		
18A8	WARNING	Sending out an e-mail report message failed. It will be retried.
Meaning: E-mail notification failed to be sent and will be retried. Action: Check if communication between the mail server and I/O slot expansion unit is available, and e-mail notification settings. If any problem in the settings, correct them.		
18A9	WARNING	Sending out an e-mail report message failed.

ID	Level	Message
Description		
Meaning: E-mail notification fails. Action: Check if communication between the mail server and I/O slot expansion unit is available, and e-mail notification settings. If any problems are in the settings, correct them.		
18AA	Info	Collecting error data for an e-mail report message failed.
Meaning: Data collection for e-mail notification fails. Data attached to e-mail may be partly lost. Action: Nothing is required. If this message frequently appears, however, consult your reseller or maintenance personnel.		
18AB	Info	Sending out an e-mail report message succeeded.
Meaning: The retried e-mail notification is successfully sent. Action: Nothing required.		
18AE	Info	The time limit for transmitting and receiving an alert has been exceeded.
Meaning: Sending and receiving alert messages to SC/BSM failed, retried, failed again, and the retry time exceeded. Alert notifications tried have not reached BSM. Action: In the device notification log window of SC/BSM console services, calculate time by subtracting the retry duration time from the time when the message ID: 18AE was generated. Check alerts notified for between the answer of the subtraction and the time when the message ID: 18E0 was generated, and work with the problem according to those alerts. You can locate the duration time of alert sending retry in Retry duration, which is displayed by executing the BSM command from the I/O expansion unit console.		
18B0	Info	The time setting was updated.
Meaning: I/O module time setting is updated. Action: Nothing required.		
18B1	WARNING	Connecting to the NTP server was failed.
Meaning: Connection to the NTP server fails. Action: Check if communication between the I/O slot expansion unit and NTP server is available. Also check the NTP server setting of the I/O slot expansion unit.		
18B2	Info	Connecting to the NTP server was restored.
Meaning: Connection between the I/O slot expansion unit and NTP server is restored. Action: Check if the I/O slot expansion unit time is correct.		
18C0	Info	On module <%s1>, An event was logged.
Meaning: An event is registered in the module shown in %s. Action: Nothing required.		
18D4	Info	On module <%s1>, F/W update was started.
Meaning: Firmware of the module shown in %s starts updating. This message may be displayed several times for maintenance work. Action: Just wait until the firmware has completely updated without connecting to or operating the I/o slot expansion unit.		
18D5	Info	On module <%s1>, F/W update was completed.
Meaning: Firmware of the module shown in %s has completely updated. This message may be displayed several times for maintenance work. Action: Nothing required.		
18DC	Info	On module <%s1>, maintenance mode was set.
Meaning: Maintenance work begins in the module shown in %s. This message may be displayed several times for maintenance work. Action: The module is under maintenance work. Do not connect to or operate that module.		
18DD	Info	On module <%s1>, maintenance mode was cancelled.

ID	Level	Message
Description		
Meaning: Maintenance work to the module shown in %s has finished. This message may be displayed several times for maintenance work. Action: Nothing required.		
18E0	Info	A connection request alert is sent.
Meaning: The I/O slot expansion unit requests connection to SC/BSM Action: Nothing required.		
18E2	Info	The IP address is changed.
Meaning: The IP address of the I/O module is changed. Action] Nothing required.		
18E3	Info	System information update alert is sent.
Meaning: An alert to notify the system update is sent to SC/BSM from the I/O slot expansion unit. Action: Nothing required.		
18E4	Info	Module information update alert is sent.
Meaning: An alert to notify information update on modules installed in the I/O slot expansion unit is sent to SC/BSM. Action: Nothing required.		
18E5	Info	Module information update alert is sent (error/degradation).
Meaning: An alert to notify information update on modules installed in the I/O slot expansion unit is sent to SC/BSM. Action: Nothing required.		

12

Logical partitioning manager

This chapter describes LPAR manager (logical partitioning manager). LPAR manager, hereinafter, stands for Hitachi Compute Blade logical partitioning feature.

LPAR manager overview 996
LPAR manager boot 1042
Basic operation of LPAR manager 1057
Guest OS operation 1090
Backup of LPAR manager 1145
LPAR manager screen operations 1147
Quit LPAR manager 1289
LPAR manager functions 1292
HCSM 1361
HVM Navigator 1362
LP model updating 1363
LPAR manager version upgrade 1363
Migration between basic environment and LPAR manager environment 1364
LPAR manager Security 1366
Cautions 1371
LPAR manager setting item 1419
Port numbers used by LPAR manager 1428
System configuration 1429
LPAR manager boot messages 1440
LPAR manager on-screen messages 1442
LPAR manager system logs screen messages 1453
HCSM (Hitachi Compute Systems Manager) Alert Message 1480
Software license 1482

LPAR manager overview

LPAR manager product specifications

Server blades supported by LPAR manager

Server blade[*1]		Supported by the following LPAR manager firmware versions
Standard server blade	X55A1	57-1X or later
	X55A2	58-1X or later
	X55R3/X55S3	59-0X or later
	X55R4	59-51 or later
High-performance server blade	X57A1	78-1X or later
	X57A2	78-7X or later

*1: Internal disks, HDD and SSD, cannot be used.

Peripheral components interconnect (PCI) devices supported by LPAR manager

PCI device			Supported (Not supported) by the following LPAR manager firmware versions
Serial port		COM1	Virtual: 57-1X or later /78-1X or later
Universal Serial Bus (USB) device		CD/DVD drive	Exclusive-shared: 57-1X or later /78-1X or later
		Floppy disk (FD) drive	Exclusive-shared: 57-1X or later /78-1X or later
		USB memory	Exclusive-shared: 58-6X or later /78-6X or later
		keyboard	Not supported
		mouse	Not supported
Remote console		CD/DVD drive	Exclusive-shared: 58-2X or later /78-2X or later
		FD drive	Exclusive-shared: 58-2X or later /78-2X or later
		keyboard	Exclusive-shared: 57-1X or later /78-1X or later
		mouse	Exclusive-shared: 57-1X or later /78-1X or later
NIC	Onboard	Intel 1 Gbps Ethernet x 2	Dedicated/Shared: 57-1X or later /78-1X or later
		Broadcom 1 Gbps Ethernet x 2[*1]	Dedicated/Shared: 59-0X or later
	Expansion card	Intel 1 Gbps Ethernet x 4	Dedicated/Shared: 57-1X or later /78-1X or later

PCI device			Supported (Not supported) by the following LPAR manager firmware versions
NIC		Emulex 10 Gbps Ethernet x 2 *2 *3 *9 *10 *11	Dedicated/Shared: 59-01 or later /79-01 or later
		Emulex 10 Gbps Ethernet x 4 *2 *3*9 *10 *11	Dedicated/Shared: 59-01 or later /79-01 or later
		Emulex 10 Gbps CNA x 2 *2 *3 *4 *9 *10 *11	Dedicated/Shared: 59-4X or later /79-4X or later
		Emulex 10 Gbps CNA x 4 *2 *3 *4 *9 *10 *11	Dedicated/Shared: 59-4X or later /79-4X or later
	PCI card	Intel 1 Gbps Ethernet x 2	Dedicated/Shared: 57-1X or later /78-1X or later
		Intel 1 Gbps Ethernet x 4	Dedicated/Shared: 57-2X or later /78-1X or later
		Intel 10 Gbps Ethernet x 2 *5* 6 *7	Dedicated: 58-4X or later /78-4X or later
		Emulex 10 Gbps CNA x 2 *2 *3 *4 *9 *10 *11	Dedicated/Shared: 59-4X or later /79-4X or later
FC	Expansion card	Hitachi 4 Gbps Fibre-channel x 2 *7	Dedicated/Shared: 57-2X or later Not supported by 78-1X or later
		Hitachi 8 Gbps Fibre-channel x 2	Dedicated/Shared: 58-1X or later /78-1X or later
		Hitachi 8 Gbps Fibre-channel x 4	Dedicated/Shared: 58-1X or later /78-1X or later
	PCI card	Hitachi 4 Gbps Fibre-channel x 2	Dedicated/Shared: 57-1X or later Not supported by 78-1X or later
		Hitachi 8 Gbps Fibre-channel x 1	Dedicated/Shared: 58-1X or later /78-1X or later
		Hitachi 8 Gbps Fibre-channel x 2	Dedicated/Shared: 58-1X or later /78-1X or later
Flash drive	PCI card	Fusion-io 365 GB PCIe Flash drive *2	Dedicated: 59-21 or later /79-21 or later
		Fusion-io 785 GB PCIe Flash drive *2	Dedicated: 59-21 or later /79-21 or later
		Fusion-io 1.2 TB PCIe Flash drive *2	Dedicated: 59-21 or later /79-21 or later

*1: This item is supported by standard server blades: X55R3/X55S3/X55R4.

*2: This item is supported by standard server blades: X55R3/X55S3/X55R4 and high-performance server blade: X57A2. Multi-channel, iSCSI, and FCoE are not supported.

*3: Multi Channel Mode is not supported. Disable Multi Channel Support using Emulex PXESelect Utility. See the Hitachi Compute Blade Emulex Adapter User's Guide for Hardware for details. With Logical partitioning Enabled, however, you cannot change the setting. If you need to change the setting, change Logical partitioning to Disabled.

*4 iSCSI mode and Fibre Channel over Ethernet (FCoE) mode are not supported. Make sure to select NIC for Personality with Emulex Preboot eXecution Environment (PXE) Select Utility. See the *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware* for details. With Logical partitioning Enabled, however, you cannot change the setting. If you need to change the setting, change Logical partitioning to Disabled.

*5: This item is not supported by standard server blade X55A1 model.

*6: The following table shows the maximum number of cards, the number of ports, to be installed.

Processor (number of cores)	Maximum number of cards: number of ports to be installed
3 or less	Not available
4 to 5	1 (2 ports)
6 to 11	2 (4 ports)
12 to 23	4 (8 ports)
24 or more	8 (16 ports)

*7: It is recommendable to use jumbo frame. If not, transmission might slow down.

*8: This item is supported only with the management module firmware version A0110 or later and BMC firmware version 3.52 or later.

*9: An LPAR, to which a shared NIC and virtual NIC are assigned, is recognized as 1 Gb LAN (Intel PRO/1000 or Intel 82576) by the guest OS.

*10: For an LPAR, to which a shared NIC and virtual NIC are assigned, total throughput is about 3 Gbps per LPAR manager.

*11: SR-IOV is supported by 59-7X/79-7X or later.

*12: Supported by standard server blade models: X55R3/X55S3 and high-performance server blade model: X57A2.

Guest OSs and Functions supported by LPAR manager on a standard server blade

Item		Supported (Not supported) by the following LPAR manager firmware versions
Guest OS * X55A1 blade	Red Hat Enterprise Linux 5.3	57-1X or later
	Red Hat Enterprise Linux 5.4	57-3X or later
	Red Hat Enterprise Linux 5.6	58-6X or later
	Red Hat Enterprise Linux 5.7	59-01 or later
	Red Hat Enterprise Linux 5.9	59-51 or later
	Red Hat Enterprise Linux 6.1	58-8X or later
	Red Hat Enterprise Linux 6.2	59-0X or later
	Red Hat Enterprise Linux 6.4	59-4X or later
	Red Hat Enterprise Linux 6.5	59-5X or later
	Red Hat Enterprise Linux 6.6	59-72 or later
	Windows Server 2003 R2 SP2	57-1X or later
	Windows Server 2008 *1	57-1X or later
	Windows Server 2008 SP2	57-1X or later
	Windows Server 2008 R2	57-3X or later
	Windows Server 2008 R2 SP1	58-6X or later
	Windows Server 2012	Not supported
	Windows Server 2012 R2	Not supported
Guest OS *X55A2 blade	Red Hat Enterprise Linux 5.3	Not supported
	Red Hat Enterprise Linux 5.4	58-1X or later
	Red Hat Enterprise Linux 5.6	58-6X or later
	Red Hat Enterprise Linux 5.7	59-01 or later
	Red Hat Enterprise Linux 5.9	59-51 or later
	Red Hat Enterprise Linux 6.1	58-8X or later
	Red Hat Enterprise Linux 6.2	59-0X or later
	Red Hat Enterprise Linux 6.4	59-4X or later
	Red Hat Enterprise Linux 6.6	59-72 or later

Item		Supported (Not supported) by the following LPAR manager firmware versions
Guest OS *X55A2 blade	Red Hat Enterprise Linux 6.5	59-5X or later
	Windows Server 2003 R2 SP2	58-1X or later
	Windows Server 2008	Not supported
	Windows Server 2008 SP2	58-1X or later r
	Windows Server 2008 R2	58-1X or later
	Windows Server 2008 R2 SP1	58-6X or later
	Windows Server 2012	Not supported
	Windows Server 2012 R2	Not supported
Guest OS *X55R3/X55 S3 blade	Red Hat Enterprise Linux 5.3	Not supported
	Red Hat Enterprise Linux 5.4	Not supported
	Red Hat Enterprise Linux 5.6	Not supported
	Red Hat Enterprise Linux 5.7	59-01 or later
	Red Hat Enterprise Linux 5.9	59-51 or later
	Red Hat Enterprise Linux 6.1	Not supported
	Red Hat Enterprise Linux 6.2	59-0X or later
	Red Hat Enterprise Linux 6.4	59-4X or later
	Red Hat Enterprise Linux 6.5	59-5X or later
	Red Hat Enterprise Linux 6.6	59-72 or later
	Windows Server 2003 R2 SP2	Not supported
	Windows Server 2008	Not supported
	Windows Server 2008 SP2	59-0X or later
	Windows Server 2008 R2	Not supported
	Windows Server 2008 R2 SP1	59-0X or later
	Windows Server 2012	59-2X or later
	Windows Server 2012 R2	Not supported
Guest OS *X55R4 blade	Red Hat Enterprise Linux 5.3	Not supported
	Red Hat Enterprise Linux 5.4	Not supported
	Red Hat Enterprise Linux 5.6	Not supported
	Red Hat Enterprise Linux 5.7	Not supported
	Red Hat Enterprise Linux 5.9	Not supported
	Red Hat Enterprise Linux 6.1	Not supported
	Red Hat Enterprise Linux 6.2	Not supported
	Red Hat Enterprise Linux 6.4	59-51 or later
	Red Hat Enterprise Linux 6.5	59-5X or later
	Red Hat Enterprise Linux 6.6	59-72 or later
	Windows Server 2003 R2 SP2	Not supported
	Windows Server 2008	Not supported
	Windows Server 2008 SP2	Not supported
	Windows Server 2008 R2	Not supported
	Windows Server 2008 R2 SP1	59-51 or later
	Windows Server 2012	59-51 or later
	Windows Server 2012 R2	59-52 or later
LPAR manager operating mode *2 *11	LPAR manager standard mode	57-1X or later
	LPAR manager expansion mode	58-7X or later
Max number of LPARs	Definable LPARs per LPAR manager	16: 57-1X or later 30: 58-8X or later
	Activatable LPARs per LPAR manager *8	

Item				Supported (Not supported) by the following LPAR manager firmware versions
		LPAR manager standard mode		16: 57-1X or later
		LPAR manager expansion mode		16: 58-7X or later 30: 58-8X or later
Processor	Minimum division unit			Core: 57-1X or later Thread: 57-3X or later
	Max number of logical processors per LPAR			16: 57-1X or later 32: 59-5X or later
	Dedicated processor			
		Allocation of physical processor numbers		57-1X or later
	Shared processor			
		Allocation of physical processor numbers		58-3X or later
		Service ratio		57-1X or later
		Idle detection		57-1X or later
		Capping		57-1X or later
	Processor group			58-3X or later
		Max number of definable groups per LPAR manager[*8]		
			LPAR manager standard mode	16: 58-3X or later
			LPAR manager expansion mode	16: 58-7X or later 30: 58-8X or later
	Hyper threading			57-3X or later
	Dynamic change in scheduling mode			58-4X or later
Memory	Minimum division unit			256 MB: 57-1X or later
	Maximum amount available for assignment per LPAR[*3]			
		LPAR manager standard mode		142.75 GB: 57-1X or later 190.75 GB: 58-1X or later 510.75 GB: 59-0X or later 766.75 GB: 59-21 or later
		LPAR manager expansion mode		190.5 GB: 58-7X or later 510.5 GB: 59-0X or later 766.5 GB: 59-21 or later
	Memory used by LPAR manager			
		LPAR manager standard mode		1.25 GB
		LPAR manager expansion mode		1.5 GB
	Non-NUMA			57-1X or later
	NUMA			59-2X or later
NIC	Multi-channel			Not supported
	iSCSI			Not supported
	FCoE			Not supported
	SR-IOV[*12]			59-7X or later
	Dedicated NIC			
		Minimum division unit		Controller: 57-1X or later
		Maximum number of dedicated NIC ports to be assigned per LPAR		Identical to the number of physical NIC ports: 57-1X or later

Item				Supported (Not supported) by the following LPAR manager firmware versions
NIC		Virtual local area network (VLAN)		
		WOL (Wake On LAN)		Not supported
		Teaming		57-1X or later
		TCP segmentation offload (TSO)		57-1X or later
		Promiscuous mode		Not supported
		Inter-LPAR packet filtering		Not supported
		PXE boot		Not supported
	Shared NIC			
		Minimum division unit		
			LPAR manager standard mode	Controller: 57-1X or later
			LPAR manager expansion mode	Port: 58-7X or later
		Maximum number of physical LAN controllers to be assigned per LPAR manager		6: 57-1X or later 8: 59-0X or later
		Maximum number of physical ports to be assigned per LPAR manager		12: 57-1X or later 16: 59-0X or later
		Maximum number of shared NICs to be assigned per LPAR		
			LPAR manager standard mode	8: 57-1X or later
			LPAR manager expansion mode	16: 58-7X or later
		Assigning a NIC port duplicately to an LPAR		
			LPAR manager standard mode	Not supported
			LPAR manager expansion mode	58-7X or later
		Assigning a NIC port respectively to an LPAR		
			LPAR manager standard mode	Not supported
			LPAR manager expansion mode	58-7X or later
		VLAN		57-1X or later
		WOL[*4 *5]		57-1X or later
		Teaming		57-1X or later
		TSO		57-1X or later
		Promiscuous mode		57-1X or later
		Inter-LPAR packet filtering		57-3X or later
		PXE boot[*4]		57-1X or later
	Virtual Function (VF) NIC			
		Minimum division unit		Port for 59-7X or later
		Maximum number of physical LAN controllers to be assigned per LPAR manager		2 for 59-7X or later
		Maximum number of physical ports to be assigned per LPAR manager		4 for 59-7X or later
		Maximum number of physical ports per port		16 for 59-7X or later
		Maximum number of VF NICs to be assigned per LPAR		16 for 59-7X or later
		Assigning a NIC port duplicately to an LPAR		59-7X or later
		Assigning a NIC port respectively to an LPAR		59-7X or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
NIC		VLAN	59-7X or later
		WOL	Not supported
		Teaming	59-7X or later
		Transmission bandwidth control	59-7X or later
		TSO	59-7X or later
		Promiscuous mode	Not supported
		Inter-LPAR transmission packet filter	59-7X or later
		PXE boot	Not supported
	Virtual NIC		
		Maximum number of network segments per LPAR manager	4: 57-1X or later
		Maximum number of virtual NIC to be assigned per LPAR	
		LPAR manager standard mode	8: 57-1X or later
		LPAR manager expansion mode	16: 58-7X or later
		VLAN	57-1X or later
		WOL	Not supported
		Teaming	57-1X or later
		TSO	57-1X or later
		Promiscuous mode	57-1X or later
		Inter-LPAR packet filtering	Not supported
		PXE boot	Not supported
FC	Dedicated FC (Fiber channel)		
		Minimum division unit	Controller: 57-1X or later
		Maximum number of dedicated FC ports per port	Identical to that of physical FC ports: 57-1X or later
		Storage area network (SAN) boot	57-1X or later
		FC switch configuration for supporting N-Port ID Virtualization (NPIV)	57-1X or later
		SAN storage direct-coupling configuration	58-1X or later
	Shared FC		
		Minimum division unit	port: 57-1X or later
		Maximum number of shared FC ports to be shared per port (4 Gbps fibre channel)	7: 57-1X or later 8: 57-2X or later 15: (58-8X or later)
		Maximum number of shared FC ports to be shared per port (8 Gbps fibre channel)	15: (58-1X or later)
		SAN boot	57-1X or later
		FC switch configuration for supporting NPIV	57-1X or later
		SAN storage direct-coupling configuration	58-1X or later
USB	USB1.1		57-1X or later
	USB2.0		58-2X or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
User interface	GUI		
		Hitachi Compute Systems Manager (HCSM)*9 *10	79-42 or later
		Hitachi Virtualization Manager (HVM) Navigator	58-6x or later
		ServerConductor (SC)/Blade Server Manager (BSM) *13	57-1X or later
User interface	CUI		
		LPAR manager screen	57-1X or later
		Guest screen	57-1X or later
	Command line interface (CLI)		
		HvmSh	57-1X or later
System operation	Hitachi Compute Systems Manager (HCSM)*9*10		79-42 or later*
	HVM Navigator		
		LPAR settings	58-6x or later
		Monitoring	57-1X or later
		Configuration viewer	58-1X or later
		LPAR migration	58-1x or later
		Firmware update	58-1x or later
		Solutions	58-6x or later
	SC/BSM*13		57-1X or later
	ServerConductor (SC)/Deployment Manager (DPM) *14		57-1X or later
	Performance Management (PFM)*13		57-3X or later
	IT Resource Management – Manager (ITRM) *6 *13		58-7X or later
	Remote console*7		57-1X or later
	Virtual communication port (COM) console		
		Maximum number of simultaneous connections	16: 57-1X or later
	Logical video graphics array (VGA) snapshot		57-1X or later
	LPAR manager system time		
		Local time	57-1X or later
		Coordinated Universal Time (UTC)	59-41 or higher
	Network Time Protocol (NTP)		
		LPAR time	57-1X or later
		LPAR manager system time	58-7X or later
	Power saving		
		Power capping	57-1X or later
		C3	57-1X or later
		C6	58-12 or later

Item		Supported (Not supported) by the following LPAR manager firmware versions
	Available virtual NIC system number at the maximum	128: 57-1X or later 1024: 59-21 or later
High reliability	N+1 cold standby	57-1X or later
	Uninterruptible power supply (UPS)	57-1X or later
Maintenance	Guest memory dump collection command	57-1X or later
	LPAR manager dump collection command	57-1X or later
	LPAR manager firmware version up	57-1X or later
	PCI Express (PCIe) error isolation	58-7X or later
Virtualization software	VMwre	Not supported
	Hyper-V	Not supported

Guest OSs and Functions supported by LPAR manager on a high-performance server blade

Item		Supported (Not supported) by the following LPAR manager firmware versions
Guest OS * X57A1 blade	Red Hat Enterprise Linux 5.3	Not supported
	Red Hat Enterprise Linux 5.4	78-1X or later
	Red Hat Enterprise Linux 5.6	78-6X or later
	Red Hat Enterprise Linux 5.7	79-01 or later
	Red Hat Enterprise Linux 6.1	78-8X or later
	Red Hat Enterprise Linux 5.9	79-51 or later
	Red Hat Enterprise Linux 6.2	78-8X or later
	Red Hat Enterprise Linux 6.4	79-4X or later
	Red Hat Enterprise Linux 6.5	79-5X or later
	Red Hat Enterprise Linux 6.6	79-72 or later
	Windows Server 2003 R2 SP2	78-1X or later
	Windows Server 2008	Not supported
	Windows Server 2008 SP2	78-1X or later
	Windows Server 2008 R2	78-1X or later
	Windows Server 2008 R2 SP1	78-7X or later
	Windows Server 2012	Not supported
	Windows Server 2012 R2	Not supported
Guest OS *X57A2 blade	Red Hat Enterprise Linux 5.3	Not supported
	Red Hat Enterprise Linux 5.4	Not supported
	Red Hat Enterprise Linux 5.6	78-7X or later
	Red Hat Enterprise Linux 5.7	79-01 or later
	Red Hat Enterprise Linux 6.1	78-8X or later
	Red Hat Enterprise Linux 5.9	79-51 or later
	Red Hat Enterprise Linux 6.2	79-0X or later
	Red Hat Enterprise Linux 6.4	79-4X or later
	Red Hat Enterprise Linux 6.5	79-5X or later
	Red Hat Enterprise Linux 6.6	79-72 or later
	Windows Server 2003 R2 SP2	Not supported
	Windows Server 2008	Not supported
	Windows Server 2008 SP2	78-7X or later
	Windows Server 2008 R2	78-7X or later
	Windows Server 2008 R2 SP1	78-7X or later
	Windows Server 2012	79-2X or later
	Windows Server 2012 R2	79-52 or later
LPAR manager operating mode *2	LPAR manager standard mode	78-1X or later
	LPAR manager expansion mode	78-7X or later
SMP configuration *X57A1 blade	2-blade SMP (Symmetric multiprocessing)	78-1X or later
	4-blade SMP	78-3X or later
SMP configuration *X57A2 blade	2-blade SMP	78-7X or later
	4-blade SMP	78-73 or later
Max number of LPARs	Maximum number of definable LPARs per LPAR manager	
	1 blade	16: 78-1X or later 60: 78-4X or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
Max number of LPARs		2-blade SMP	16: 78-1X or later 60: 78-4X or later
		4-blade SMP	16: 78-3X or later 60: 78-4X or later
	Maximum number of activatable LPARs per LPAR manager [*8]		
		1 blade	16 : 78-1X or later 60 : 78-6X or later
		2-blade SMP	16 : 78-1X or later 60 : 78-6X or later
		4-blade SMP	16 : 78-3X or later 60 : 78-6X or later
Processor	Minimum division unit		Thread: 78-1X or later
	Maximum number of logical processors per LPAR manager		
		1 blade	32: 78-1X or later 64: 78-3X or later
		2-blade SMP	32: 78-1X or later 64: 78-3X or later
		4-blade SMP	64: 78-3X or later
	Dedicated processor		
		Assignment of physical processor numbers	78-1X or later
	Shared processor		
		Assignment of physical processor numbers	78-3X or later
		Service ratio	78-1X or later
		Idle detection	78-1X or later
		Capping	78-1X or later
	Processor group		78-3X or later
		Max number of definable groups per LPAR manager [*8]	
		1 blade	16 : 78-3X or later 60 : 78-6X or later
		2-blade SMP	16 : 78-3X or later 60 : 78-6X or later
		4-blade SMP	16 : 78-3X or later 60 : 78-6X or later
	Hyper threading		78-1X or later
	Dynamic change in scheduling mode		78-4X or later
Memory	Minimum division unit		256 MB: 78-1X or later
	Maximum amount available for assignment per LPAR [*3]		
		1 blade	254.5 GB: 78-1X or later 382.5 GB: 78-7X or later 766.5 GB: 79-21 or later
		2-blade SMP	510.5 GB: 78-1X or later 766.5 GB: 78-7X or later 1534.5 GB: 79-21 or later
		4-blade SMP	1022.5 GB: 78-3X or later 1534.5 GB: 78-7X or later 3070.5 GB: 79-21 or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
	Memory used by LPAR manager		1.5 GB
Memory	Non-NUMA		78-1X or later
	NUMA		79-2X or later
NIC	Multi-channel		Not supported
	iSCSI		Not supported
	FCoE		Not supported
	SR-IOV[*12]		79-7X or later
	Dedicated NIC		
		Minimum division unit	Controller: 78-1X or later
		Maximum number of dedicated NIC ports to be assigned per LPAR	Identical to the number of physical NIC ports: 78-1X or later
		VLAN	78-1X or later
		WOL	Not supported
		Teaming	78-1X or later
		TSO	78-1X or later
		Promiscuous mode	Not supported
		Inter-LPAR packet filtering	Not supported
		PXE boot	Not supported
	Shared NIC		
		Minimum division unit	
		LPAR manager standard mode	Controller: 78-1X or later
		LPAR manager expansion mode	Port: 78-7X or later
		Maximum number of physical LAN controllers to be assigned per LPAR manager	6: 78-1X or later 8: 79-0X or later
		Maximum number of physical ports to be assigned per LPAR manager	12: 78-1X or later 16: 79-0X or later
		Maximum number of shared NICs to be assigned per LPAR	
		LPAR manager standard mode	8: 78-1X or later
		LPAR manager expansion mode	16: 78-7X or later
		Assigning a NIC port duplicate to an LPAR	
		LPAR manager standard mode	Not supported
		LPAR manager expansion mode	78-7X or later
		Assigning a NIC port respectively to an LPAR	
		LPAR manager standard mode	Not supported
		LPAR manager expansion mode	78-7X or later
		VLAN	78-1X or later
		WOL[*4 *5]	78-1X or later
		Teaming	78-1X or later
		TSO	78-1X or later
		Promiscuous mode	78-1X or later
		Inter-LPAR packet filtering	78-1X or later
		PXE boot[*4]	78-1X or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
NIC	Virtual Function (VF) NIC		
		Minimum division unit	Port for 79-7X or later
		Maximum number of physical LAN controllers to be assigned per LPAR manager	2 for 79-7X or later
		Maximum number of physical ports to be assigned per LPAR manager	4 for 79-7X or later
		Maximum number of shared physical ports per port	16 for 79-7X or later
		Maximum number of VF NICs to be assigned per LPAR	16 for 79-7X or later
		Assigning a NIC port duplicately to an LPAR	79-7X or later
		Assigning a NIC port respectively to an LPAR	79-7X or later
		VLAN	79-7X or later
		WOL	Not supported
		Teaming	79-7X or later
		Transmission bandwidth control	79-7X or later
		TSO	79-7X or later
		Promiscuous mode	Not supported
		Inter-LPAR transmission packet filter	79-7X or later
		PXE boot	Not supported
	Virtual NIC		
		Maximum number of network segments per LPAR manager	4: 78-1X or later
		Maximum number of virtual NIC to be assigned per LPAR	
		LPAR manager standard mode	8: 78-1X or later
		LPAR manager expansion mode	16: 78-7X or later
		VLAN	78-1X or later
		WOL	Not supported
		Teaming	78-1X or later
		TSO	78-1X or later
		Promiscuous mode	78-1X or later
		Inter-LPAR packet filtering	Not supported
		PXE boot	Not supported
FC	Dedicated FC		
		Minimum division unit	Controller: 78-1X or later
		Maximum number of dedicated FC ports per port	Identical to that of physical FC ports: 78-1X or later
		SAN boot	78-1X or later
		FC switch configuration for supporting NPIV	78-1X or later
		SAN storage direct-coupling configuration	78-1X or later

Item			Supported (Not supported) by the following LPAR manager firmware versions
FC	Shared FC		
		Minimum division unit	port: 78-1X or later
		Maximum number of FC ports per port (4 Gbps Fibre-channel)	Not supported
		Maximum number of shared FC ports per port (8 Gbps Fibre-channel)	15: (78-1X or later)
		SAN boot	78-1X or later
		FC switch configuration for supporting NPIV	78-1X or later
		SAN storage direct-coupling configuration	78-1X or later
USB	USB1.1		78-1X or later
	USB2.0		78-2X or later
User interface	GUI		
		HCSM[*9] [*10]	79-42 or later
		HVM Navigator	78-6x or later
		SC/BSM[*13]	78-1X or later
	Character-based user interface (CUI)		
		LPAR manager screen	78-1X or later
		Guest screen	78-1X or later
	CLI		
		HvmSh	78-1X or later
System operation	HCSM[*9] [*10]		79-42 or later
	HVM Navigator		
		LPAR settings	78-6x or later
		Monitoring	78-1X or later
		Configuration viewer	78-1X or later
		LPAR migration	78-1x or later
		Firmware update	78-1x or later
		Solutions	78-6x or later
	SC/BSM[*13]		78-1X or later
	SC/DPM[*14]		78-1X or later
	Performance Management (PFM) [*13]		78-1X or later
	IT Resource Management – Manager (ITRM)[*6] [*13]		78-7X or later
	Remote console[*7]		78-1X or later
	Virtual COM console		
		Maximum number of simultaneous connections	16: 78-1X or later
	LPAR manager system time		
		Local time	78-1X or later

Item		Supported (Not supported) by the following LPAR manager firmware versions
	UTC	79-41 or higher
	Logical VGA snapshot	78-1X or later
	NTP	
	LPAR time	78-1X or later
	LPAR manager system time	78-7X or later
	Power saving	
	Power capping	78-1X or later
	C3	78-1X or later
	C6	78-1X or later
	Available virtual NIC system number at the maximum	128: 78-1X or later 1024: 79-21 or later
High reliability	N+1 cold standby	78-1X or later
	UPS	78-1X or later
Maintenance	Guest memory dump collection command	78-1X or later
	LPAR manager dump collection command	78-1X or later
	LPAR manager firmware version up	78-1X or later
	PCIe error isolation	78-7X or later
Virtualization software	VMwre	Not supported
	Hyper-V	Not supported

*1: Windows Server 2008 Datacenter Edition is not supported.
*2: The item is supported by LPAR manager firmware version 58-71/78-71 or later.
*3: Max memory amount available for assignment = (Max physical memory) – (Memory amount used by LPAR manager)
*4: This item is available only with the onboard LAN controller on a server blade, not with an expansion card or PCI card.
*5: This item is available only through WOL by SC/BSM, SC/DPM, or HCSM.
With LPAR manager firmware version 58-80/78-80 or earlier, use shared NIC #0 to #7.
*6: This item is supported only with 58-72X/78-73 or later.
*7: DVD remote FD function of the remote console is not available with LPAR manager firmware version 58-1X/78-1X or earlier.
*8: Up to 2 for Essential models.
*9 This item is supported by standard server blade: X55R3/X55S3/X55R4 models and high-performance server blade: X57A2 model.
*10 HCSM 7.5.1 or later is supported.
*11 Standard server blade: X55R4 model supports LPAR manager expansion mode only.
*12 See Notes on using SR-IOV for details.
*13 VF NIC view and settings are not supported.
*14 VF NIC does not support this item.

Architecture overview

LPAR manager logically partitions the physical resources of one server blade to create multiple server environments, each of which can operate independently. Each of the server environments constructed in this way from partitioned physical resources is called an LPAR (Logical PARtition). It is possible to run a different operating system on each LPAR simultaneously. The operating system on an LPAR is called a guest OS.

Each LPAR operates as a completely independent and isolated server environment, and the guest OS running on a LPAR is not affected by other LPARs.

The mode in which a server blade is logically partitioned to allow the operation of multiple LPARs is called the LP mode.

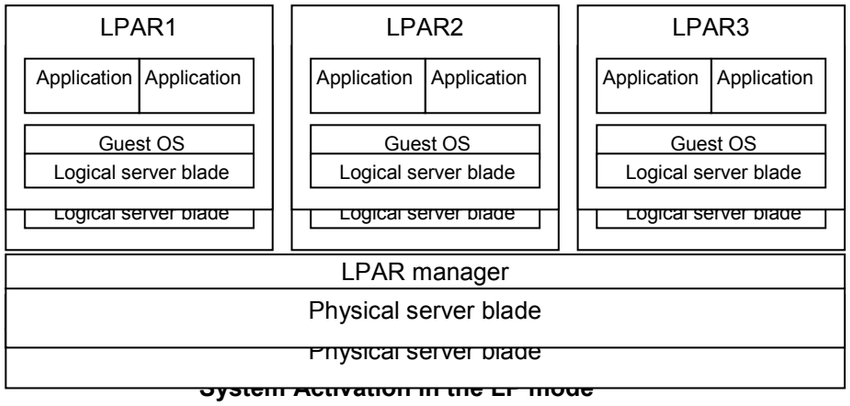
The conventional mode of operating a server blade without partitioning is called the Basic mode.

Unless explicitly specified, the terms *physical* and *logical* are used in this chapter as defined in the table below.

Term: Physical and Logical

Term	Description
Physical	Indicates the resources that actually exist in the system. "Physical" is sometimes omitted, except where this would cause confusion.
Logical	Indicates the logical resources that exist on a LPAR or for software on LPARs. Thus, there might or might not exist an actual resource for each logical resource.

An image when the system is booted in the LP mode is as follows:



System Activation in the LP mode

In addition, in this chapter:

- Symbols embraced by square brackets [ ] indicate keys on the keyboard.
- If two keys are joined by a "+", such as "[A] + [B]", it means the two keys are to be pressed together.

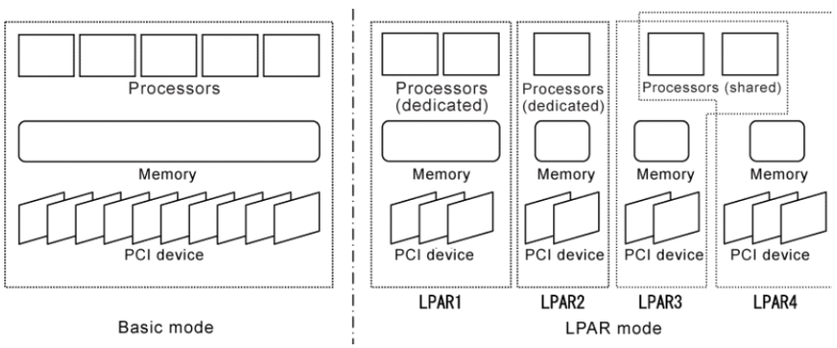
Logical partitioning

❑ Dedicated resources and shared resources

Although the LP mode makes it possible to logically partition the hardware resources of a server blade, the method of logical partitioning varies depending on the hardware resource.
Some types of logical partitioning are shown in the table below.

Type of logical partitioning

Term		Description	Typical hardware resources
Dedicated		Either LPAR manager or the particular LPAR to which a hardware resource has been allocated can exclusively use the hardware resource. It cannot be used by LPARs to which it has not been allocated. To switch the LPAR that can use resources, make sure to shut down the LPAR once to change the configuration definition.	Processors Memories PCI devices
Shared	Exclusive-shared	Either LPAR manager or the particular LPAR to which a hardware resource has been allocated can exclusively use the hardware resource, but the LPAR using the resource can be switched dynamically.	Serial ports USB devices
	Time-shared	Either LPAR manager or particular LPARs to which a hardware resource has been allocated timeshares the resource. LPAR manager keeps switching LPARs that can use a device at very short time intervals.	Processors PCI devices



Logical partitioning of hardware resources

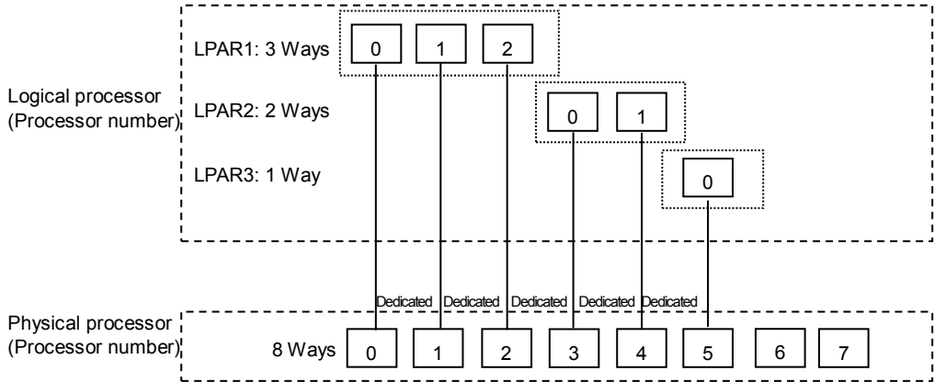
❑ Logical partitioning of processors

The method of logically splitting the physical processor is referred to as the scheduling mode. This mode allows you to specify dedicated or shared. They are called the dedicated mode and shared mode. Different features of each mode are shown in the table below.

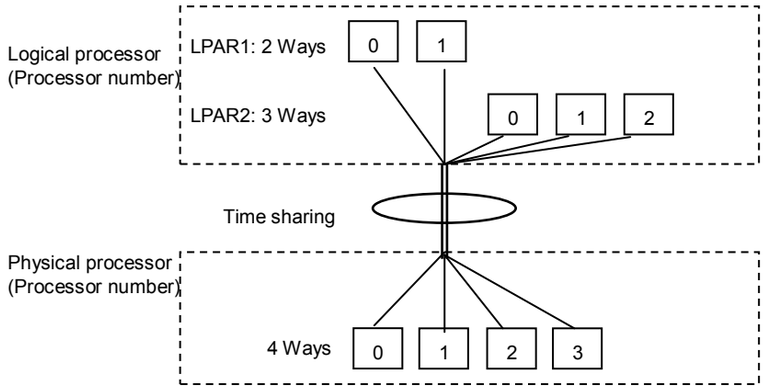
Processor scheduling mode

Mode	Explanation
Dedicated mode	The logical processor on a LPAR exclusively uses the corresponding physical processor. For each LPAR, it is possible to specify the number of logical processors assigned. (However, it is not possible to specify more than the number of physical processors available.) It is also possible to specify the physical processor number that a logical processor uses. If the physical processor number is not specified, LPAR manager determines to assign the number to be used when the LPAR is activated. Since there is no overhead for switching the physical processors between the logical processors, the LPAR performs faster.
Shared mode	Physical processors are time-shared among the logical processors defined in the LPAR for which the shared mode is specified. The number of logical processors to be used in the shared mode can be set for each LPAR. (It is possible to specify more than the number of physical processors available, but operations might slow down to an extreme level.). The utilization rate of the physical processors can be set dynamically for each LPAR, allowing flexible use of physical processor resources.

The scheduling mode for processors is set per LPAR, so it is not possible to specify a different scheduling mode for each individual logical processor within a single LPAR.



Dedicated mode (example)



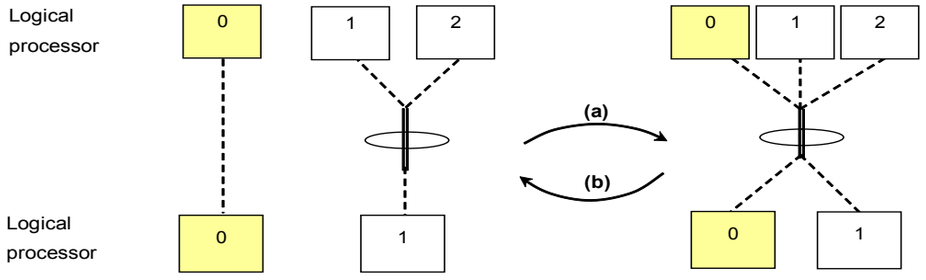
Shared mode (example)

(1) Dynamic change in scheduling mode

With LPAR manager firmware version 58-3X/78-3X or later, LPAR modes can be dynamically changed between dedicated and shared modes without deactivating LPARs.

(a) A logical processor in dedicated mode can be dynamically changed to the one in shared mode.

(b) A logical processor in shared mode can be dynamically changed to the one in dedicated mode.



(2) Service ratio

To the LPARs in the Shared Processor Mode, you can set the relative processor resource allocation rate (called Service Ratio), which represents the ratio of the time period in which the LPAR actually runs on the physical processors (called Service Time). The Service Ratio can be specified from 1 to 999.

LPAR manager partitions the performance of the physical processor used in shared mode in 1 percent units. LPAR manager calculates the relative allocation rate of the service time with 10-millisecond time-slice accuracy, which equals 1% of a unit processor time (1 second).

The service ratio can be available only for LPARs in shared mode and not for LPARs in dedicated mode to which the service ratio cannot be specified.

The relation between Service Ratio and allocation rate is shown in the following examples:

Example 1

This example shows the allocation rates of LPAR1 (Service Ratio=100, the number of the logical processors=2) and LPAR2 (Service Ratio=100, the number of the logical processors=2) when the number of the physical processor can be used by the shared mode LPARs is 3.

	Service Ratio	Actual resource allocation rate	Actual allocation of the time period of physical processor (millisecond) per unit time (1 sec)
LPAR1 (# of logical processors=2)	100	50%	1,500
LPAR2 (# of logical processors=2)	100	50%	1,500
Total	200	100%	3,000 (*1)

*1:Total available time period in an entire system in a unit time (1 sec) = 3,000 milliseconds
("1 sec = 1000 milliseconds" X "Number of physical processors = 3" = 3000 milliseconds)

Example 2

This example shows the allocation rates of LPAR1 (Service Ratio=100, the number of the logical processors=2), LPAR2 (Service Ratio=100, the number of the logical processors=2) and LPAR3 (Service Ratio=100, the number of the logical processors=3), when the number of the physical processor can be used by the shared mode LPARs is 3, and LPAR3 is added while LPAR1 and LPAR2 are running.

	Service Ratio	Actual resource allocation rate	Actual allocation of the time period of physical processor (millisecond) per unit time (1 sec)
LPAR1 (# of logical processors=2)	100	50%	1,500
LPAR2 (# of logical processors=2)	100	50%	1,500
Total	200	100%	3,000

Add LPAR

LPAR1 (# of logical processors=2)	100	33.33…%	1,000
LPAR2 (# of logical processors=2)	100	33.33…%	1,000
LPAR2 (# of logical processors=3)	100	33.33…%	1,000
Total	300	100%	3,000

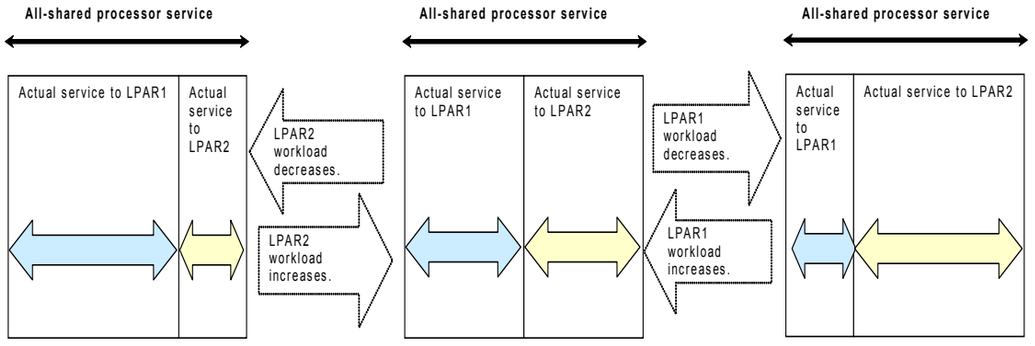
LPAR manager modifies the allocation rate from the shared LPAR definition when it meets the following condition:

- If the allocation rate for the calculation per logical processor is less than 1 %, the service rate is compensated so that the time in which a single logical processor uses the physical processor becomes 1% (10 milliseconds) of the unit processor time (1 second).
- If the number of logical processors allocated to a single LPAR does not satisfy the assigned allocation rate, the allocation rate is compensated to the one that is based on the number of logical processors.

(3) Idle detection

A shared mode LPAR, which is enabling its idle detection and not using much CPU compared to the allocated rate, can give its processor time to another shared mode LPAR requiring it. The busy shared mode LPAR that takes over the processor time can use more processor-time than the allocation rate. As a result, the system can use CPUs time more efficiently.

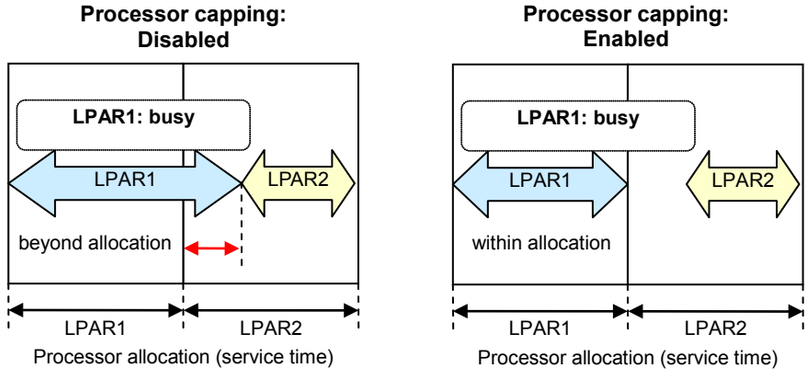
Although this function does not work to a dedicated mode LPAR, make sure to set the default value: Y for correct performance.



(4) Processor capping

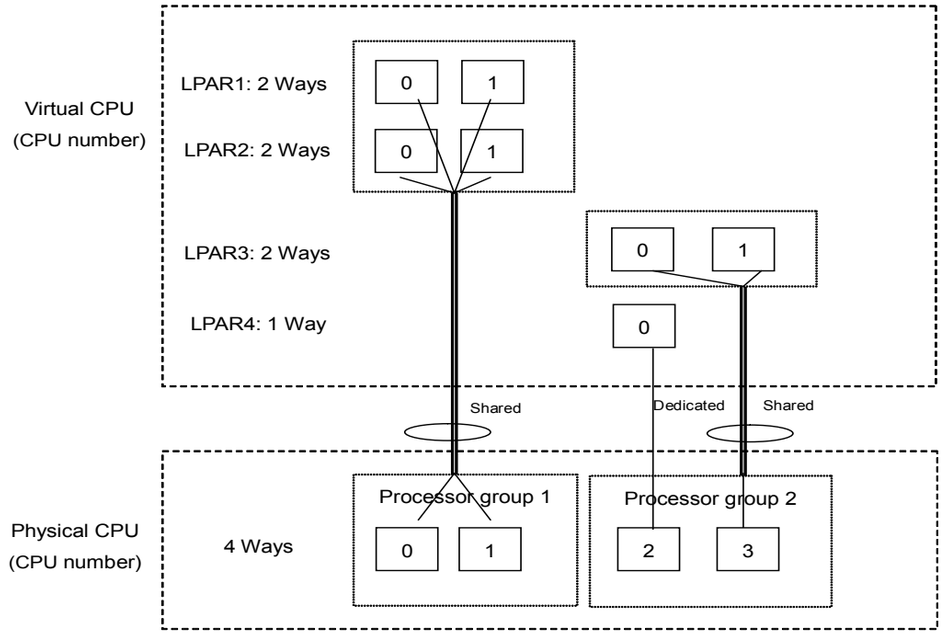
With the processor capping function on, the shared mode LPAR does not take on the unused (idle) capacity of other LPARs even if the LPAR requires more performance than its allocation rate (busy status). Therefore, the LPAR's processor-time never uses more processor-time than the allocation rate, even if it is busy. However, because the LPAR manager allocation rate control allows a tolerance of 1% for each unit of processor-time, a shared mode LPAR is allocated a maximum processor-time that is 1% greater than the total service time of the physical processors assigned to it, and might exceed the allocation rate.

The processor capping can be available only for LPARs in shared mode and not for LPARs in dedicated mode, to which the service ratio cannot be specified.



(5) Processor group

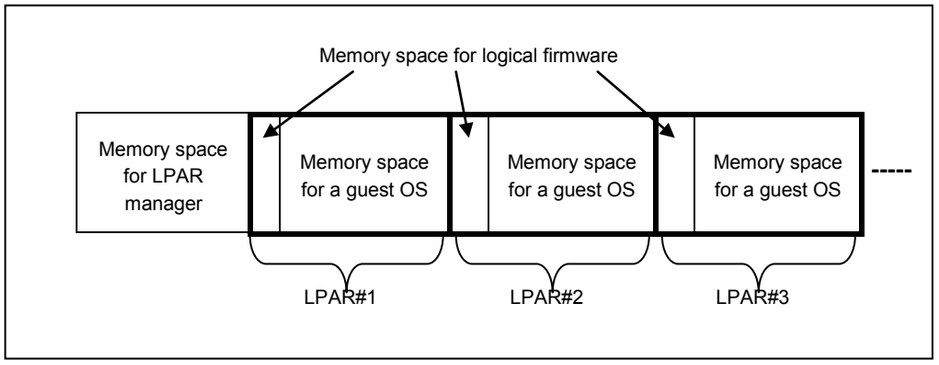
You can restrict the use of physical processors for a group of LPARs by forming a group of physical processors with one processor. Any number can be defined as a number of a physical processor group. A processor with no processor number defined belongs to the processor group “0”. A processor group number can be specified by the core.



❑ Logical partitioning of memory

The memory size to be allocated to each LPAR can be specified for each LPAR (in multiples of 256 MB). Each guest OS has exclusive use of the memory assigned to its LPAR.

LPAR manager automatically determines which physical memory offset areas to allocate to an LPAR when the LPAR is activated.



- Memory space for LPAR manager

  LPAR manager uses a part of physical memory as follows:

Standard server blade		High-performance server blade	
LPAR manager standard mode	**LPAR manager expansion mode**	**LPAR manager standard mode**	**LPAR manager expansion mode**
1280 MB	1536 MB	1536 MB	1536 MB



When LPAR manager operating mode is changed from standard mode to expansion mode, LPAR manager starts with memory to which 256 MB is added. For example, the memory for the guest OS is reduced by 256 MB. This might cause some LPARs not to activate due to a memory shortage if the maximum memory has been used in LPAR manager standard mode.

- Memory space for logical firmware

  Logical firmware uses a part of memory space assigned to each LPAR.
  Memory space used by logical firmware can be estimated using the following equations.

  (a) Less than 8 GB memory assigned to an LPAR
  0.6% of memory assigned to the LPAR + Number of logical processors X 2.25 MB + 65 MB

  (b) 8 GB or more memory assigned to an LPAR
  0.25% of memory assigned to the LPAR + Number of logical processors X 2.25 MB + 80 MB

- Memory space for a guest OS

  Memory space available for a guest OS is calculated by subtracting the amount of memory the logical firmware uses from the amount assigned to the LPAR. This value is usually the same as the memory space displayed for the guest OS. However, all assigned memory space may not be available depending on the guest OS specifications or environment.



When the amount of memory for a guest OS is not enough against the amount applications use, memory swap might cause performance degradation. When assigning an amount of memory, make sure to take the memory amount for firmware as well as that used by the OS and applications into account.

❑ NUMA (Non-Uniform Memory Access)



It is necessary to assign the processor and memory to the LPARs while understanding the NUMA feature well when using the NUMA setting.

LPAR manager recommends using the non-NUMA on all server blades.

It is unnecessary to set NUMA when the NUMA features are not required.

Outline

The server blade of the NUMA configuration has two or more nodes which consists of a socket (group of processors) and memory connected to it. Nodes are connected by the interconnection.

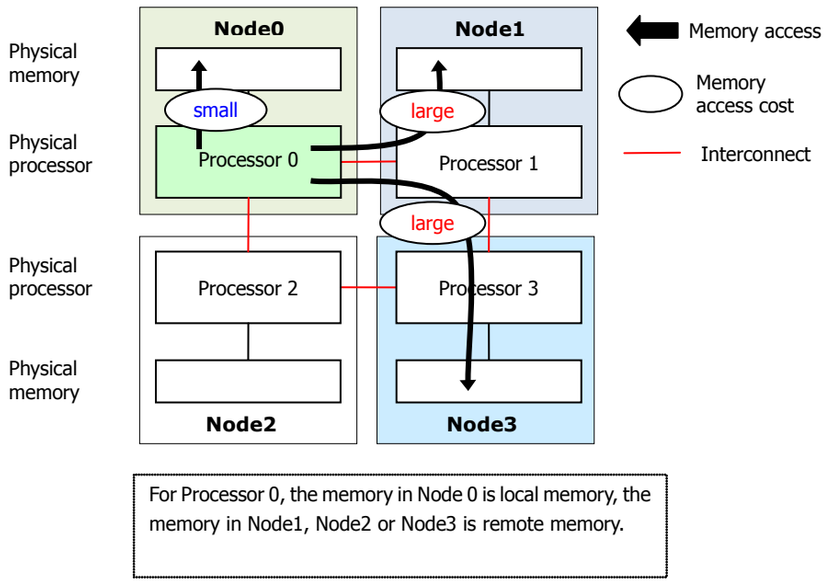
The memory in the same node for a processor is called local memory, and the memory in the other node is called remote memory.

The processor and the local memory are connected directly and close. But the distance to remote memory connected by an interconnection is physically further away compared with local memory.

Each processor can use the memory in all nodes, but the access costs (a delay time) to the memory are influenced by the physical distance.

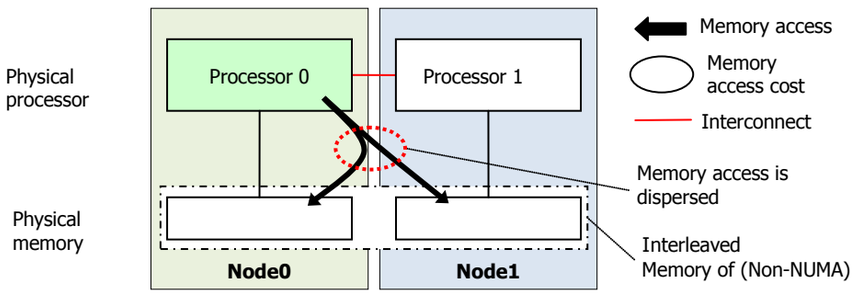
The memory access cost to the local memory is smaller than the remote memory, because the distance to the local memory is shorter than the remote memory. This means that the local memory access performance is higher than the remote one.

The memory access cost from the processor in Node0 to the memory in Node3 is larger than the access cost to the memory in Node1, since it is necessary to go through Node1 to access memory in Node3.



Memory accesses on the NUMA configuration (in the case of four nodes)

In the server blade, which is set to non-NUMA, memory is automatically interleaved and any programs do not need to access the memory, the memory access performance to all the memory area becomes middle of the memory access performance of local memory and remote memory.



Memory accesses on the Non-NUMA configuration

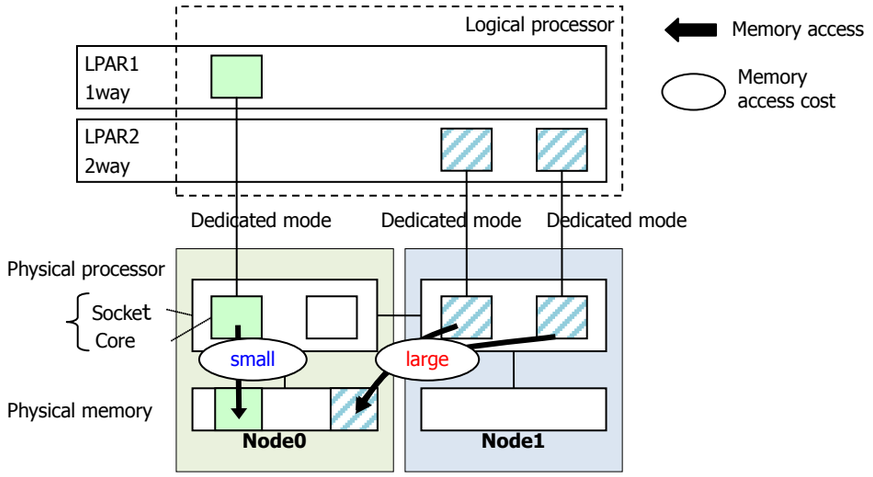
LPAR manager operation on the server blade in NUMA configuration

When Scheduling mode is dedicated mode

The high memory access performance is gained when assigning the physical memory and physical processor in the same node to the LPAR (shown as LPAR1), which is because the the logical processor of the LPAR uses local memory at any time.

When assigning the physical memory and physical processor in the different node to the LPAR (shown as LPAR2), the access memory performance becomes lower, which is because the logical processors of the LPAR use remote memory at any time.

The memory access performance depends on the configuration which processor and memory are assigned to LPAR in dedicated mode, there might be a difference between LPARs.

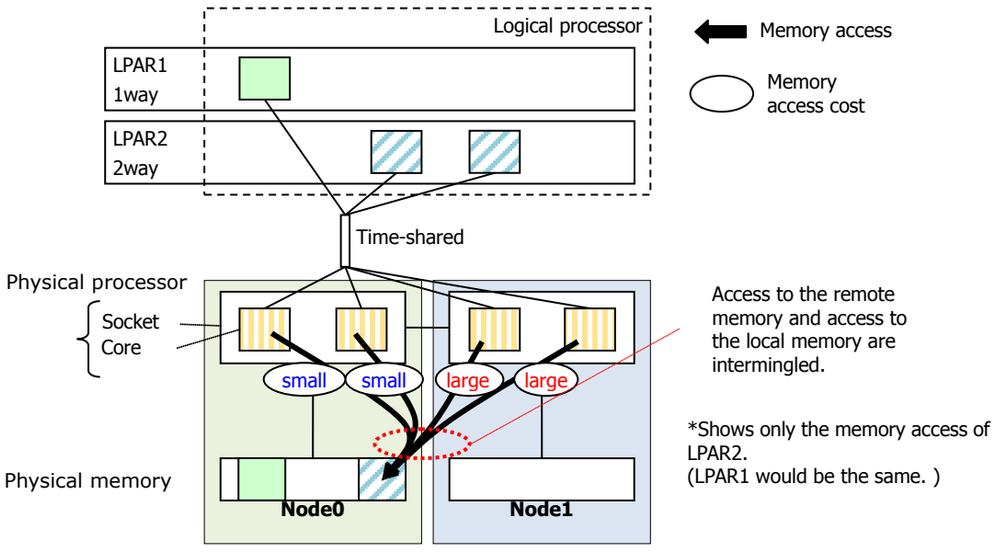


Memory accesses of processors in dedicated mode

When Scheduling mode is shared mode

In the case of the Shared mode, the memory access of logical processors are generally dispersed to multiple nodes, and access to local memory and remote memory are intermingled.

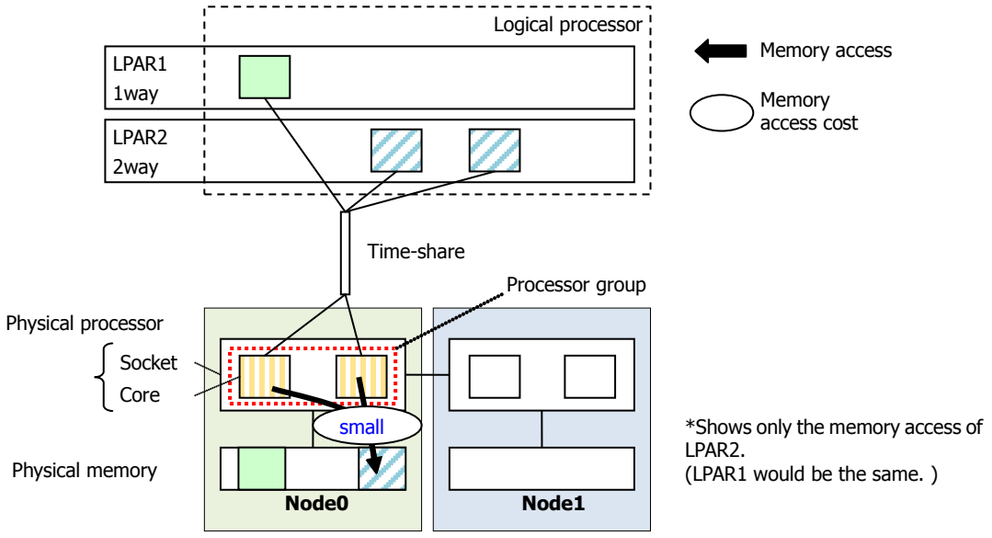
The memory access performance of all LPARs in shared mode will be between the local one and remote one, and there will be almost no difference between LPARs. (See LPAR 1 and LPAR 2 below.)



When the processor group is not configured,
The memory access performance of all the LPAR in share mode will be between local one and remote one.

Memory access of processors in dedicated mode without any processor group

When a processor group is configured by the node, the memory access performance becomes high. That is because the logical processor of LPARs , like LPAR1 and LPAR2 below, always uses the local memory in configuration where the processor group and the physical memory in the same node are assigned to the LPAR.



When making the processor group in a node and allocating the memory in the same node, the memory accesses are always performed in the local memory and the memory cost must be smallest.

Memory access of processors in a shared mode (processor group configuration)

Memory allocation

LPAR manager firmware version 59-2X/79-2X or later supports the following two types of memory allocation; the automatic memory allocation and the memory allocation by specified node. The former considers the node of the physical processor automatically, and the latter allocates the physical memory in one node, which is specified manually by the user. These operations are as follows:

Description of the memory allocation

Memory allocation	Description
Automatic memory allocation	When the activating LPAR is in Dedicated mode, LPAR manager assigns the memory in the node to which the assigned processor belongs to. When the activating LPAR is in Shared mode and the processor group is configured, the LPAR manager assigns the memory in the node of the processor group in which the LPAR is included. When the activating LPAR is in Shared mode and the processor group is not configured, LPAR manager assigns the memory in any node. LPAR manager allocates preferentially the LPAR to the free physical memory that belongs in the same node with the assigned physical processor to the LPAR. When the free physical memory in the same node does not reach the requirement, the LPAR manager allocates the shortage from the other node. * When the total amount of free memory in all nodes does not satisfy the requirement, LPAR activation will fail.
Memory allocation by specified node (manual allocation)	LPAR manager allocates the LPAR the free physical memory in the node specified by the user. * When the free physical memory in the specified node does not satisfy the requirement, LPAR manager does not search the other node and LPAR activation will fail.

The physical processor that is assigned to the LPAR can be changed dynamically by the “scheduling mode dynamic change function”.

However, the physical memory which is allocated to the LPAR is determined in the LPAR activation, and it cannot be changed after activation.

Recommended example of LPAR configuration reducing the memory access cost

When the memory access performance is very important, you should assign the processor and memory to LPAR so that they might be configured in one node.

Please note the following points.

- The memory access cost can be reduced only when the memory amount of LPAR is not more than the one in single node.
- Basically, it is unnecessary to specify a memory node. (Use the automatic memory assignment.)
- However, when you need to suppress the activation if there is not enough free memory in the node, specify the memory node.
- Specify the memory node to all LPARs when you make at least one LPAR which specifies the memory node.
- Do not intermingle the LPAR which specifies the memory node and the LPAR which does not specify the memory node.
- See the Logical partition configuration screen for details of the operation.
- See the Logical processor configuration screen for specifying the physical processor number.

In the server blade of a NUMA configuration, the configuration example of the processor and the memory to the LPAR, which is recommended from the memory access performance perspective, is shown below.

When the Scheduling mode is the dedicated mode

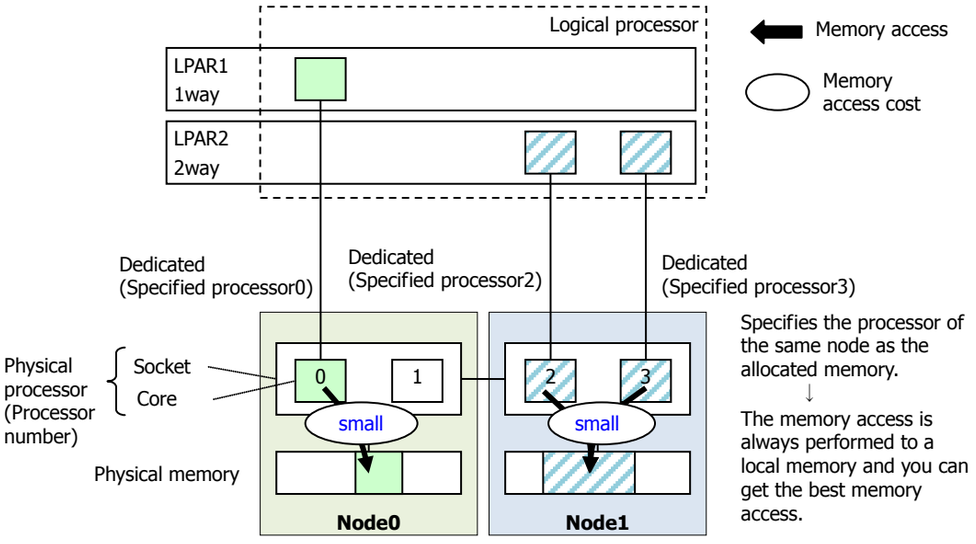
There are two types for improving the memory access performance:

- When specifying the physical processor number, and
- When configuring the processor group

When configuring a processor group, it is possible to skip specifying the physical processor number in the LPAR configuration.

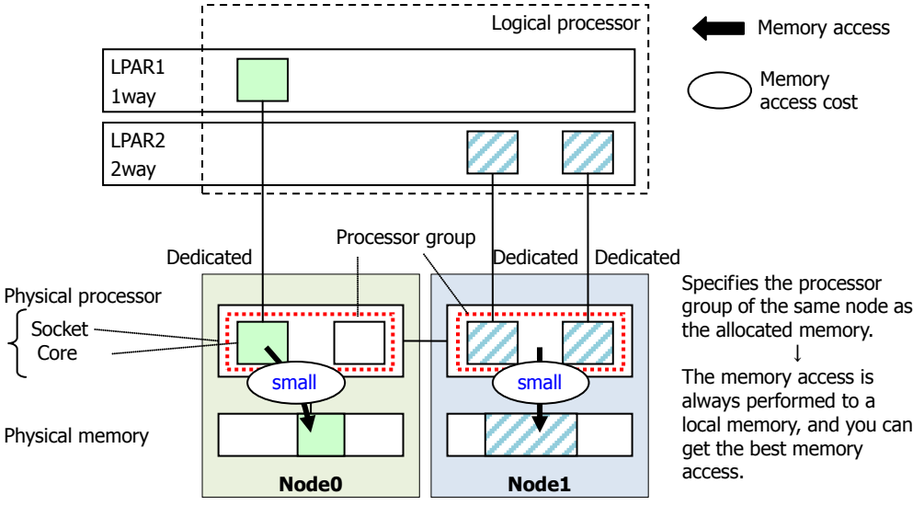
Those are the same memory access performance.

When specifying the physical processor number



A recommended example when in dedicated mode (specifying the physical processor number)

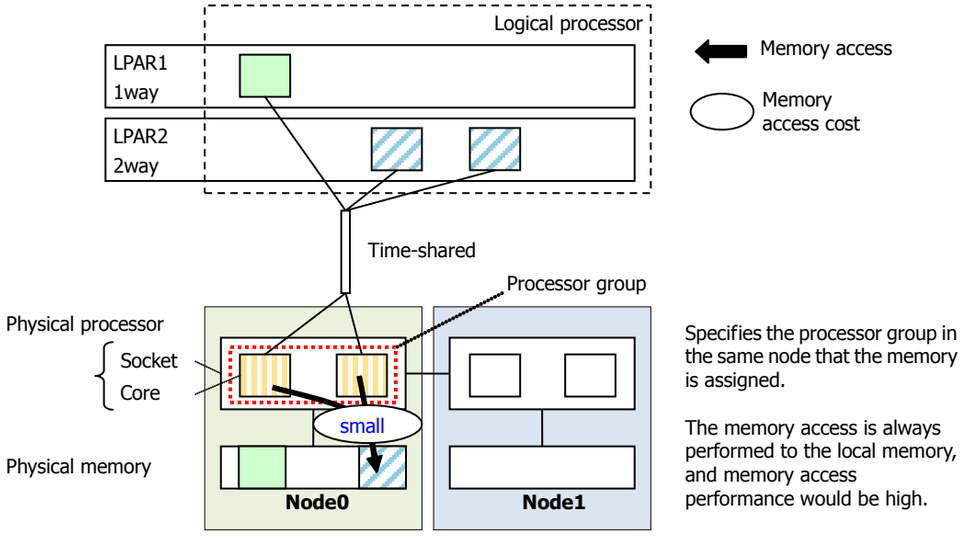
When configuring the processor group



A recommended example when using dedicated mode (configuring the processor group)

When the Scheduling mode is the shared mode

The memory access performance would be high by configuring processor group per node.



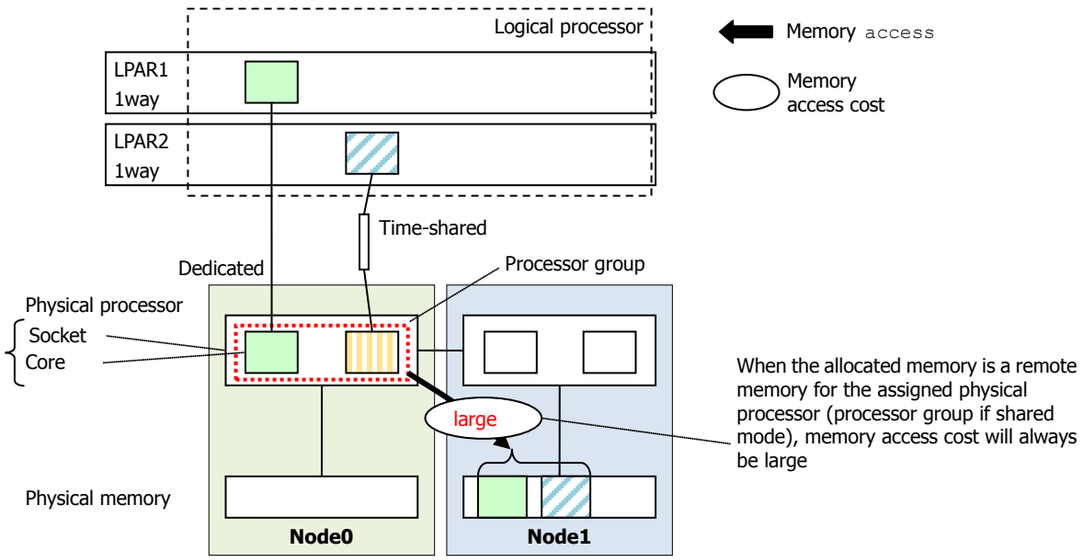
A recommended example when using shared mode

Note for LPAR configuration

There is a risk that memory access cost will be large in the following two types of LPAR configurations.

- When the physical processor and the physical memory that are assigned to the LPAR belong to the different nodes.
- When the physical processors in more than one node are assigned to LPAR in dedicated mode, or the memory in more than one node is assigned to LPAR in dedicated mode.

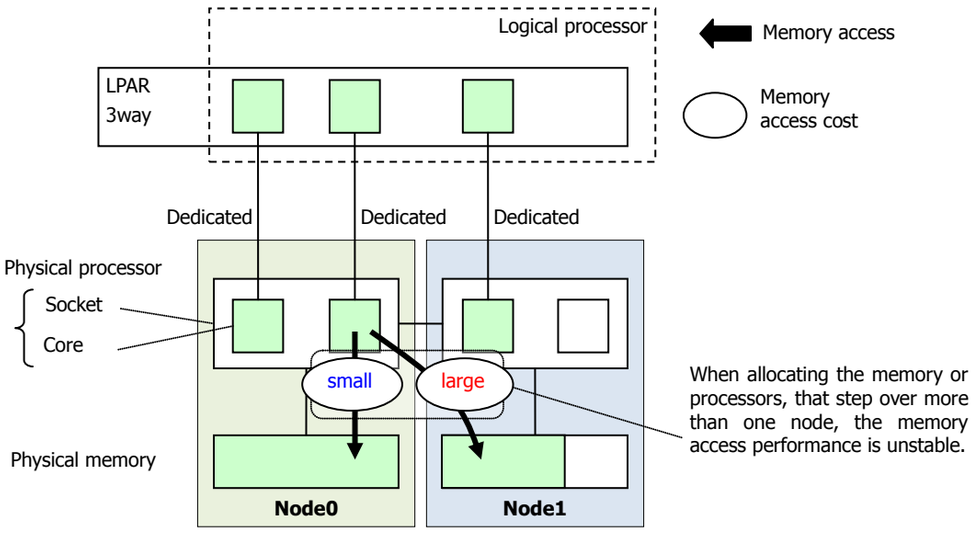
(a) When the physical processors in more than one node, or memory in more than one node, are assigned to the LPAR



When the physical processor and memory are assigned in a different node.

Avoid the configuration above and configure the LPAR using the physical processor and physical memory within one node.

(b) When the LPAR configuration in dedicated mode is large and steps over more than one node.



A large of the large LPAR running in dedicated mode

When LPAR configuration is large, as shown in the figure above, use the shared mode and do not use dedicated mode.

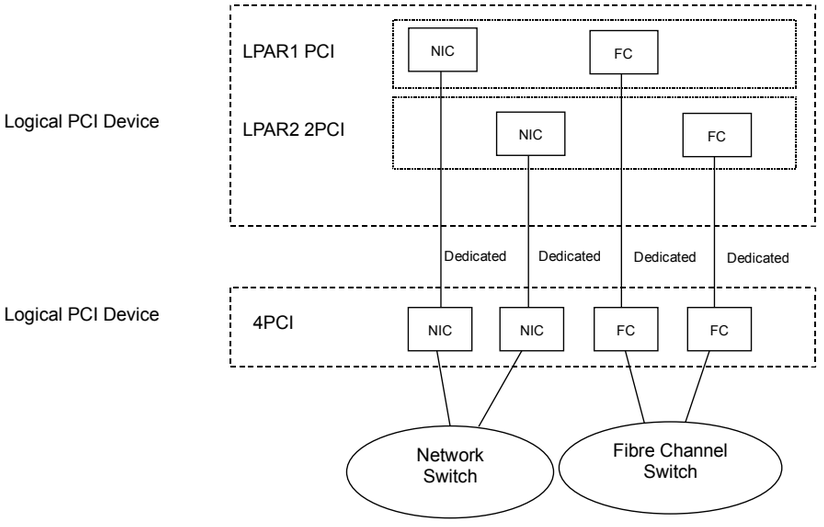
❑ Logical partitioning of PCI devices

In LP mode, PCI devices are assigned to each LPAR in either dedicated or shared mode.

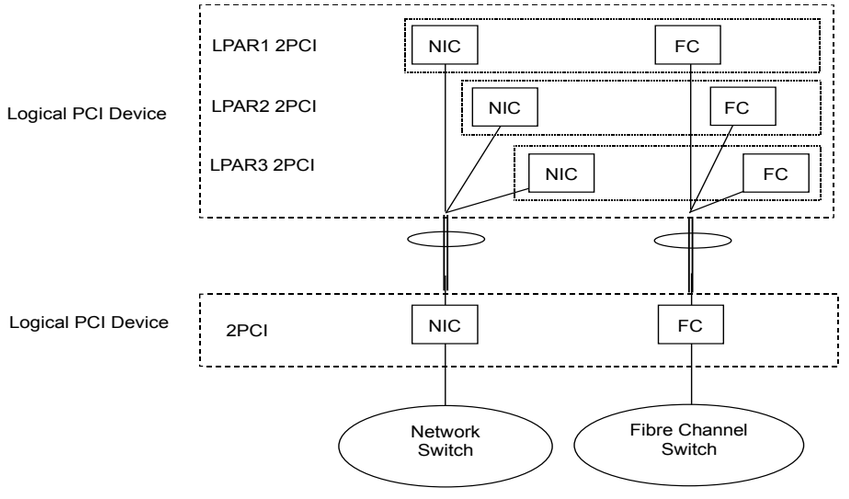
The following table shows features of each mode.

Mode	Feature	Recommended system
Dedicated mode	・ A single PCI device is assigned to a single LPAR (guest OS). The guest OS uses the assigned PCI device exclusively, so that its I/O performance is stable. ・ When 2 ports are implemented in a PCI device, each port cannot be assigned to a separate LPAR.	・ System required high processing performance ・ System required critical time period and high processing in performance
Shared mode	・ A single PCI device is assigned to multiple LPARs (guest OSs). Each guest OS can use the assigned PCI device at the same time without knowing that the PCI device is shared with other OSs. ・ NIC performance of an LPAR is affected by I/O load of other LPARs.	・ System required cost efficiency and flexibility rather than high processing performance ・ System required balanced processing between LPARs

- Example of Dedicated mode



- Example of Shared mode
- For further details of the PCI device shared mode, see Virtual NIC functions and Shared FC Functions in LPAR manager functions.



Network interface card (NIC)

LPAR manager supports the following four virtual NIC functions. See Virtual NIC Functions for details.

Mode	NIC type	Feature
Dedicated	Dedicated NIC	- Stable performance: not affected by other LPARs - High-speed data transmission
Shared	VF NIC	- SR-IOV, a physical NIC function, is used. Supported physical NIC, server blade, and OS are limited. - High-speed data transmission equivalent to Dedicated NIC - Lighter load on physical processors than Shared and Virtual NIC - Transmission bandwidth can be limited by the 100 Mbps.
	Shared NIC	- A physical NIC can be shared by multiple LPARs. - Performance depends on the number of LPARs and traffic volume. - Less restrictions on NIC functions than VF NIC.
Dedicated and Shared	Virtual NIC	- Available only for inter-LPAR transmission - No physical NIC is required.

Fibre Channel (FC)

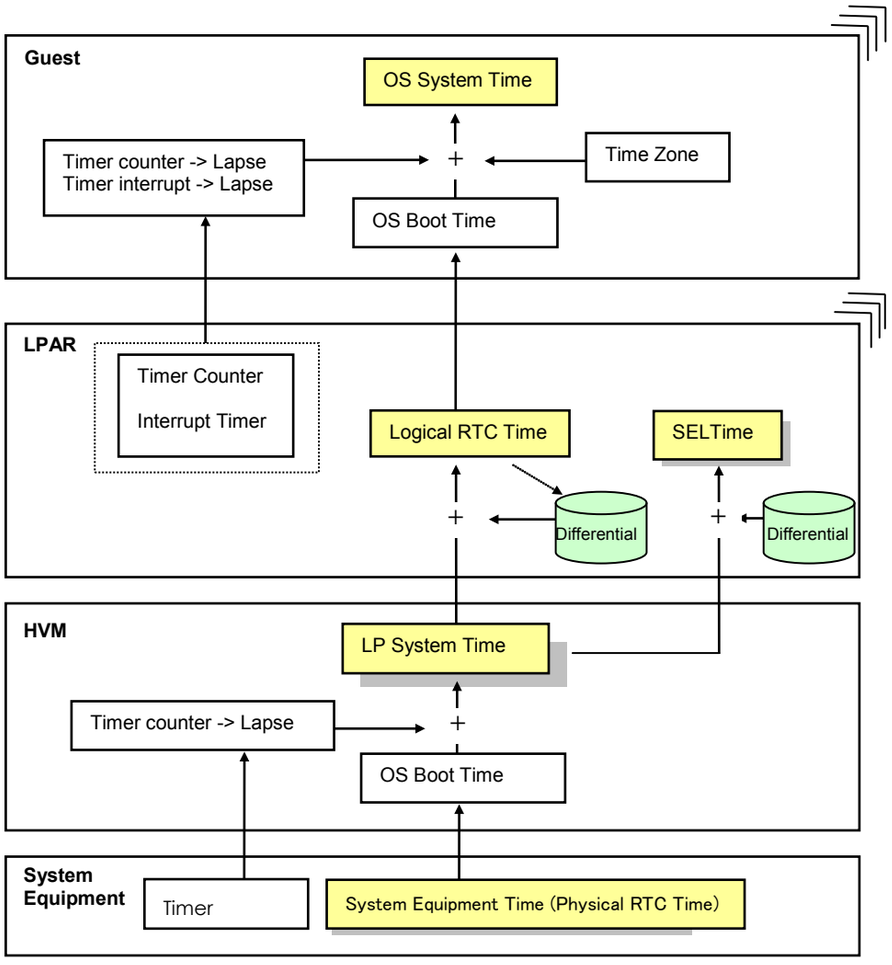
LPAR manager supports the following two Fibre Channel functions. See Shared FC Functions for details.

Mode	FC type	Feature
Dedicated	Dedicated FC	- Stable performance: not affected by other LPARs - High-speed data transmission
Shared	Shared FC	- A port of FC adapter can be shared by multiple LPARs. - Performance depends on the number of LPARs and traffic volume.

❑ Logical partitioning of timers

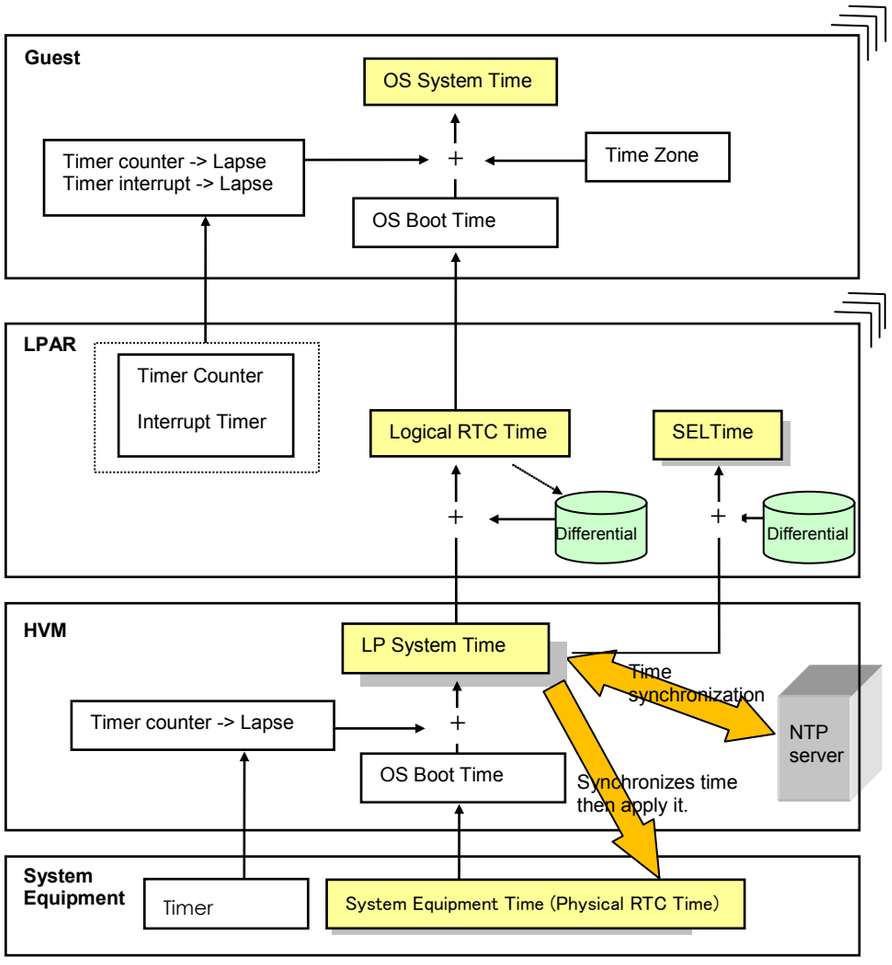
The following figure shows logical partitioning of time in an image. See Timer Functions for details.

No time synchronization with NTP server for LPAR manager system



Note: RTC: Real Time Clock
SEL: System Event Log

Time synchronization with NTP server for LPAR manager system



Note: RTC: Real Time Clock
SEL: System Event Log

LPAR manager manages some types of time shown in the following table. LPAR manager creates each time using differentials between different times.

Based on the LPAR manager system time, LPAR manager creates the logical timer for each LPAR. A guest OS on the LPAR manages “OS system time” using this logical timer.

LPAR manager manages the following time shown in the table below.

Time	Description
System equipment time (Physical RTC time)	A clock in the server blade running by the battery: shows a local time. LPAR manager system time is based on this time.
LPAR manager system time	Used for the LPAR manager screen display as the LPAR manager time. Added elapsed time calculated with the timer counter (TSC) to the physical RTC time at the LPAR manager boot.
Logical RTC time	Is the basis for the OS system time. Calculated using the differentials from the LPAR manager system time.
OS system time	Used as a guest OS time. Added the elapsed time calculated using the logical timer counter, timer interrupt, and the time zone to the logical RTC time at the OS boot.
SEL time	Used as the timestamp of the logical SEL. Calculated using the differentials from the LPAR manager system time.

The following table shows precision on timers and how to adjust time.

Item	Time/ Timer counter	Precision sec./day	Time synchronization	
			Before Save Time Config is supported	After Save Time Config is supported
System equipment	System equipment time (physical RTC time)	± 4	・ EFI setup menu ・ Enable LPAR manager system time synchronization ・ LPAR manager boot with system time synchronization enabled	・ EFI setup menu ・ Enable LPAR manager system time synchronization. ・ LPAR manager boot with system time synchronization enabled. ・ Periodic time synchronization once every 24 hours ・ Date and Time screen (*1) ・ Saving HVM configuration ・ LPAR manager shutdown
LPAR manager	LPAR manager system time (Timer counter) (*5)	TSC: ± 4 Cpu Frequency: ± 1	・ Enable LPAR manager system time synchronization. ・ LPAR manager boot with system time synchronization enabled	・ Enable LPAR manager system time synchronization. ・ LPAR manager boot with system time synchronization enabled

Item	Time/ Timer counter	Precision sec./day	Time synchronization	
			Before Save Time Config is supported	After Save Time Config is supported
				・ Periodic time synchronization once every 15 minutes ・ Date and Time screen (*1)
LPAR	Logical RTC time	± 1	・ Use a command such as guest firmware command and guest OS command. ・ Date and Time screen (*1)(*2)	・ Use a command, such as guest firmware command and guest OS command. ・ Date and Time screen (*1) ・ Periodic time synchronization once every 15 minutes)
	SEL time	± 1	・ Date and Time screen (*1)(*2) ・ SC/Agent	・ Date and Time screen (*1) ・ SC/Agent ・ Periodic time synchronization once every 15 minutes
	Timer counter	± 1	-	-
	Interrupt timer	± 1	-	-
Guest	Time zone	-	Use a command such as the guest OS command.	Use a command such as the guest OS command.
	OS system time (*3)(*4) (*5)(*6)	± 2	Use a command such as the guest OS command.	Use a command such as the guest OS command.

(*1) When the LPAR is deactivated, you can adjust the logical RTC time. If you have adjusted the system equipment time or if an external NTP server has caused time difference from the LPAR manager system time, it is strongly recommended that you should adjust the differentials between the physical RTC time and LPAR manager system time using “Adjust LPAR Time” before booting the guest OS.

(*2) The differentials between the logical RTC time and logical SEL time will be saved by pressing the F9 key: Save Configuration on the LPAR manager Menu screen. LPAR manager does not save the differential information automatically. When you adjust the logical RTC, press F9: Save Configuration on the LPAR manager Menu screen. If you shut down or reboot LPAR manager before saving it or the N+M cold standby function changes server blades, the adjusted differentials are lost.

(*3) Kernel parameters not recommended by LPAR manager might cause problems such as large delay in the OS system time or failure in OS boot. See the *Hitachi Compute Blade 2000 Software Guide* for details.

(*4) When the scheduling is in shared mode and the service time is extremely low with Red Hat Enterprise Linux 5.3 (AMD/Intel 64), a time lag might be around 10 seconds a day. If this happens, check the service ratio and processor group settings and adjust them if necessary.

(*5) You can select LP TimerCounter Precision on the Options screen. See “LP

TimerCounter Base” in Options for details.

(*6) It is recommended that you synchronize the OS system time to the NTP server to keep it correct



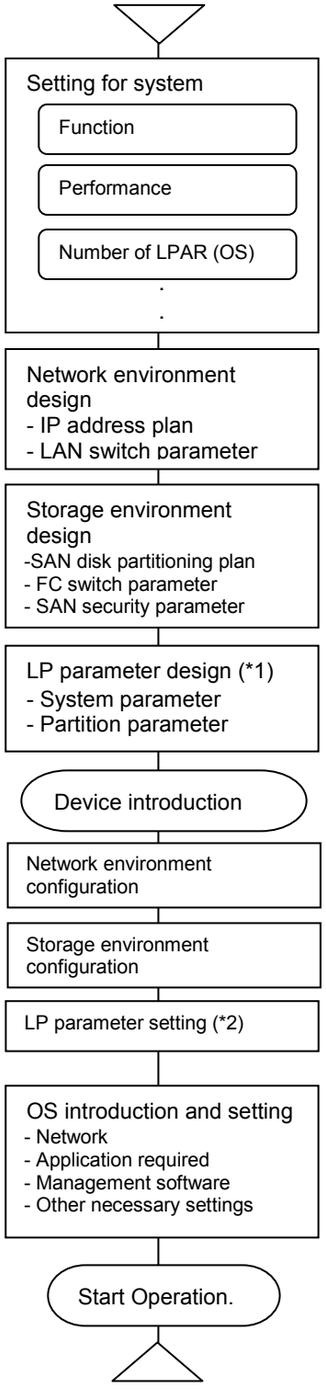
“Save Time Config”, a function to automatically save and update physical and logical RTC time, eliminates guest OS time differentials at the guest OS reboot or LPAR manager reboot. Thus, enabling “Save Time Config” is highly recommended.

See Options for how to enable the function and restrictions.

LPAR manager introduction

❑ Overview of introducing LPAR manager

The following flow chart shows how to introduce LPAR manager.



(*1) Create the parameter sheet using the system requirements. Refer to “LPAR manager setting item” for details.

(*2) Set the LP/EFI driver on the LPAR manager screen and guest screen according to the parameter sheet.

Console used in LPAR manager

The following table shows consoles used in LPAR manager.

Item	Server blade Web console *1	LPAR manager screen *2	Guest screen *2	Virtual COM console *3	Remote console *4	Remote desktop *5	LPAR manager Web system console *6	SC/BSM console *7	HVM Navigator console *8	HCSM console *10
EFI setting	✓	-	-	-	-	-	-	-	-	✓
LP mode setting	✓	-	-	-	-	-	-	-	-	✓
LPAR manager firmware bank number setting	✓	-	-	-	-	-	-	-	-	-
LPAR manager boot	✓	-	-	-	-	-	-	✓	-	✓
LPAR manager screen operation	-	✓	-	-	-	-	-	✓	✓	✓
EFI driver setting	-	-	✓	✓	✓	-	-	-	✓ *9	-
Creating boot options	-	-	✓	✓	✓	-	-	-	✓ *9	-
Guest OS installation	-	-	✓	✓	✓	-	-	-	-	-
Guest OS operation	-	-	-	-	-	✓	-	-	-	-
Guest OS shutdown	-	-	-	-	-	✓	-	-	-	-
Guest OS failure	-	-	✓	✓	✓	-	✓	-	-	-
LPAR manager shutdown	-	✓	-	-	-	-	-	✓	✓	✓
Version-up/Revision-up	-	-	-	-	-	-	✓	-	✓ *9	-
LPAR migration	-	-	-	-	-	-	-	-	✓	✓-

✓: Available; - : Unavailable

*1 Log into BMC via Web browser for connection.

*2 Log into BMC via terminal software for connection.

*3 Log into LPAR manager via terminal software for connection.

*4 See “Remote console connection” for connection.

*5 See the manual of the guest OS.

*6 Log into LPAR manager via Web browser for connection.

*7 See “ServerConductor/BSM Manual” for connection.

*8 See the *HVM Navigator User’s Guide* for connection.

*9 HVM Navigator version 02-01 or later supports this function.

*10 See the *Compute Systems Manager Software User’s Guide*.

Preparation for LPAR manager boot

❑ Terminal software setting

It is recommended to use the latest version of Tera Term (4.XX or later versions) for LPAR manager. If any other kind of terminal software is used, PFkey, PageUp, and/or PageDown might not be available.

If those functions cannot be used with Tera Term earlier versions, change the Tera Term key setting by following the steps below:

1 Open KEYBOARD in the Tera Term folder: Open a text file and then drag and drop KEYBOARD on it.

2 Change the Video Terminal (VT) editor keypad setting to those in the following table, and save it.

Before change	After change
Find=338	Find=327
Insert=327	Insert=338
Remove=329	Remove=339
Select=339	Select=335
Prev=335	Prev=329

3 Start **Tera Term** and execute **Setup > Read key map**. When some files are displayed, select **KEYBOARD.CNF** and then execute **Open**.

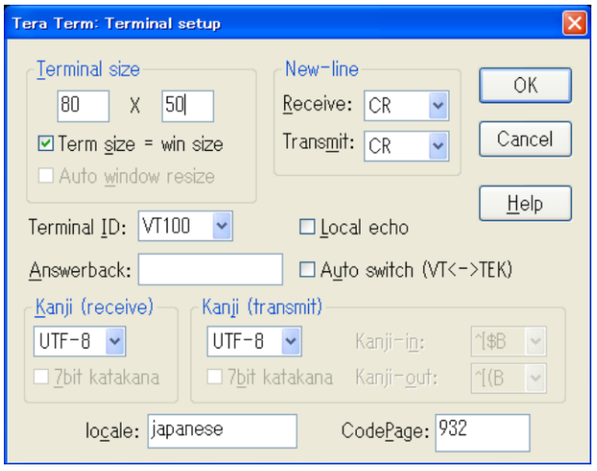
4 Confirm that the PageUp key is available by scrolling pages up and down on the LPAR Configuration screen.

Initial settings for Tera Term as follows:

Be sure to use a Telnet connection. Proper operation with serial connection is not guaranteed.

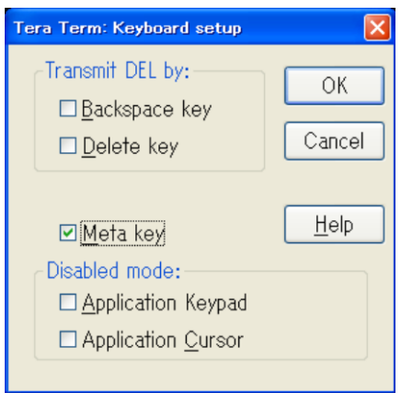
5 Execute **Setup > Terminal** to change the setting to those in the following table.

Item	Setting value
Terminal size	80x50
Terminal ID	VT100
Line feed code	CR
Chinese character	UTF-8



6 Execute **Setup > Keyboard** to change the setting as follows:

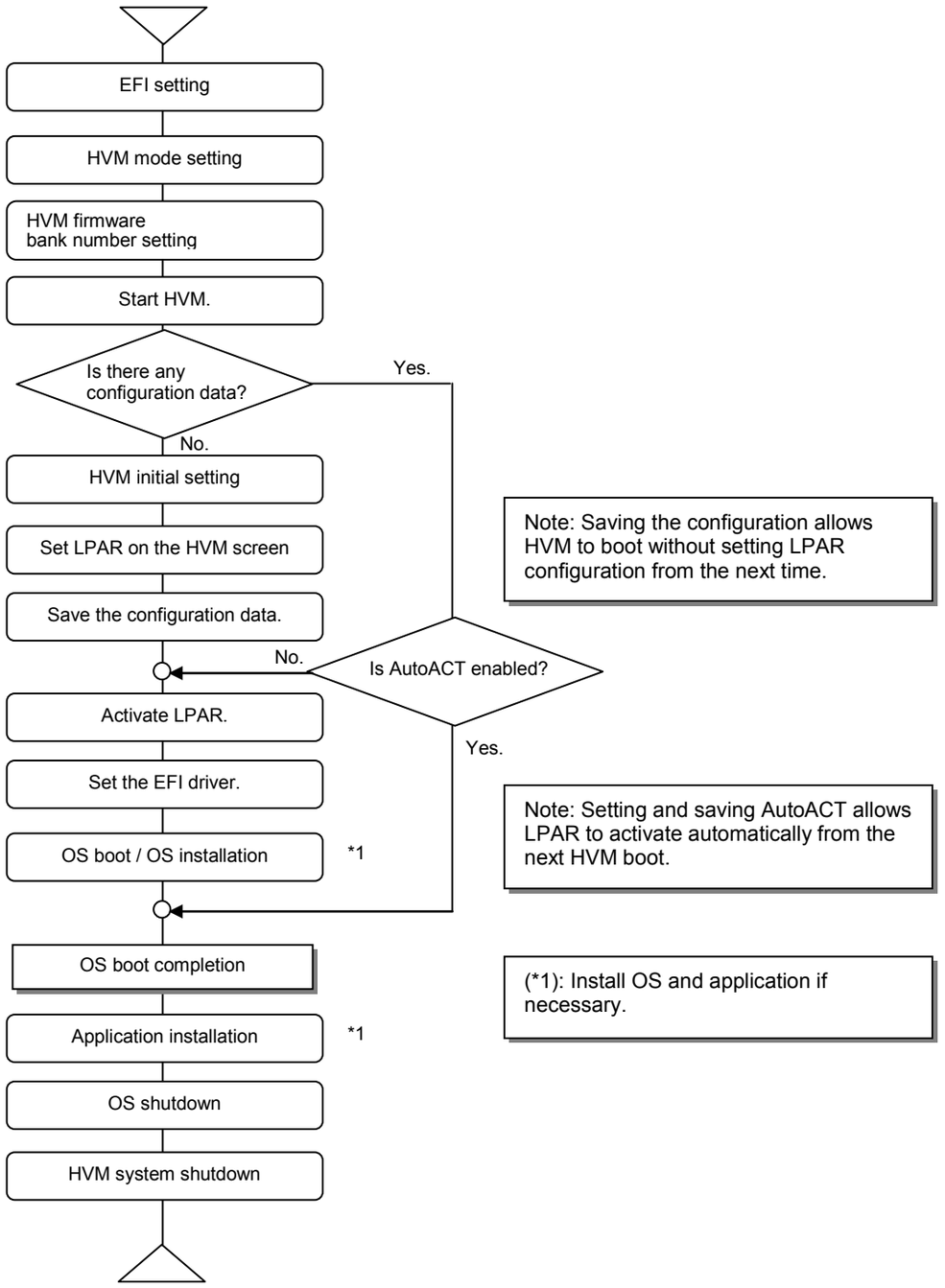
Item	Setting value
Meta key	Checked



Tip

With the Meta key checked, you can use the **Alt** key as a meta key. When a function key is not available on the LPAR manager screen, the Meta key might be used as a function key. **Alt + 8** keys, for example, might be used as the **F8** key.

Operation flow



LPAR manager boot

This section describes how to boot LPAR manager using the server blade Web console.

Screen displays or defaults might be different from those in this manual depending on the firmware version of the server blade Web console.

LPAR manager screen displays might be different from those in this manual depending on the LPAR manager firmware version.

EFI setting

Check that extensible firmware interface (EFI) settings of the server blade where LPAR manager boots as described in the table below. It is recommended that other EFI settings should be the default values.

Item		Setting value	Remarks
SMT (Simultaneous Multi-Threading)		Disable *1	LPAR manager firmware version 57-2X or earlier
		Disable/ Enable	LPAR manager firmware version 57-3X or later
Mode		xAPIC *2	High-performance server blades with BMC firmware version 04-48 or later, or 06-01 or later
Socket Interleave		Non-NUMA	LP firmware version 59-1X/79-1X or earlier
		Non-NUMA/ NUMA *5	LP firmware version 59-2X/79-2X or later
PCI Error Handling Mode *3		Legacy	LPAR manager firmware version 58-6X/78-6X or earlier
		Legacy/PCIe Error Isolation *4	LPAR manager firmware version 58-7X/78-7X or later
PCIe Error Isolation *4	Mezzanine	Disable	LPAR manager firmware version 58-7X/78-7X or earlier
		Disable/ Enable	LPAR manager firmware version 58-8X/78-8X or later
Others		Default	

*1 If SMT setting is Enable, LPAR manager cannot boot. See LPAR manager boot messages for details.

*2 If APIC Mode is not set to xAPIC, LPAR manager cannot boot. See LPAR manager boot messages for details.

*3 The following table describes what happens during PCIe failure.

PCI Error Handling Mode	Behavior at PCIe failure	
	LPAR manager	Guest OS
Legacy	Immediately reboots the server blade forcibly.	Goes down.
PCIe Error Isolation	Isolates the faulty PCI device: deconfigure operation	Non-redundant NIC: IP address and media access control (MAC) assigned to the NIC are unavailable due to the NIC

PCI Error Handling Mode	Behavior at PCIe failure	
	LPAR manager	Guest OS
		unavailable. Redundant NIC: IP address and MAC remain available due to bus replacement. Maintenance in operation is available. Non-redundant host bus adapter (HBA): Hangs up or reboots forcibly because no dump is obtained due to the HBA unavailable. Redundant HBA: Does not go down due to bus replacement. Maintenance in operation is available.

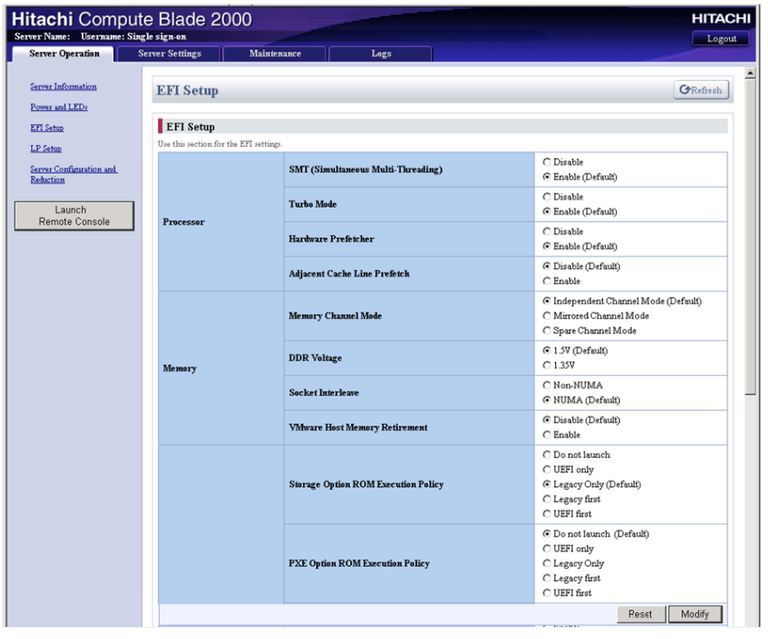
*4 When using PCIe Error Isolation, use the following firmware versions.

Standard server blades with EFI 03-43/04-43 or later; BMC 03-78 or later
High-performance server blades with EFI 03-17/04-17 or later; BMC 04-33 or later, or 06-01 or later

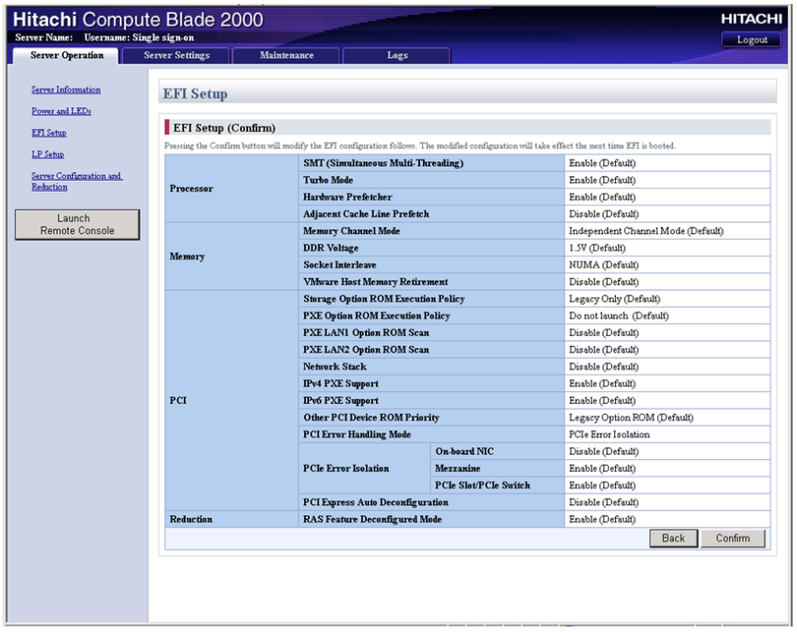
See Chapter 13: System Operation and Management > PCI Error Handling Mode for details.

*5 When setting NUMA to Socket Interleave, you need to assign memory and a processor carefully considering the features. Non-NUMA is basically recommendable.

When you have confirmed that EFI settings are correct, click **Modify**.



Click **Confirm**, and the EFI setup is updated as shown below.



Tip

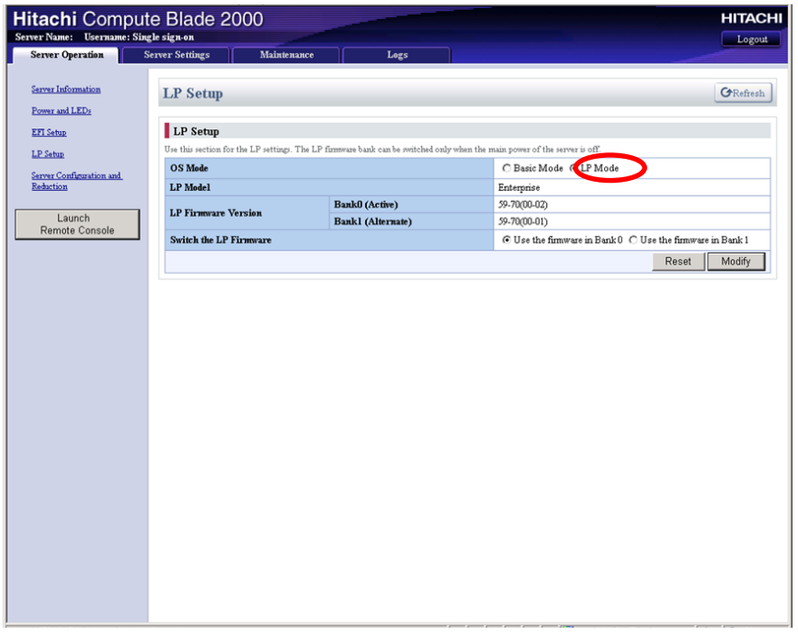
- These settings allow you to boot LPAR manager and operate the LPAR manager screen.
- If booting LPAR manager in the Basic mode after setting EFI, restore all settings to the default values.

LP mode setting

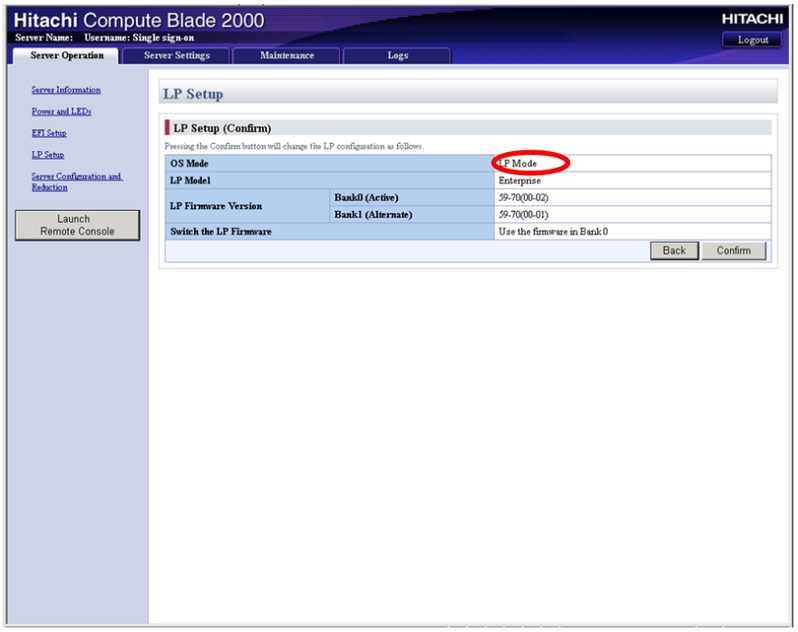
❑ Setting the LP mode

Using the server blade Web console, select **Server Operation>LP Setup>OS mode** and change modes from Basic to" LP mode".

Confirm that the OS mode setting is LP mode and then click **Modify**.



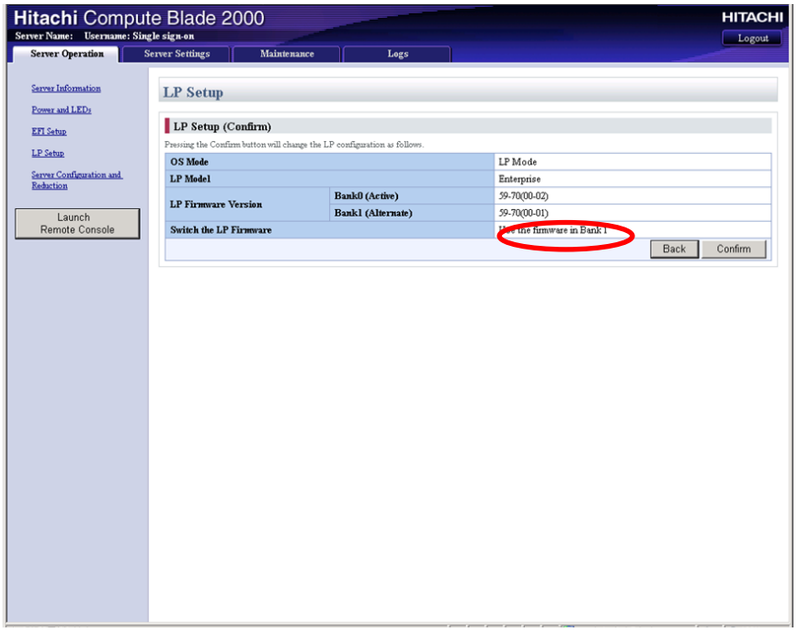
Click **Confirm**, and the OS setting is updated, as shown in the following screen.



LPAR manager firmware bank number selection

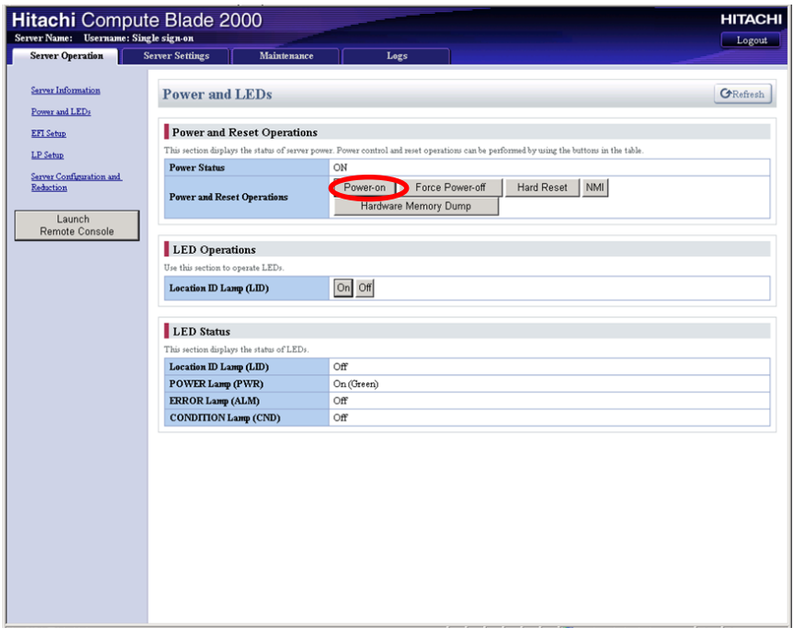
Using the server blade Web console, select **Server Operation**-**LP Setup**-**Switch LP F/W** and click the bank number to boot.
Confirm that the bank number is correct for your requirement, and click **Modify**.

The setting for the number of a bank to boot by pressing **Confirm** is updated as shown below.



Booting LPAR manager

1 Select **Server Operation > Power and LEDs** with the server blade Web console, and click **Power on** to turn on power to the server blade.



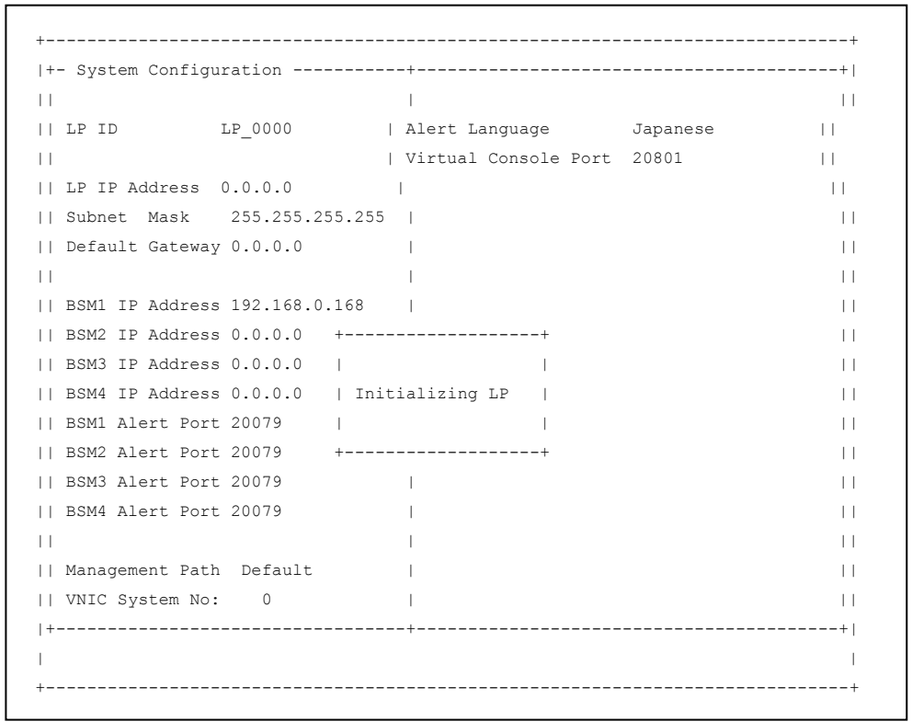
2 Log in to BMC via terminal software to connect to the LPAR manager screen.

Note

When using the LPAR manager screen, connect to the LPAR manager screen via BMC: connect to the BMC IP address via Telnet.

If you connect to the LPAR manager screen via the OS console connected to the management module, some problems might occur. For example, a screen might change to another screen when you press an arrow key on the LPAR manager screen, which is the same behavior when pressing Esc, and setting values might not display correctly.

3 In about five or six minutes after power-on, a message “Initializing LP” will be displayed.



4 In a couple of minutes, LPAR manager initialization is completed and “Initializing LP” will disappear.

Required time for LPAR manager boot is different depending on the SMP configuration or PCI devices installed.

LPAR manager initial settings

1 The System Configuration screen is displayed at the first LPAR manager boot after applying LPAR manager.

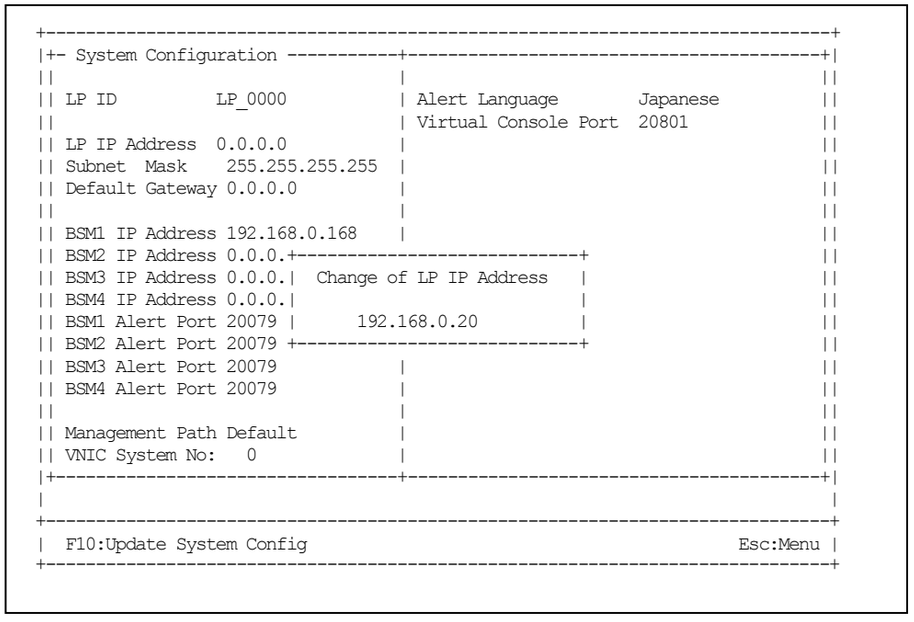
When having set and saved the following items on this screen, the LPAR manager Menu appears to operate the LPAR manager screen.

- Logical partitioning manager (LP) Internet Protocol (IP) Address
- Subnet Mask
- Virtual NIC (VNIC) System No

- LP IP Address setting

  Put the cursor on the **LP IP Address**, and press **Enter**.

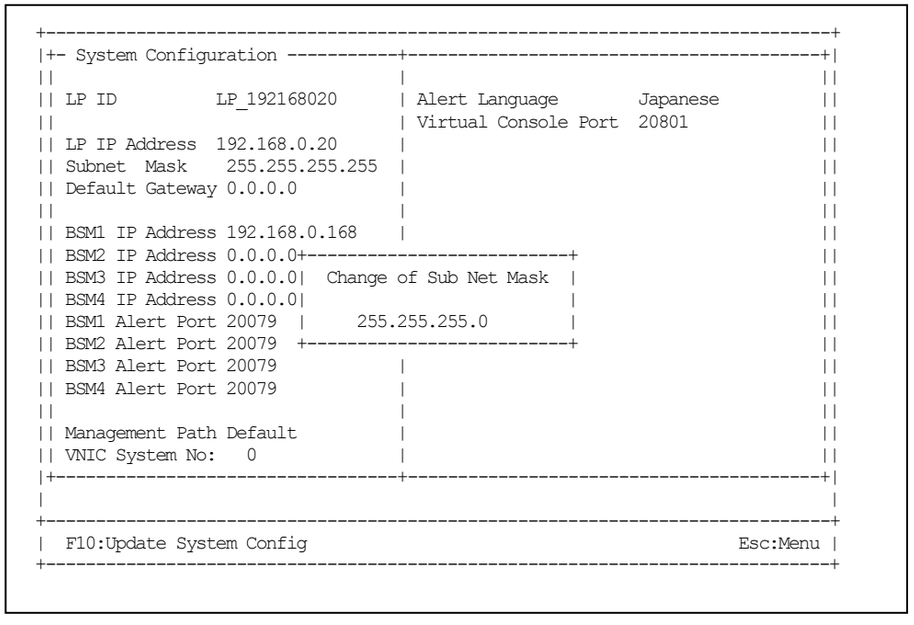
  Input the LP IP address to set in the **Change of LP IP Address** subscreen, and press **Enter**.



- Subnet Mask setting

  Put the cursor on the **Subnet Mask**, and press **Enter**.

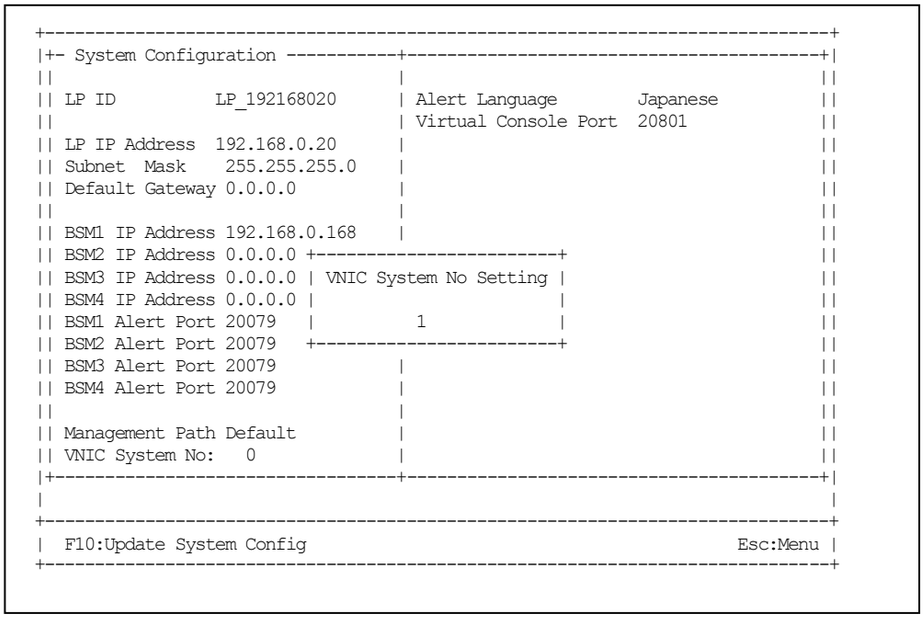
  Input `Subnet Mask` to set in the subscreen to **Change of Net Mask**, and press **Enter**.



- VNIC System No setting

  Put the cursor on **VNIC System No**, and press **Enter**.

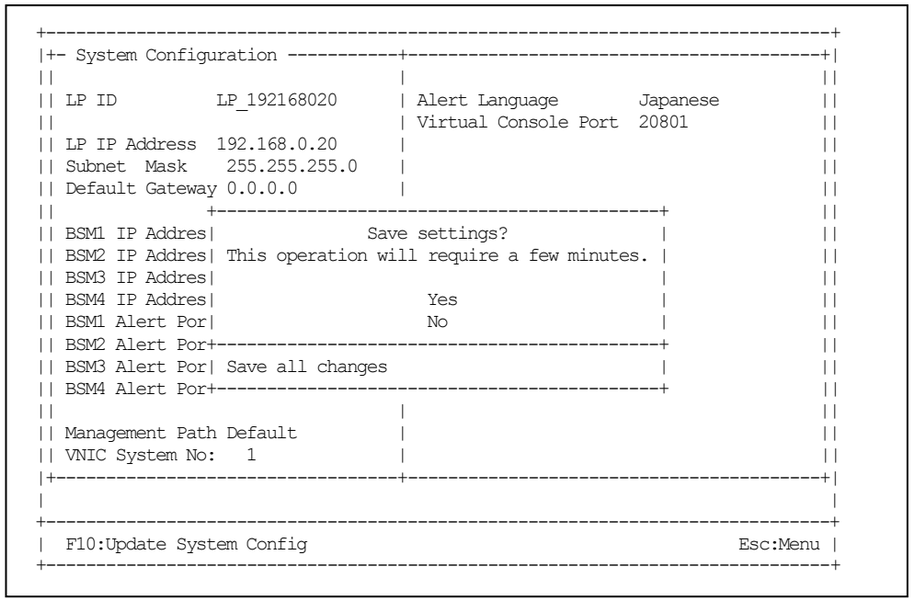
  Input `VNIC System No` to set in the subscreen to `VNIC System No Setting`, and press **Enter**.



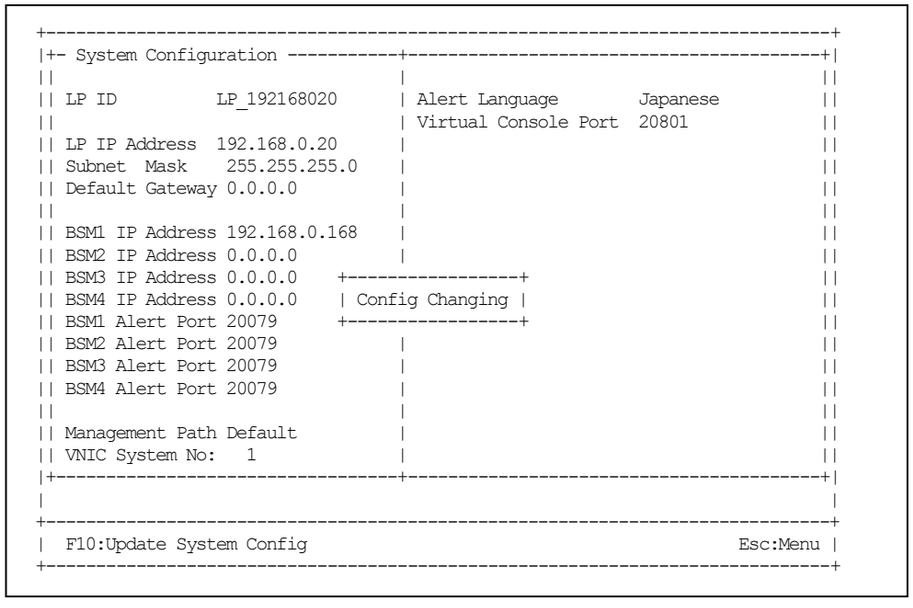


VNIC System No is used to create the MAC address to avoid creating the duplicate virtual NIC MAC address, the default value. Specify a unique value to every LPAR manager system including Compute Blade 1000, Compute Blade 2000, and Compute Blade 320. See “(1) MAC Address for Virtual NIC” for further details about MAC address for the virtual NIC.

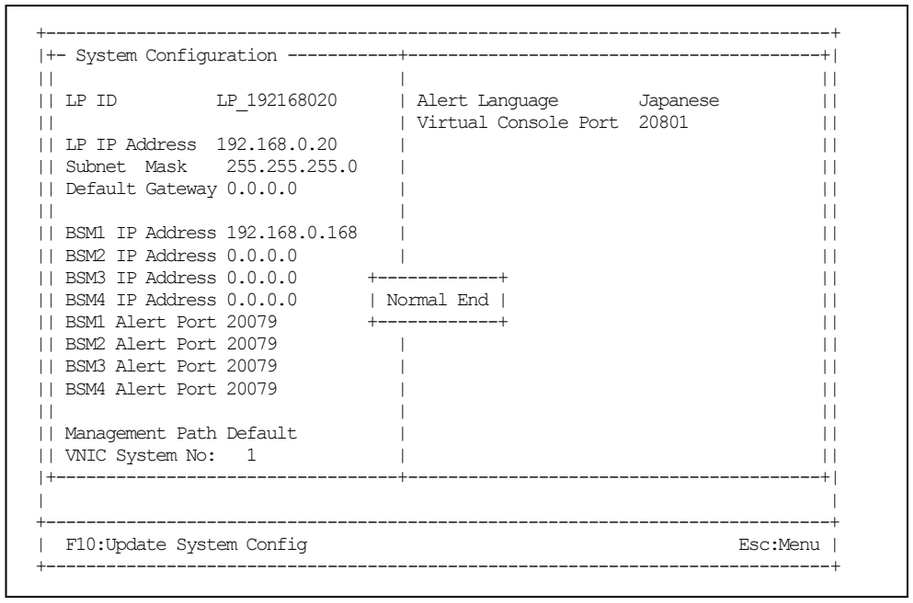
- Press **F10 (Update System Config)** after step 1, and select **Yes** on the **Save settings?** subscreen.



A message “Config Changing” is displayed.



A message “Normal End” is displayed in about 40 seconds.



Tip

The operation with the F10 key (Update system Config) provides a temporary change in the screen when LPAR manager is running. Thus, the setting, which is not saved, will disappear when LPAR manager is rebooted. Execute the F9 key (Save configuration) in the LPAR manager Menu screen to save the new setting. See Save configuration changed on LPAR manager screen for details.

2 Configure settings for LPAR manager system time zone and for LPAR manager system time synchronization with NTP.

LPAR manager firmware version 58-6X/78-6X or earlier

- Go to the Date and Time screen.
- Press **F7: Change System Time Zone** to display a subscreen. Set your time zone on the subscreen and press Enter.

```
|+- System Date and Time ------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-------------------------------------------------------------------------+|
|                                                                           |
 +-------------------------------------------------------------------------+
```

LPAR manager firmware version 58-7X/78-7X or later

- Go to the Date and Time screen.
- Press **F7 key: Change System Time Zone** to display a subscreen. Set your time zone on the subscreen and press **Enter**.

```
|+- System Date and Time ------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting--------------------------------------------------------------+|
|| Import Config None                                                      ||
|| TimeSync      Disable                                                   ||
|+-------------------------------------------------------------------------+|
```

- Point the cursor on Timesync on the Date and the System screen and press **Enter** to display a subscreen. Select **SVP** and press **Enter**.

```
||  7                       +-------------------+                          ||
||  8                       | Select NTP Server |                          ||
||  9                       |                   |                          ||
|| 10                       |      Disable      |                          ||
|+--------------------------|      NTP          |--------------------------+|
|                          |      SVP          |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+-------------------+--------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting--------------------------------------------------------------+|
|| Import Config None                                                      ||
|| TimeSync      Disable                                                   ||
|+-------------------------------------------------------------------------+|
```

- Confirm that the NTP setting is SYNC on the System Service State screen.

```
|+- System Service--------------------++-- Virtual LAN Segment State----------+|
||  SVP Access   : RUN                ||   PORT#/NIC# :  V  1  2  3  4  5  6  ||
||  BSM Access   : RUN                ||       a      :  S  S                 ||
||  HA Monitor   : RUN                ||       b      :  S  S                 ||
||  NTP          : SYNC               ||       c      :  S                    ||
||                    Force Recovery  ||       d      :  S                    ||
|+-----------------------------------++-----------------------------------------+|
```

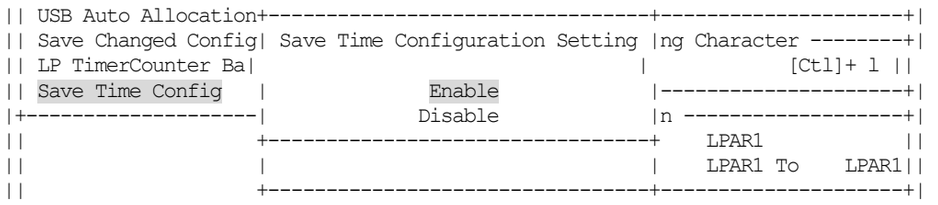
For LPAR manager firmware version 58-7X/78-7X or later, synchronizing LPAR manager system time with NTP server is recommended.

If you reboot LPAR manager after operating it for a long time without time synchronization with NTP server, or if a system failure in LPAR manager or failover with N+M cold standby unexpectedly occurs, a time lag occurs in the guest OS.

3 Configure settings for automatically saving time information

LPAR manager firmware version 59-41/79-41 or earlier

- Go to the Options screen.
- On Options screen, place the cursor on **Save Time Config** and press **Enter** to display the subscreen. Select **Enable** and press **Enter**.



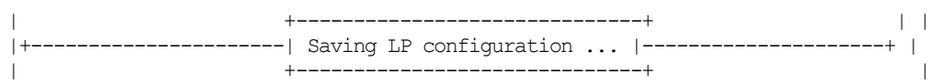
With LPAR manager firmware version 59-41/79-41 or later, enabling “Save Time Config” is recommended. You can change settings for “Save Time Config” while LPAR manager is running.

If you reboot LPAR manager after operating it for a long time with “Save Time Config” disabled, or if a system failure in LPAR manager or failover with N+M cold standby unexpectedly occurs, a time lag occurs in the guest OS.

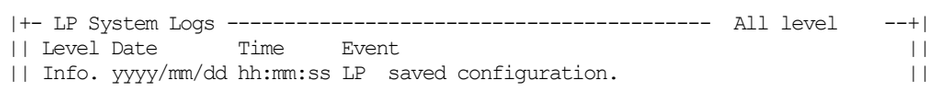
If changing LPAR manager configuration or LPAR configuration with “Save Time Config” enabled, make sure to press the F9 key at the end of the setting change. Although LPAR manager configuration is saved at time adjustment with “Save Time Config” enabled, the timing cannot be specified.

When LPAR manager configuration is saved at time adjustment, LPAR manager screen appears; system event logs are collected; the alert is notified. Those operations can be prevented by disabling “Save Time Config”.

<LPAR manager screen>



<System event log>



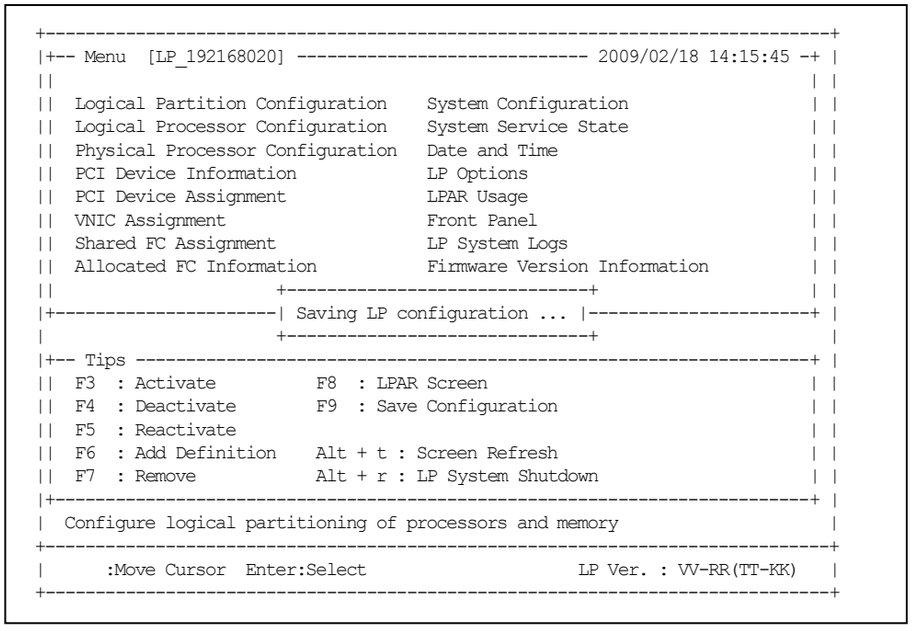
<Alert>

Alert ID: 0x1531

Message: LP configuration was saved. (RC=6)

4 Save the new settings on the LPAR manager screen.

- Go to the LPAR manager Menu screen.
- Press **F9: Save Configuration** on the LPAR manager Menu screen.



Then you can perform operation on the LPAR manager screen.

Basic operation of LPAR manager

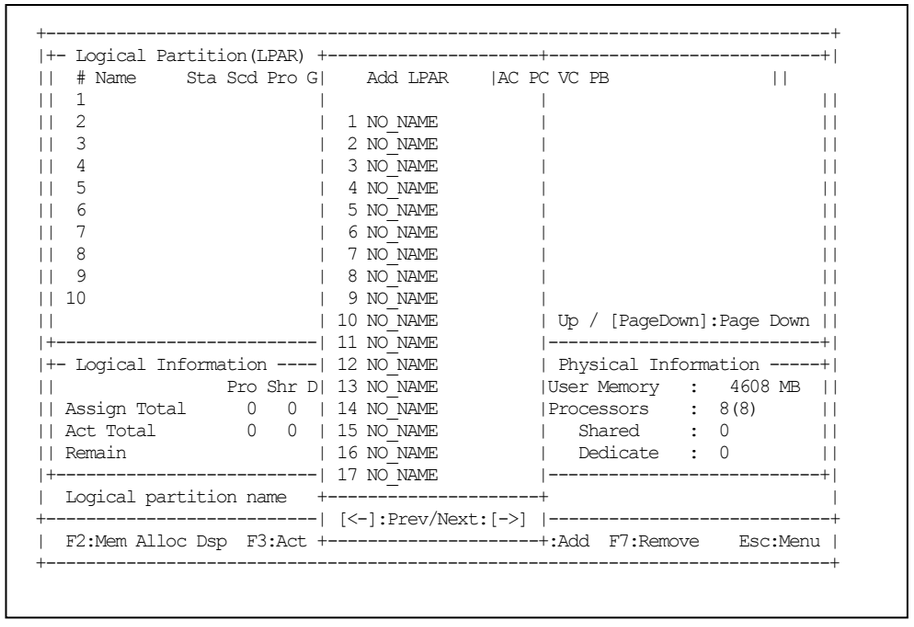
This section describes the basic screen settings and operations to boot a guest OS.

LPAR manager screen displays might be different from those in this manual depending on the LPAR manager firmware version.

Add LPAR and change LPAR name

In the initial state, no LPAR is defined. Follow the procedure below to add LPARs.

1. On the **LPAR manager Menu** screen, press **F6; Add Definition**.
2. Select **NO_NAME** and press **Enter**. (Place the cursor on 1 and press **Enter**.)

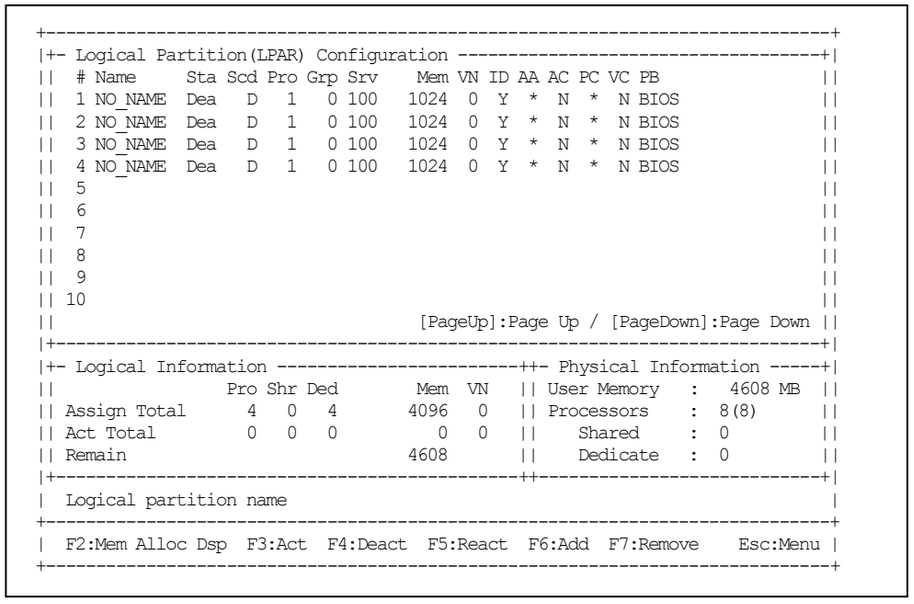




When the number of definable LPARs is 18 or larger, you can switch the subscreen using arrow keys, [←] or [→]. When the number of them is 17 or smaller, those arrow keys are not displayed.

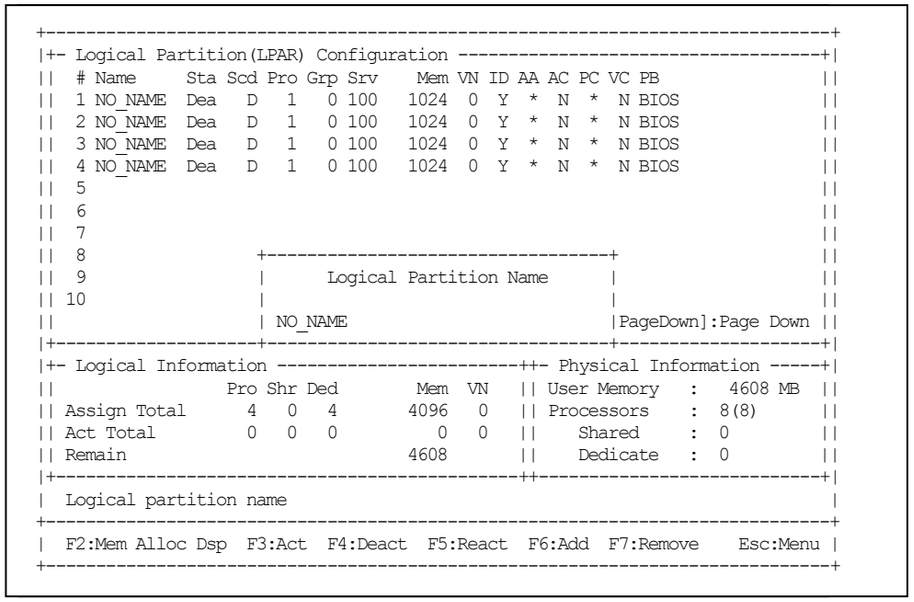
3 You can add multiple LPARs in the same say.

■ Example of Logical Partition (LPAR) Configuration

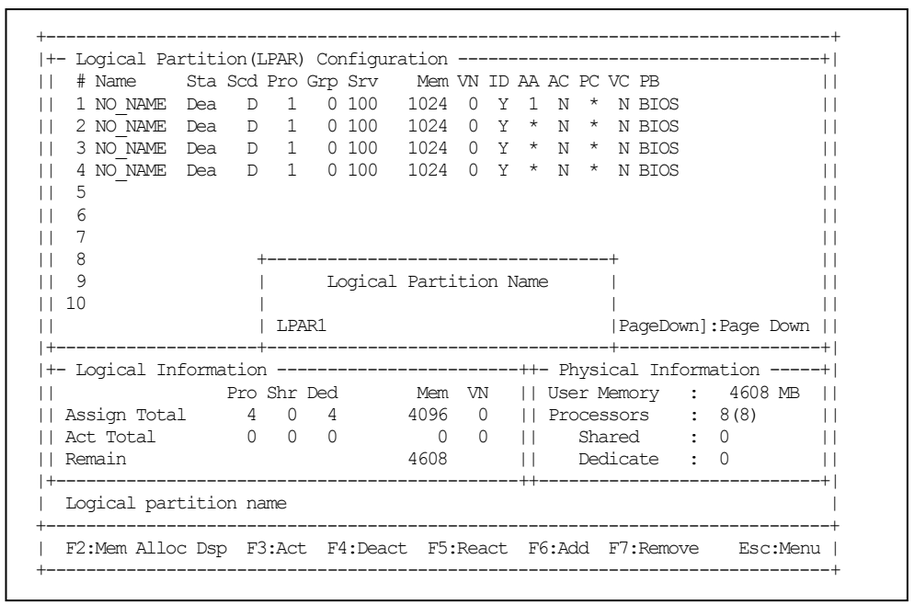


Names of added LPARs are the default value “NO_NAME”. Set LPAR names in the following procedure. You can change LPAR names already set in the same way.

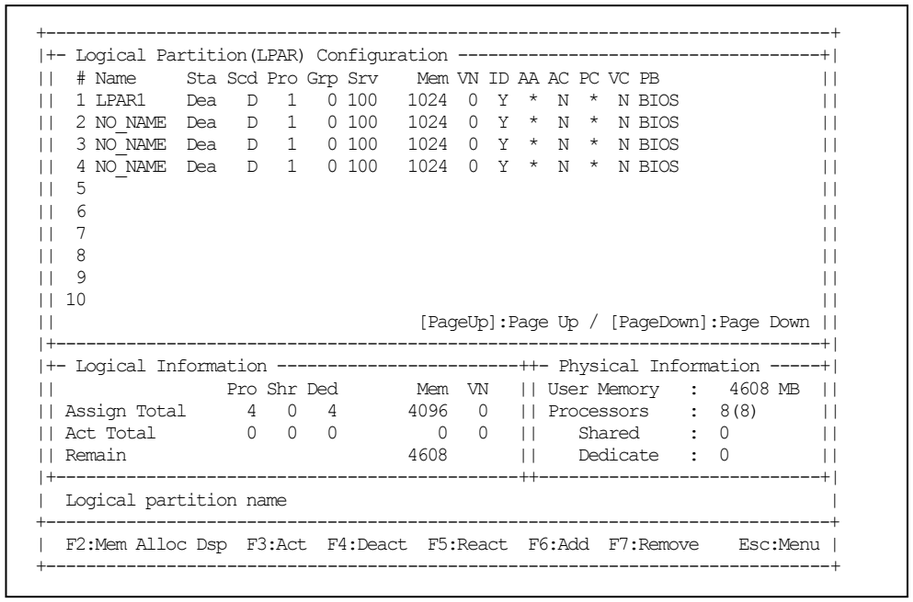
4 Select an LPAR name and press **Enter**. A subscreen “Logical Partition Name” is displayed.



5 Change the LPAR name on the subscreen.



6 Press **Enter**.



Tip

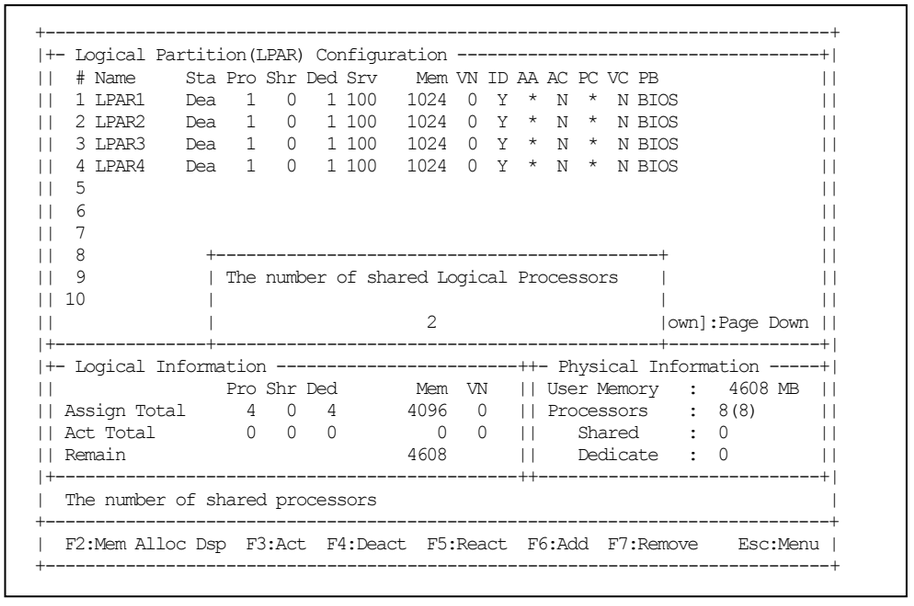
- Set the LPAR name with up to 31 characters. However, the only first 8 characters are displayed on the LPAR manager screen. (If you set more than 8 characters, the 8th character shown on the terminal will become "~".
- You can use the following characters: "0" – "9", "a" – "z", "A" – "Z", "-" and "_". However, the first character in a LPAR name must be a letter: "a" – "z" or "A" – "Z".
- The LPAR name is used as an identifier of the LPARs. It is used for the functions such as the HA monitor. Set a unique name within the LPAR manager system.

Assign scheduling mode and processors to LPARs

To change assignments of scheduling modes or the number of processors to an LPAR, make the following settings on the Logical Partition Configuration screen.

For: Standard sever blades with LPAR manager firmware 58-2X or earlier versions
High-performance server blades with LPAR manager firmware 78-2X or earlier versions

1. Place the cursor on **Shr** of the LPAR to change, and press **Enter**.
2. Type the number of processors in **The number of Shared Logical Processors** subscreen, and press **Enter**.



Example of Logical Partition Configuration (Processor number) setting

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ----------------------------------+|
||  # Name     Sta Pro Shr Ded Srv    Mem VN ID AA AC PC VC PB               ||
||  1 LPAR1    Dea   2   2   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  2 LPAR2    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  3 LPAR3    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  4 LPAR4    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  5                                                                        ||
||  6                                                                        ||
||  7                                                                        ||
||  8                                                                        ||
||  9                                                                        ||
|| 10                                                                        ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+-------------------------------------------------------------------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                Pro Shr Ded       Mem  VN   || User Memory   :   4608 MB  ||
|| Assign Total     5   2   3      4096   0   || Processors    :  8(8)      ||
|| Act Total        0   0   0         0   0   ||    Shared     :  0         ||
|| Remain                          4608       ||    Dedicate   :  0         ||
|+-----------------------------------------++-----------------------------+|
|  The number of shared processors                                          |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

For: Standard sever blades with LPAR manager firmware 58-3X or earlier versions
High-performance server blades with LPAR manager firmware 78-3X or earlier versions

1 Place the cursor on **Scd** of the LPAR to change, and press **Enter**.

2 Select a mode to assign in **Logical Processors Scheduling mode Assignment** subscreen, and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta Scd Pro Grp Srv    Mem VN ID AA AC PC VC PB                ||
||  1 LPAR1    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  2 LPAR2    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  3 LPAR3    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  4 LPAR4    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  5                                                                         ||
||  6                                                                         ||
||  7          +---------------------------------------------+               ||
||  8          | Logical Processors Scheduling mode Assignment |              ||
||  9          |                                             |               ||
|| 10          |                      D                      |               ||
||             |                      S                      |wn]:Page Down ||
|+-------------+---------------------------------------------+--------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                 Pro Shr Ded       Mem  VN    || User Memory   :   4608 MB  ||
|| Assign Total      4   0   4      4096   0    || Processors    :  8(8)      ||
|| Act Total         0   0   0         0   0    ||    Shared     :  0         ||
|| Remain                          4608        ||    Dedicate   :  0         ||
|+-------------------------------------------++-----------------------------+|
|  Logical processors scheduling mode                                          |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
      +-------------------------------------------------------------------------
```

Example of Logical Partition Configuration (Scheduling mode) setting

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta Scd Pro Grp Srv    Mem VN ID AA AC PC VC PB                ||
||  1 LPAR1    Dea   S   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  2 LPAR2    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  3 LPAR3    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  4 LPAR4    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS              ||
||  5                                                                         ||
||  6                                                                         ||
||  7                                                                         ||
||  8                                                                         ||
||  9                                                                         ||
|| 10                                                                         ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+-------------------------------------------------------------------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                 Pro Shr Ded       Mem  VN    || User Memory   :   4608 MB  ||
|| Assign Total      4   1   3      4096   0    || Processors    :  8(8)      ||
|| Act Total         0   0   0         0   0    ||    Shared     :  0         ||
|| Remain                          4608        ||    Dedicate   :  0         ||
|+-------------------------------------------++-----------------------------+|
|  Logical processors scheduling mode                                          |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

3 Place the cursor on **Pro** of the LPAR to change, and press **Enter**.

4 Type the number of processors in **The number of Logical Processors** subscreen, and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ----------------------------------+|
||  # Name     Sta Scd Pro Grp Srv    Mem VN ID AA AC PC VC PB               ||
||  1 LPAR1    Dea   S   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  2 LPAR2    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  3 LPAR3    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  4 LPAR4    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  5                                                                        ||
||  6                                                                        ||
||  7                                                                        ||
||  8                +---------------------------------+                   ||
||  9                | The number of Logical Processors |                   ||
|| 10                |                                  |                   ||
||                    |               2                  |PageDown]:Page Down ||
|+-------------------+----------------------------------+--------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                Pro Shr Ded       Mem  VN    || User Memory   :   4608 MB  ||
|| Assign Total     4   1   3      4096   0    || Processors    :  8(8)       ||
|| Act Total        0   0   0         0   0    ||    Shared     :  0          ||
|| Remain                         4608        ||    Dedicate   :  0          ||
|+-----------------------------------------++-----------------------------+|
|  The number of logical processors                                         |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

Example of Logical Partition Configuration (Processor number) setting

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ----------------------------------+|
||  # Name     Sta Scd Pro Grp Srv    Mem VN ID AA AC PC VC PB               ||
||  1 LPAR1    Dea   S   2   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  2 LPAR2    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  3 LPAR3    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  4 LPAR4    Dea   D   1   0 100   1024  0  Y  *  N  *  N BIOS             ||
||  5                                                                        ||
||  6                                                                        ||
||  7                                                                        ||
||  8                                                                        ||
||  9                                                                        ||
|| 10                                                                        ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+-------------------------------------------------------------------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                Pro Shr Ded       Mem  VN    || User Memory   :   4608 MB  ||
|| Assign Total     5   2   3      4096   0    || Processors    :  8(8)       ||
|| Act Total        0   0   0         0   0    ||    Shared     :  0          ||
|| Remain                         4608        ||    Dedicate   :  0          ||
|+-----------------------------------------++-----------------------------+|
|  The number of logical processors                                         |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

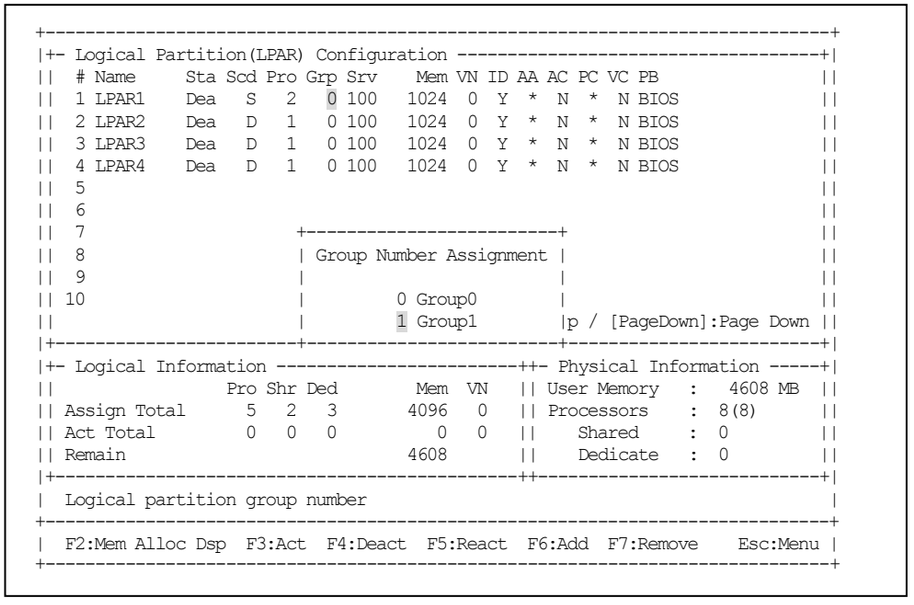
Change processor group assignment

To change processor groups to assign to an LPAR, make the following settings on the Logical Partition Configuration screen.

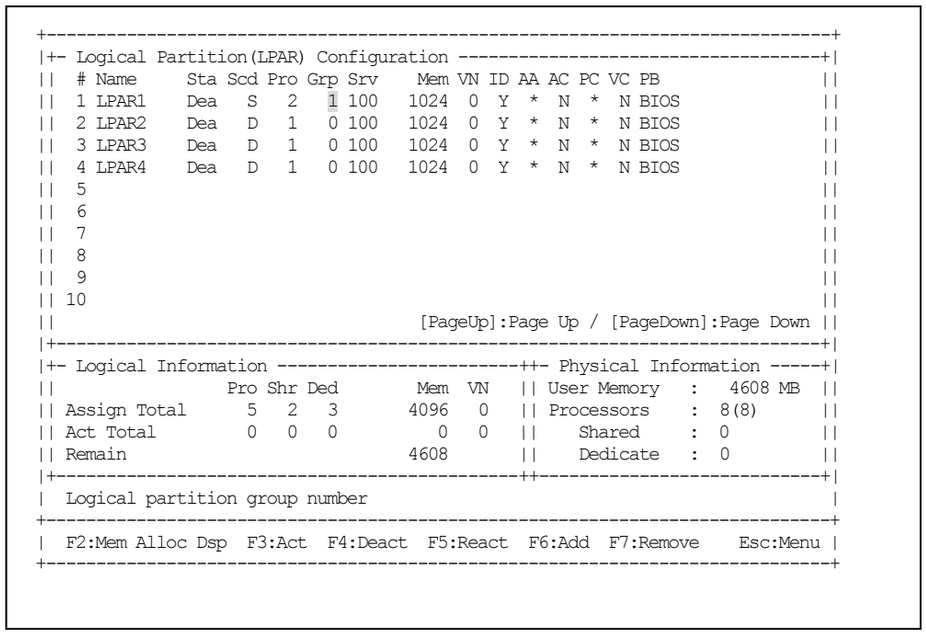
See (3) How to add a processor group and (1) How to change the number of a processor group for adding and setting a processor group number.

For: Standard sever blades with LPAR manager firmware 58-3X or later versions
High-performance server blades with LPAR manager firmware 78-3X or later versions

1. Place the cursor on **Grp** of the LPAR to change, and press **Enter**.
2. Type the number of a processor group in **Group Number Assignment** subscreen, and press **Enter**.



Example of Logical Partition Configuration (Processor group) setting

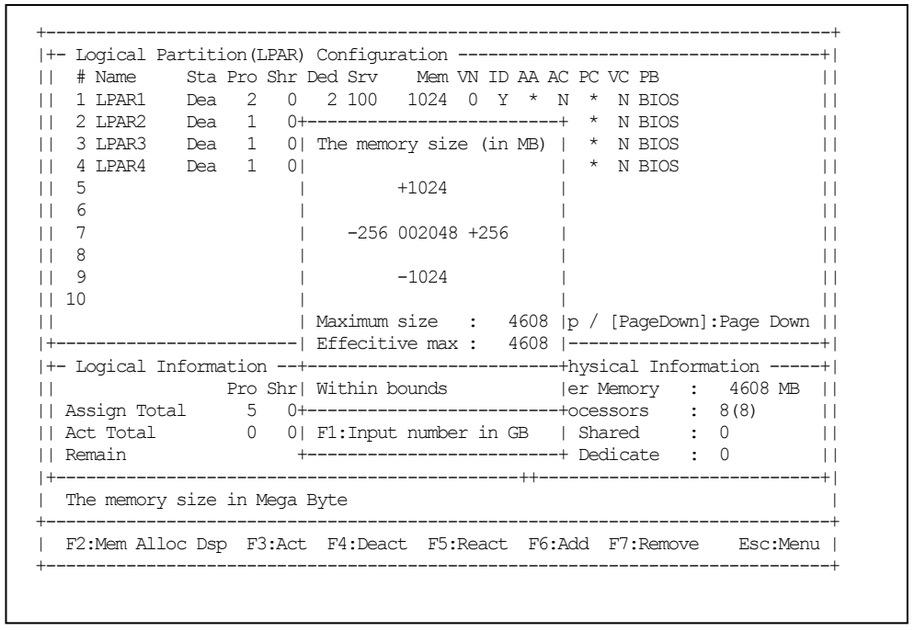


Change memory size assignment

To change the memory size to assign an LPAR, make the following settings on the Logical Partition Configuration screen.

1 Place the cursor on **Mem** of the LPAR to change, and press **Enter**.

On the **Memory Size (in MB)** subscreen, use the arrow keys ([↑], [↓], [←], [→]) to select ±1024 or ±256, determine the memory size you wish to assign, and press **Enter**.



Example of Logical Partition Configuration (memory) setting:

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ----------------------------------+|
||  # Name     Sta Pro Shr Ded Srv    Mem VN ID AA AC PC VC PB               ||
||  1 LPAR1    Dea   2   0   2 100   2048  0  Y  *  N  *  N BIOS             ||
||  2 LPAR2    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  3 LPAR3    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  4 LPAR4    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS             ||
||  5                                                                        ||
||  6                                                                        ||
||  7                                                                        ||
||  8                                                                        ||
||  9                                                                        ||
|| 10                                                                        ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+--------------------------------------------------------------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                 Pro Shr Ded        Mem  VN   || User Memory   :   4608 MB  ||
|| Assign Total      5   0   5       5120   0   || Processors    :  8(8)      ||
|| Act Total         0   0   0          0   0   ||    Shared     :  0         ||
|| Remain                           4608       ||    Dedicate   :  0         ||
|+-----------------------------------------++-----------------------------+|
|  The memory size in Mega Byte                                             |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

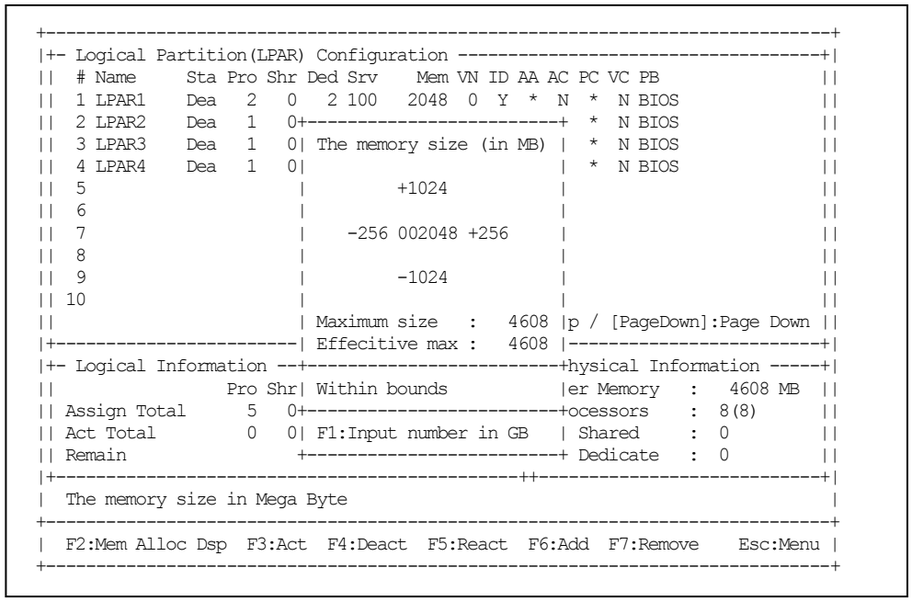


You cannot assign the memory area, which is isolated due to memory failure detected, to an LPAR.

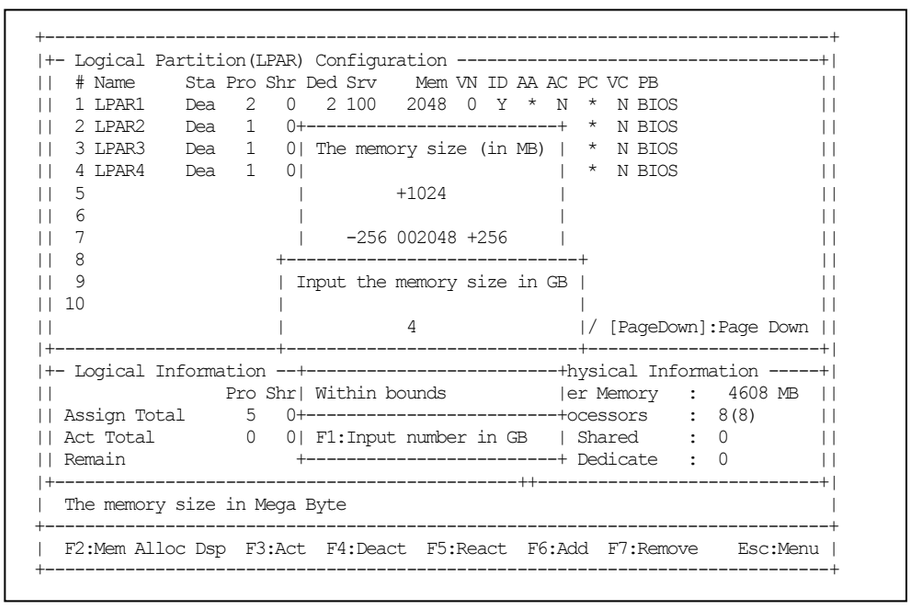
The size of the memory to be assigned to the LPAR can be specified in GB unit. The following shows an example of assigning the 4 GB memory to LPAR1:

1 Place the cursor on **Mem** for the target LPAR and press **Enter**.

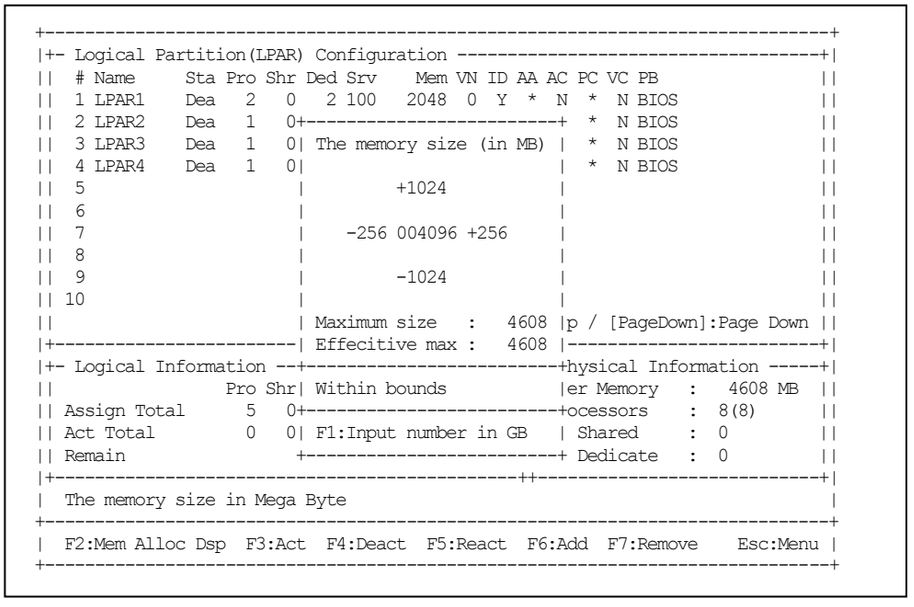
2 On the **memory size (in MB)** sub-screen, press the **F1** key.



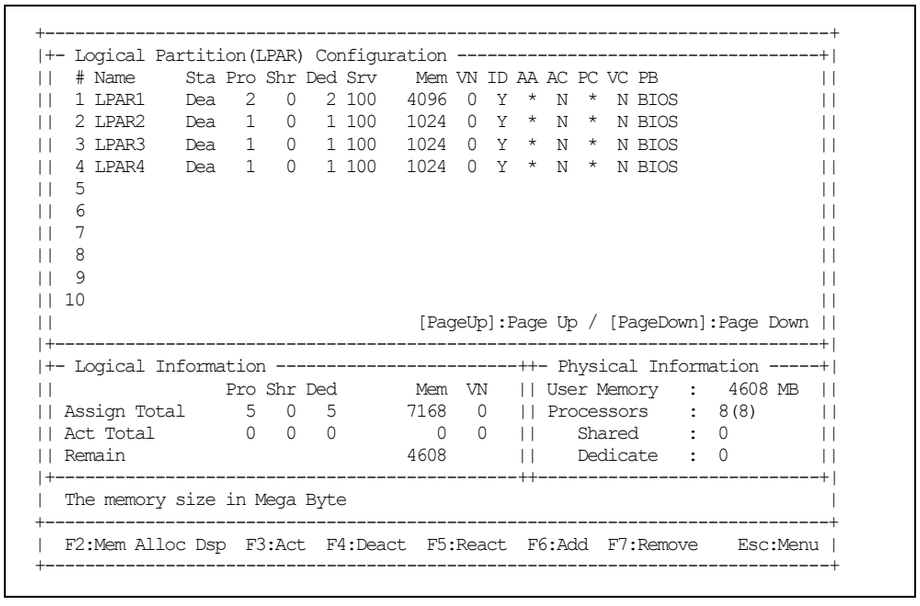
3 On the **Input the memory size in GB** sub-screen, enter the memory size in GB units and press **Enter**.



4 The memory size in **The memory size (in MB)** sub-screen is updated with the entered size in GB units. To fix the size, press **Enter**. To further modify the size in MB units, select ±1024 or ±256 and specify another size using the arrow keys ([↑], [↓], [←], [→]), and press **Enter**.



Example of Logical Partition Configuration (memory) setting:





You cannot assign the memory area, which is isolated due to memory failure detected, to an LPAR.

Set Auto Activate to LPAR

When you set Auto Activate to an LPAR, it will automatically activate once the LPAR manager initialization is complete.

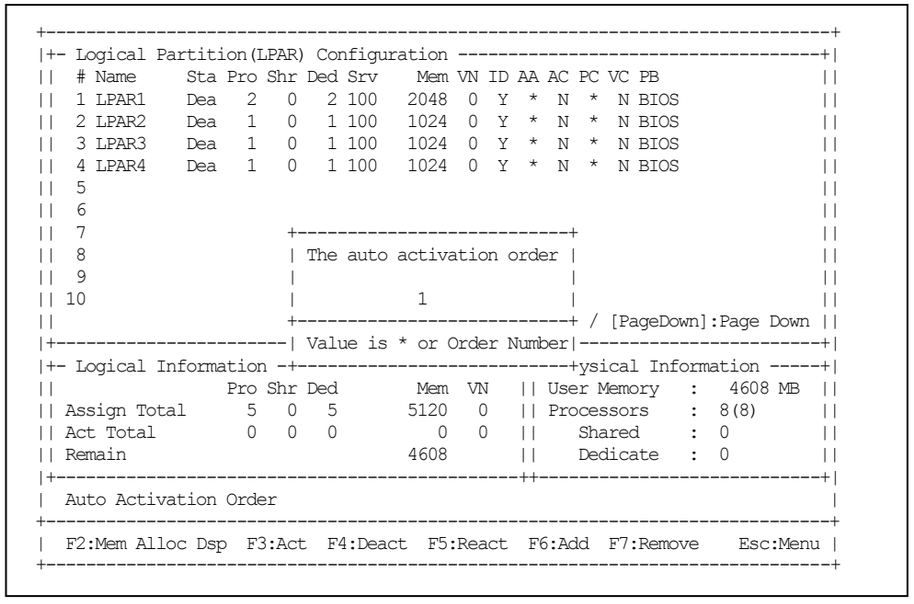
To set Auto Activate, make the AA (Order Number) setting on the **Logical Partition Configuration** screen.

❑ Setting order number to LPAR AA with Auto Activate

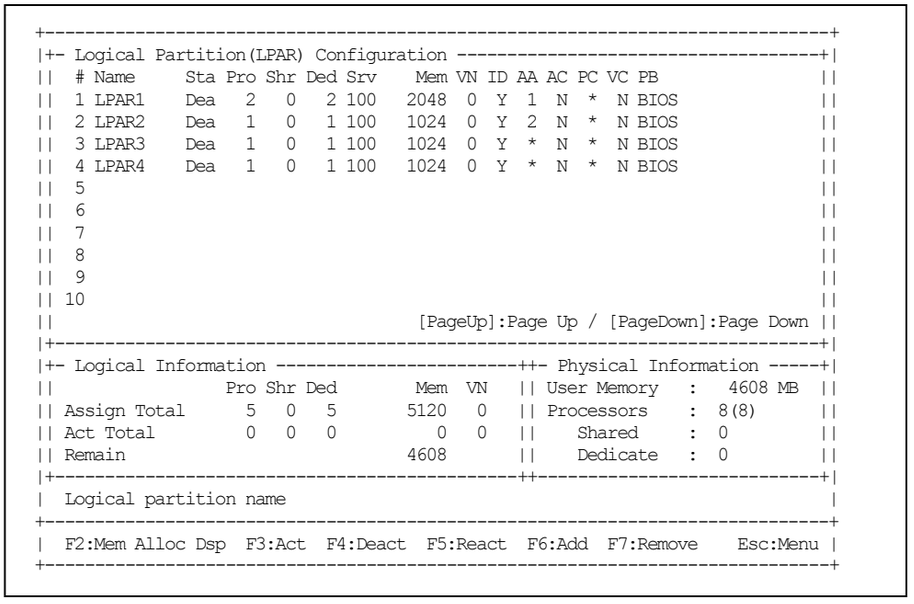
Order Number follows the order of LPARS to activate, prioritizing a smaller number.

If the same number is set to two LPAR AAs, Auto Activate is executed from the smaller LPAR number.

1. Put the cursor on the target **LPAR AA**, and press **Enter**.
2. Set Order Number on **The auto activation order** subscreen, and press **Enter**.



- Example of setting Order Number=1 to LPAR1 and Order Number=2 to LPAR2 (LPAR1 is activated first, and then LPAR2 is activated.)



❑ Canceling Auto Activate processing during operation

HVM accepts the cancellation requests for 15 seconds before starting the Auto Activate. Press and hold the **Ctrl + c** keys for a while.

Cancellation will not be accepted once Auto Activate has started.

Tip

With **Pre-State Auto Activation** Enabled, if you reboot LPAR manager without shutting down the LPAR manager system, Auto Activate will be executed to restore the LPAR to the same condition as it was before the reboot. Auto Activation Order settings are ignored in this Auto Activate. See “Options” for further details about Pre-State Auto Activation.

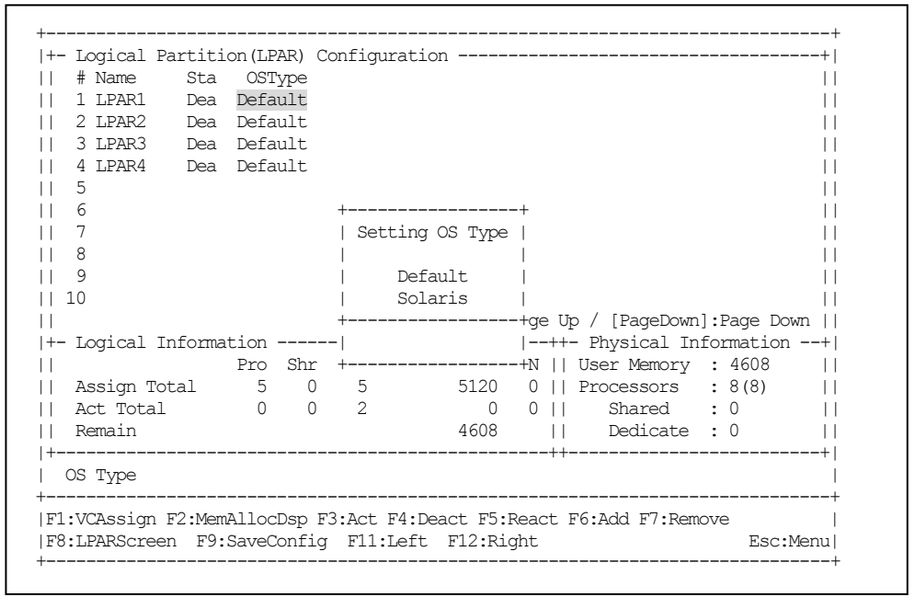
Change OS Types on LPARs

When changing the OS type on LPARs, change settings on Logical Partition Configuration screen.

For Standard server blades with LPAR manager firmware version 59-5X or later versions; For High-performance server blades with LPAR manager firmware version 79-5X or later versions

You can scroll the window to the left or right with the **F11** key or **F12** key.

Place the cursor at the intersection of a row of the target LPAR and the OS Type column, and press **Enter** to display a subscreen. Move the cursor with arrow keys: [↑] or [↓] to select Default or Solaris, and press **Enter**.



Assign PCI devices to LPARs



For Linux OS, the number of NIC ports to assign to an LPAR is limited. See Maximum Number of NIC Ports to Assign on Linux for details.

For Windows OS, the number of NIC ports to assign to an LPAR is limited. See Maximum Number of NIC Ports to Assign on Windows.

Use the **PCI Device Assignment** screen to change the PCI device scheduling mode or to assign the PCI device to an LPAR.

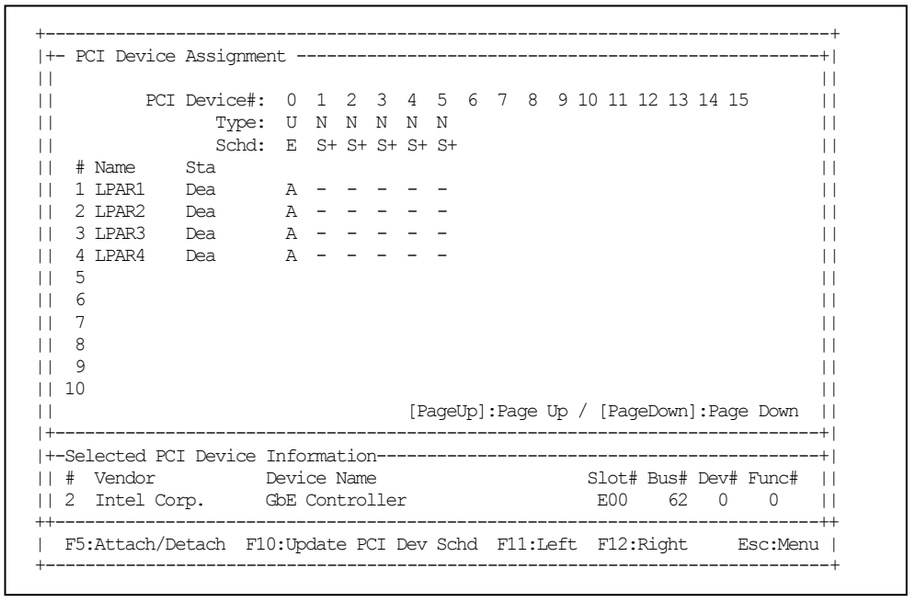
- The PCI Device Assignment screen displays information on the PCI devices installed in the server blade of the specified physical partition and inserted into the PCI Slot.
- PCI devices in the shared mode shown as “-“ whose assignment cannot be changed on this screen. See Assign VNICs (Virtual NICs) to LPARs for information about how to assign the shared NIC, and See Assign shared FCs to LPARs for information about how to assign the shared FC.
- Onboard USB ports assigned to an LPAR dedicatedly can be changed to another LPAR without stopping the LPAR. This switching is available only for the USB port of the primary server blade.

❑ Changing the scheduling mode of the PCI device

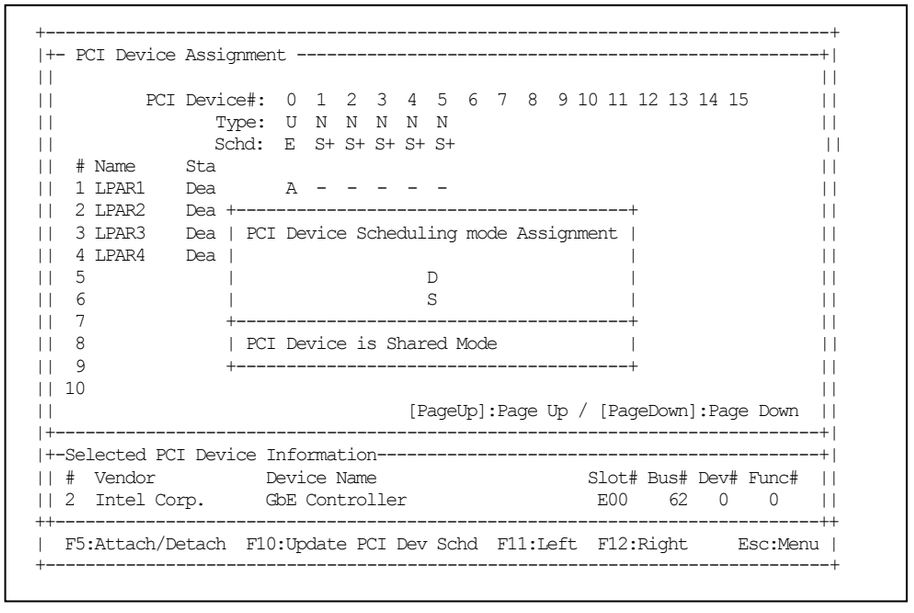
Use the procedure shown below to change the scheduling mode of the PCI device.

Note that all LPARs must be deactivated when you change the scheduling mode.

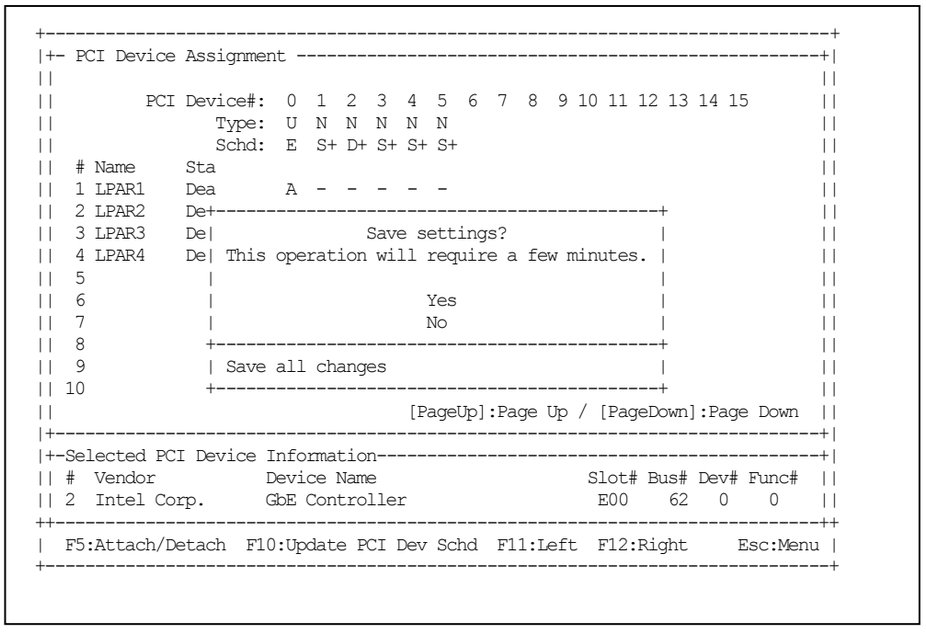
1 On the **PCI Device Assignment** screen, place the cursor at **Schd** of the PCI device whose scheduling mode is to be changed and press **Enter**.



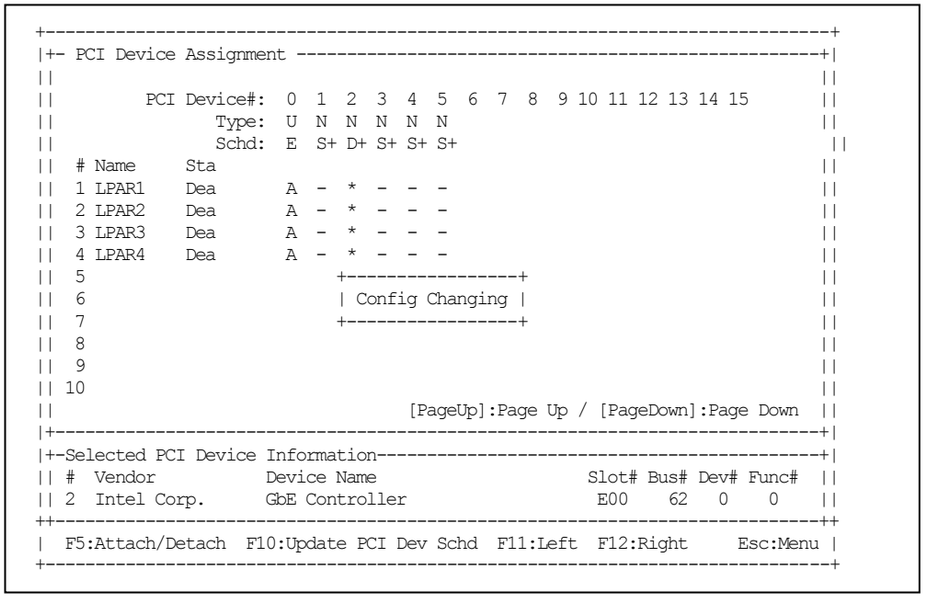
2 On the **PCI Device Scheduling mode Assignment** subscreen, select **D** (dedicated mode) or **S** (shared mode), and press **Enter**.



3 Reflect the changed scheduling mode of the PCI device into the LPAR manager system. Press the **F10** key to display the **Save settings?** subscreen. Select **Yes** and press **Enter**.



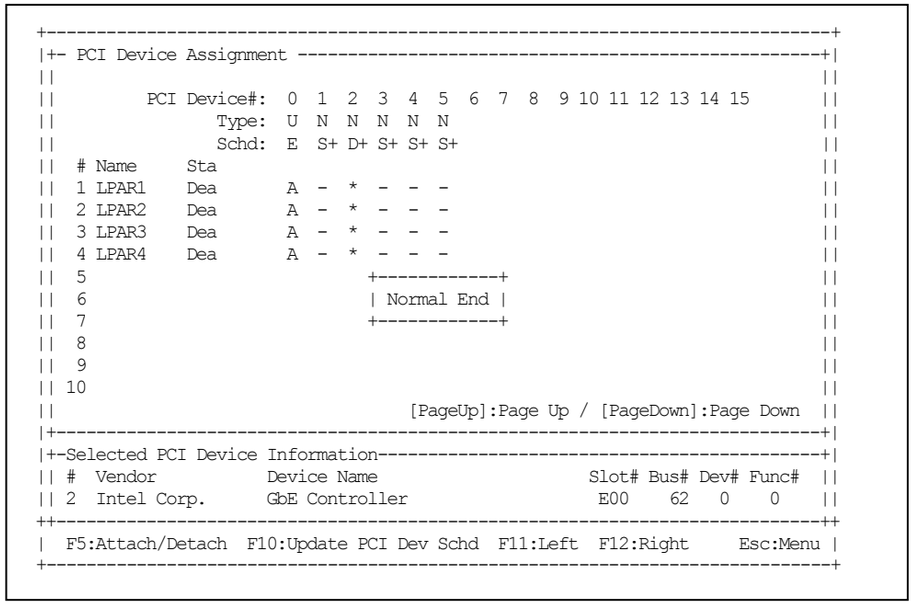
4 After a couple of minutes, the **Config Changing** message appears.





When the port status of a shared FC is LinkDown, it takes a different time required for changing the scheduling mode of a PCI device depending on the number of ports with LinkDown. See Shared FC port status for details.

5 The Normal End subscreen appears, which completes the changing of the scheduling mode.

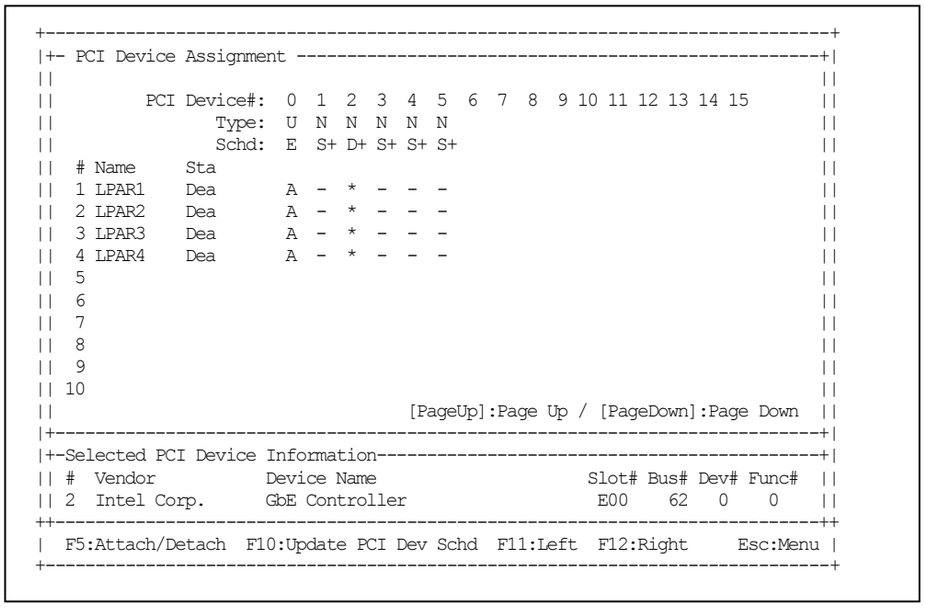


❑ Assigning the PCI device to an LPAR

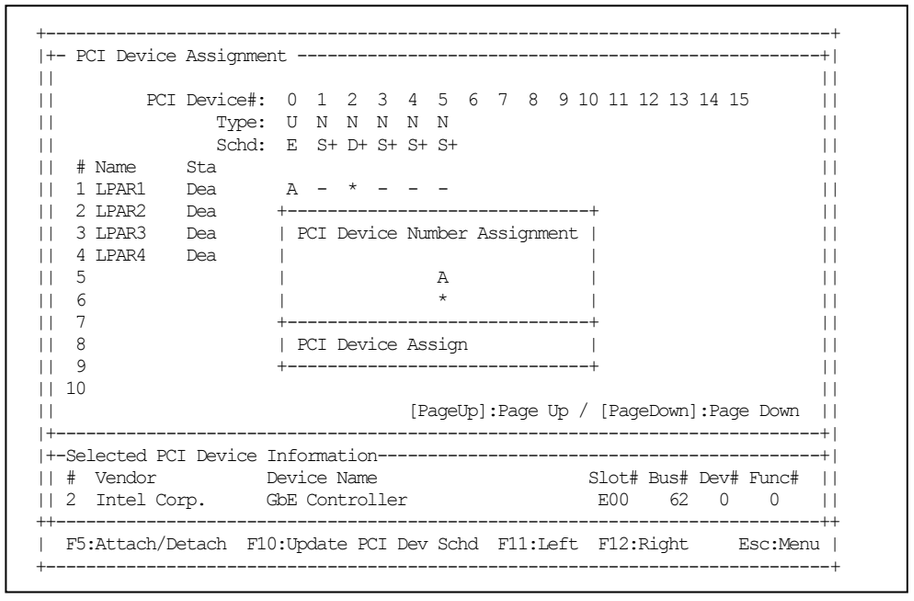
Use the following procedure to assign the PCI device to an LPAR.

Deactivate the LPAR to which the PCI device is assigned.

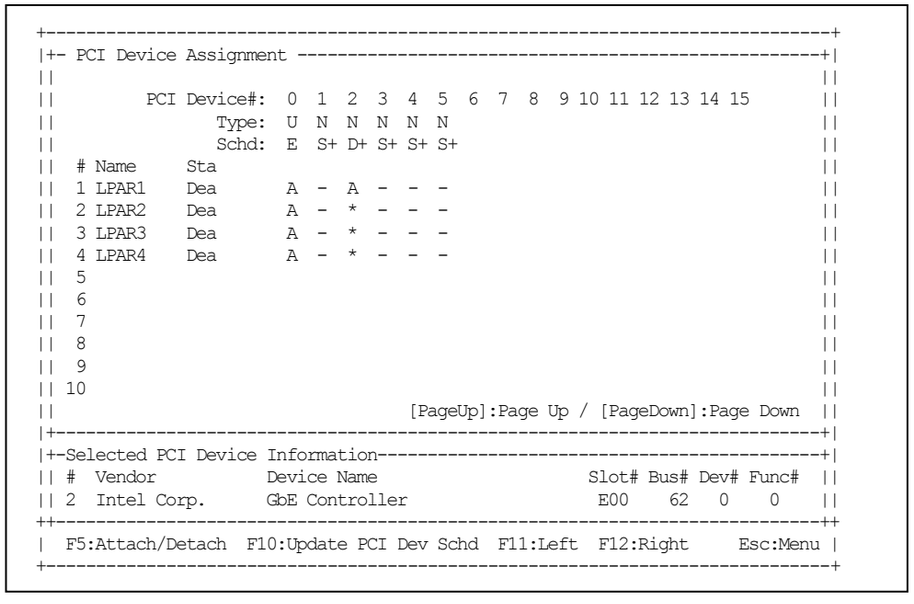
1 Place the cursor on the PCI device of the LPAR to which that device is assigned and press **Enter**.



2 On the **PCI Device Number Assignment** subscreen, select **A** (assignment) or *(unassignment) and press **Enter**.



■ Example of PCI Device Assignment setting



* Assignment can be specified for multiple LPARs. However, only LPAR activated first can actually use the PCI device. For another LPAR to use the PCI device used by the LPAR activated first, deactivate the LPAR using that PCI device and then activate another LPAR.

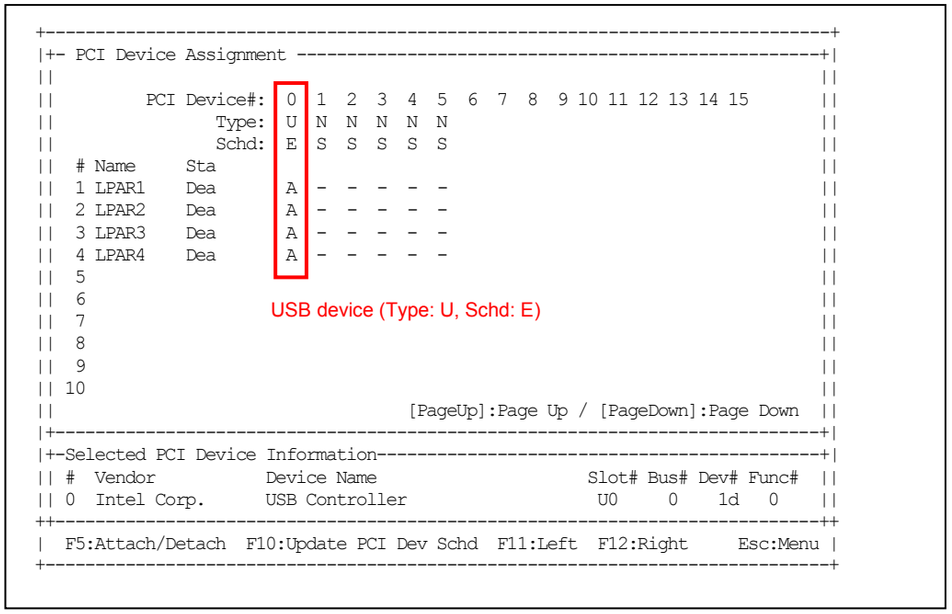
Assign USB devices to LPARs

The USB device is exclusively used by the active LPAR to which that device is assigned with no assignment mode. Moreover, if the USB device is in the exclusively-shared mode, its assignment can be dynamically changed without deactivating operation among multiple active LPARs that are activated after that USB device is assigned.

❑ Assigning USB devices to LPARs

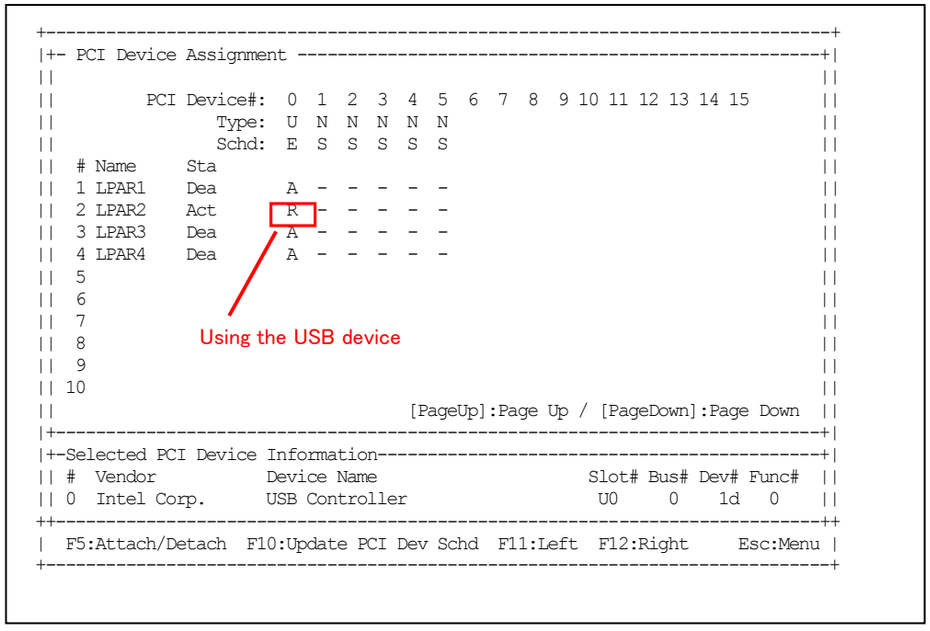
Assign a USB device on the PCI Device **Assignment** screen. **E** is displayed in the Schd field for the USB device used in the exclusively-shared mode as shown below.

Deactivate the LPAR to assign the USB device. A USB device can be assigned to multiple LPARs as other PCI devices.



When an exclusively-shared USB device is assigned to multiple LPARs, the LPAR activated first can use the USB device and the other LPARs activated later cannot use it. To change LPARS to use the USB device, execute the procedure to change LPARs that is described later in this manual.

On the **PCI Device Assignment** screen, **R** is shown as the assignment status for the active LPAR actually using the exclusively-shared USB device.



❑ Attaching/detaching the USB device

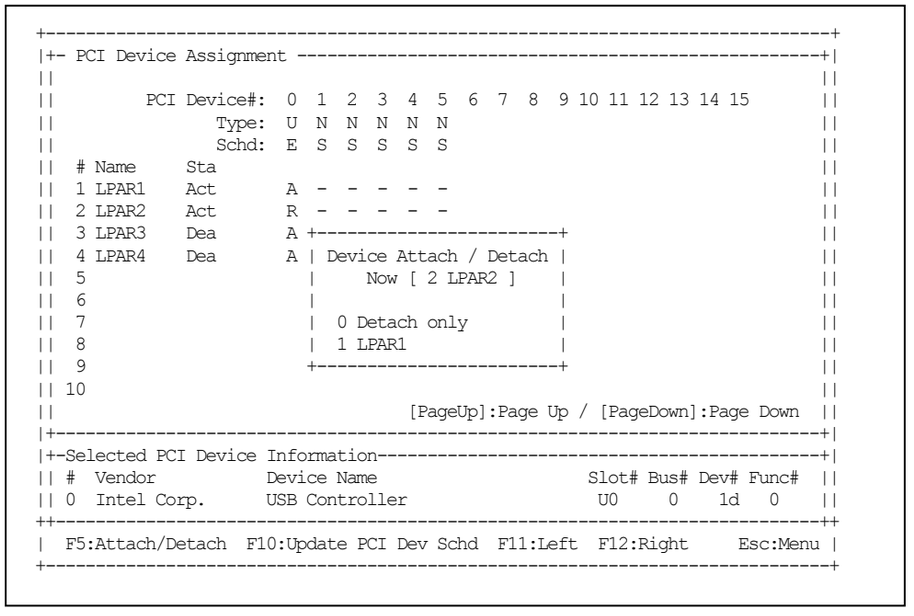
1. Move the cursor to the USB device column on the **PCI Device Assignment** screen, and press **F5: Attach/Detach**.
2. The USB Device **Attach and Detach** subscreen will be displayed. Follow the screen message to select a number.

   When the new LPAR number is entered, the USB device will be attached to the selected LPAR: Attach. If the USB device is being attached to another LPAR at the time, the USB device will be detached from the LPAR: Detach and attached to the newly selected LPAR.

   When '0: Detach only' is selected, the USB device will be simply detached from the LPAR.

Tip

After the attachment operation, it might take about 30 seconds until the USB device becomes available on the firmware or OS in the LPAR.



Assign remote consoles to LPARs

Assign a remote console to an LPAR in the same way as the USB device assignment.

Connecting the LPAR to which the USB device is assigned via remote console, you can operate the guest OS.

To change the remote console connection to another guest OS, assign the USB device to that destination.

As changing the USB device assignment, the remote console assignment is changed.

For further details, see Assign USB devices to LPARs.



- When connecting via remote console, the remote console screen display or mouse operation might become slower due to Super Video Graphics Array (SVGA) emulation.
- When the USB device is assigned to another guest OS, it might take about 30 seconds before you can operate the keyboard and mouse.
- When transferring from the Basic environment to LPAR manager environment, the screen might not be displayed with the remote console connection. For further details, see Migration between basic environment and LPAR manager environment.



Since remote console connection gives graphic processing overhead on the LPAR, the assigned performance declines a bit. When executing application that requires performance, detach it from the LPAR.

Assign VNICs (Virtual NICs) to LPARs



For Linux OS, the number of NIC ports to assign to an LPAR is limited. See Maximum Number of NIC Ports to Assign on Linux.

For Windows OS, the number of NIC ports to assign to an LPAR is limited. See Maximum Number of NIC Ports to Assign on Windows.

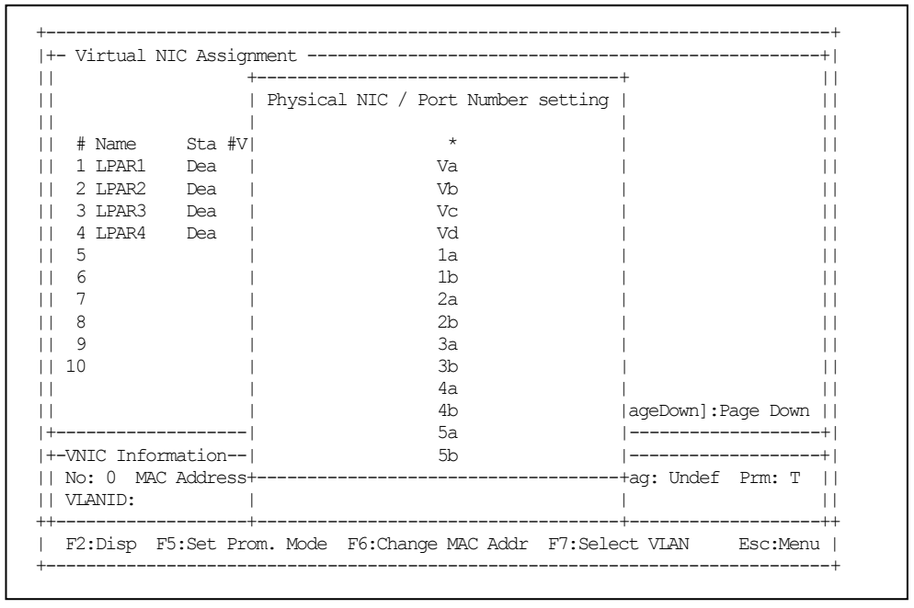
Assign a virtual NIC on the **Virtual NIC Assignment screen**. Deactivate the LPAR to assign the virtual NIC.

1 Place the cursor on **Virtual NIC Number** of the LPAR to which the virtual NIC is to be assigned and then press **Enter**.

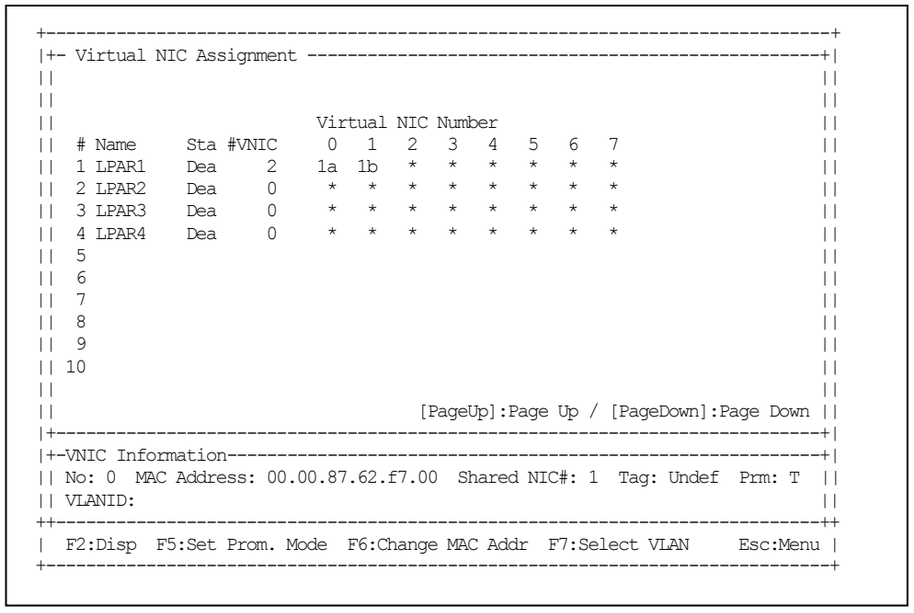
```
+-------------------------------------------------------------------------------+
|+- Virtual NIC Assignment ------------------------------------------------+|
||                                                                          ||
||                                                                          ||
||                           Virtual NIC Number                             ||
||  # Name     Sta #VNIC     0   1   2   3   4   5   6   7                  ||
||  1 LPAR1    Dea      0    *   *   *   *   *   *   *   *                  ||
||  2 LPAR2    Dea      0    *   *   *   *   *   *   *   *                  ||
||  3 LPAR3    Dea      0    *   *   *   *   *   *   *   *                  ||
||  4 LPAR4    Dea      0    *   *   *   *   *   *   *   *                  ||
||  5                                                                       ||
||  6                                                                       ||
||  7                                                                       ||
||  8                                                                       ||
||  9                                                                       ||
|| 10                                                                       ||
||                                                                          ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+-------------------------------------------------------------------------+|
|+-VNIC Information-------------------------------------------------------+|
|| No: 0  MAC Address: 00.00.87.62.f7.00  Shared NIC#: 0  Tag: Undef  Prm: T  ||
|| VLANID:                                                                  ||
++-------------------------------------------------------------------------++
|  F2:Disp  F5:Set Prom. Mode  F6:Change MAC Addr  F7:Select VLAN     Esc:Menu |
+-------------------------------------------------------------------------+
```

2 In the **Physical NIC/Port Number setting** subscreen, select the virtual NIC type (1a, 1b, and so on) to be specified and press **Enter**.

For more on virtual NIC types, see Overview of virtual NIC functions.



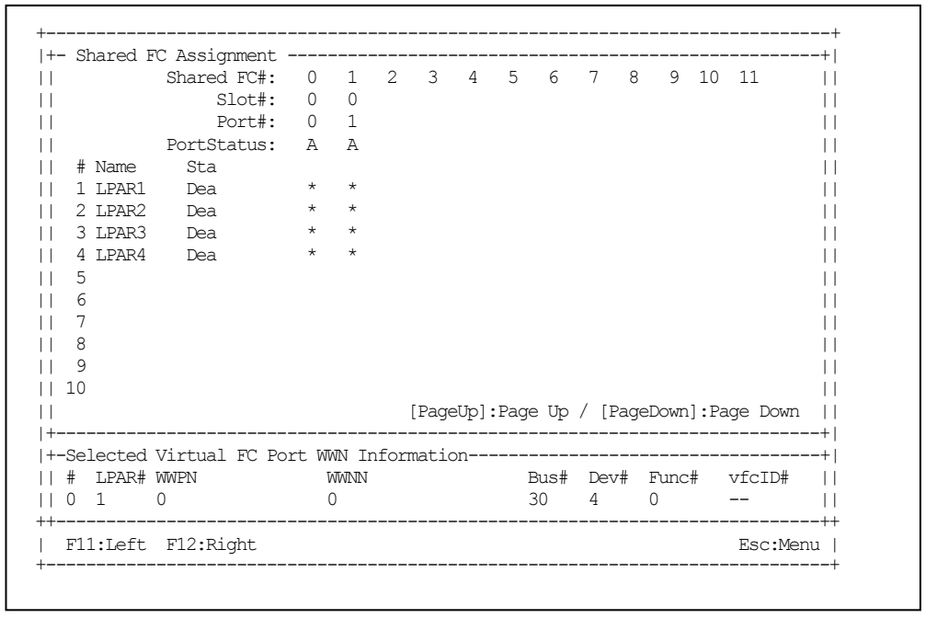
■ Example of Virtual NIC Assignment setting



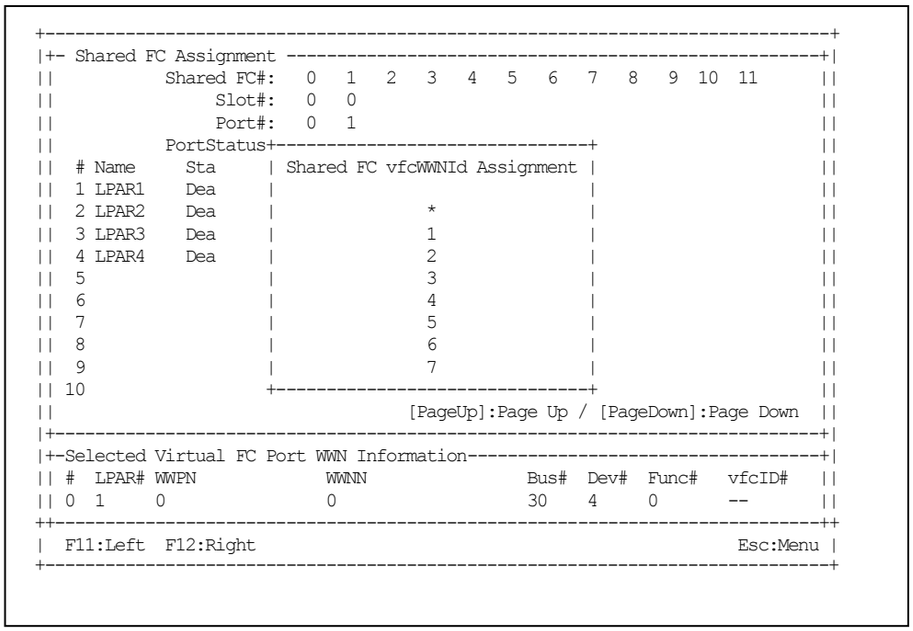
Assign shared FCs to LPARs

Follow the steps below to assign a shared FC adapter to an LPAR. Deactivate the LPAR before assigning the shared fibre channel (FC).

1. Change the FC adapter to be used to the shared mode. See Changing the scheduling mode of the PCI device for how to change the mode. If the FC adapter is already in the shared mode, skip this step.
2. Assign the shared FC to the LPAR on the **Shared FC** Assignment screen. Place the cursor on the Shared FC# to assign to the LPAR, and press **Enter**.



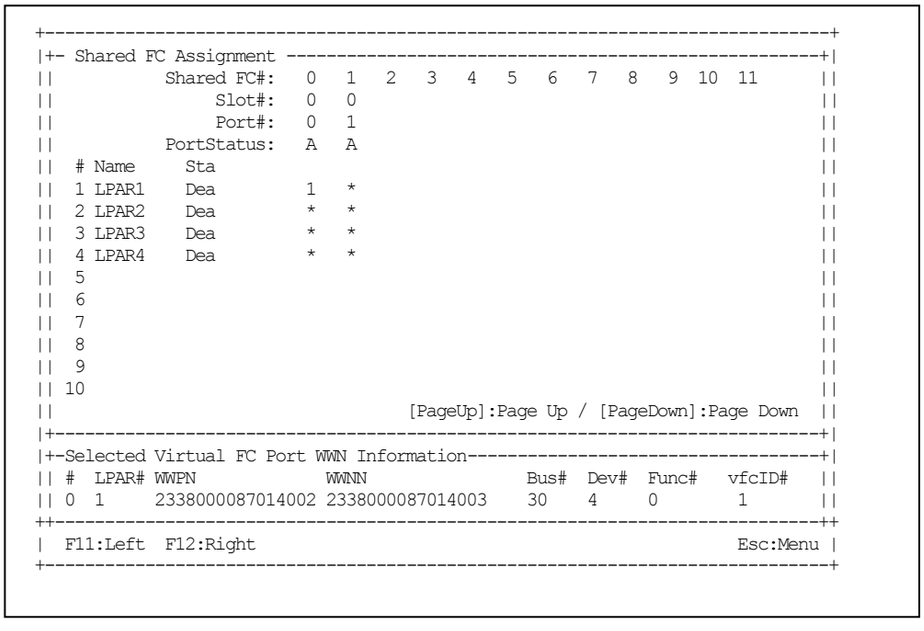
3 When the **Shared FC vfcWWNId Assignment** subscreen is displayed, select **vfcID** and press **Enter**.



Tip

- vfcID can be selected from the range for each port shown in the subscreen. However, the same vfcID# cannot be set for multiple LPARs. For details of vfcID, see “(1) world wide port name (WWPN)/world wide node name (WWNN) for a Shared FC”.
- Displayed values might be different depending on adapters installed.

Example of Shared FC Assignment setting

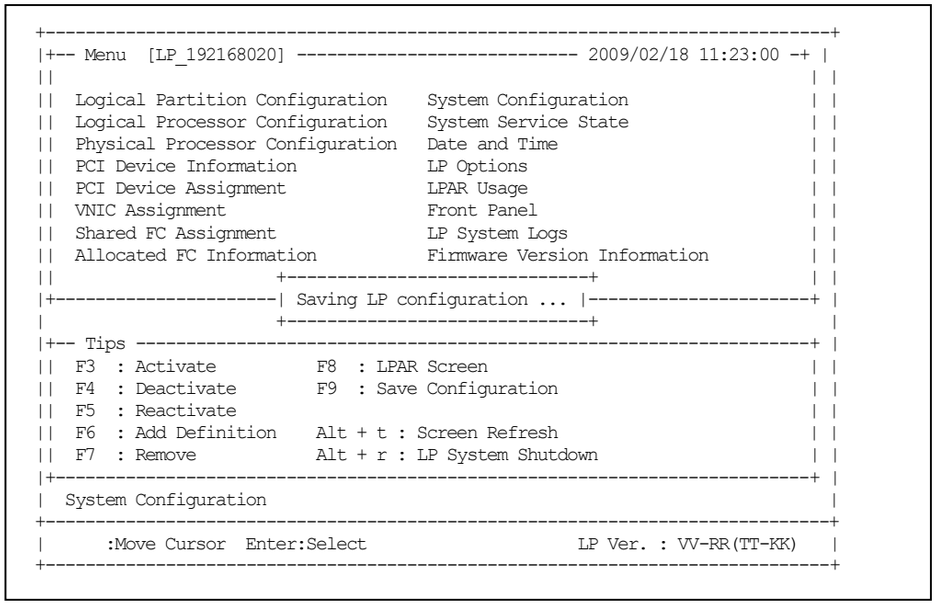


Save configuration changed on LPAR manager screen

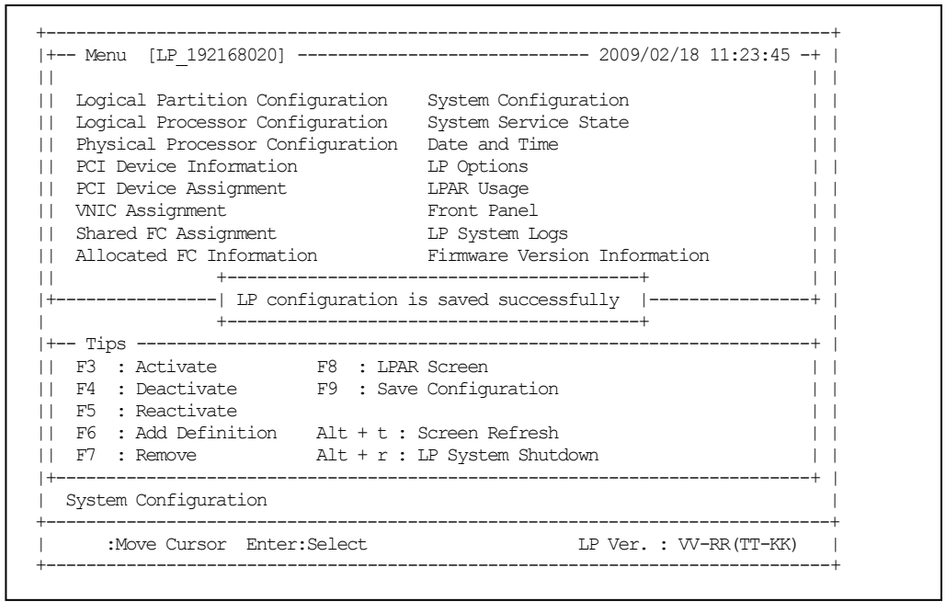
To save settings you have made or changed on LPAR manager screens, go to the **LPAR manager Menu** screen and press **F9: Save Configuration**. The guest timer settings changed on the guest OSs also need to be saved by **F9** after the change before the LPAR manager shutdown or reboot; otherwise, the changed values might be lost.

Example of pressing **F9: Save Configuration** on the LPAR manager Menu screen:

A subscreen is displayed, showing that LPAR manager configuration is being saved.



When the new configuration has been saved successfully, a message “LP configuration is saved successfully” is displayed.



* Saving the contents set on the LPAR manager screen, the LPAR manager will boot with the saved configuration reflected at the next boot.



Time required for **F9: Save Configuration** increases depending on the number of defined LPARs. It usually finishes in a minute. When a heavy load is on the LPAR manager, it might take several minutes for saving.

Guest OS operation

Boot the guest OS

This section describes how to activate an LPAR and how to boot the OS.

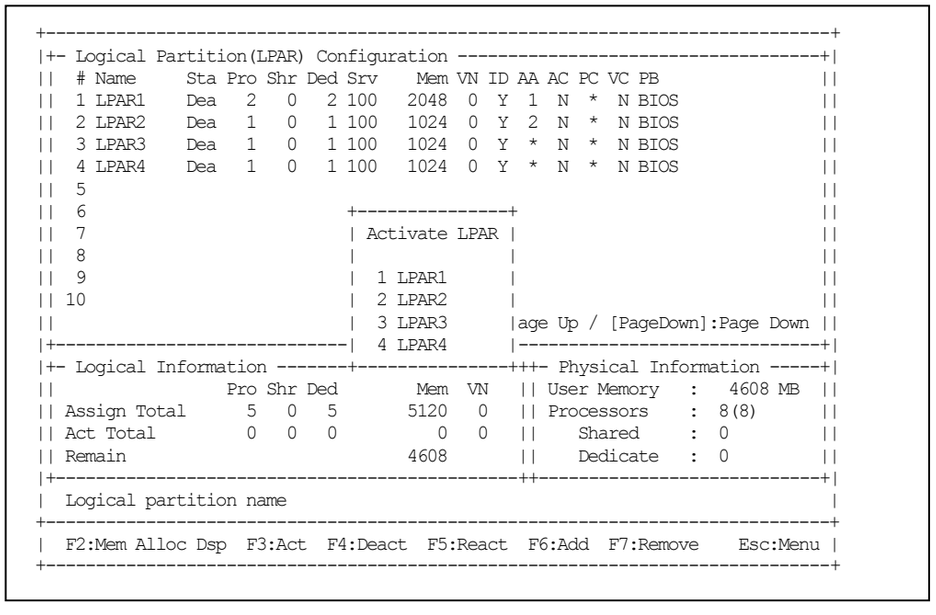
❑ Assigning USB device

1 Check if a USB device is assigned. If the USB device has been assigned, skip this step. See Assign USB devices to LPARs.

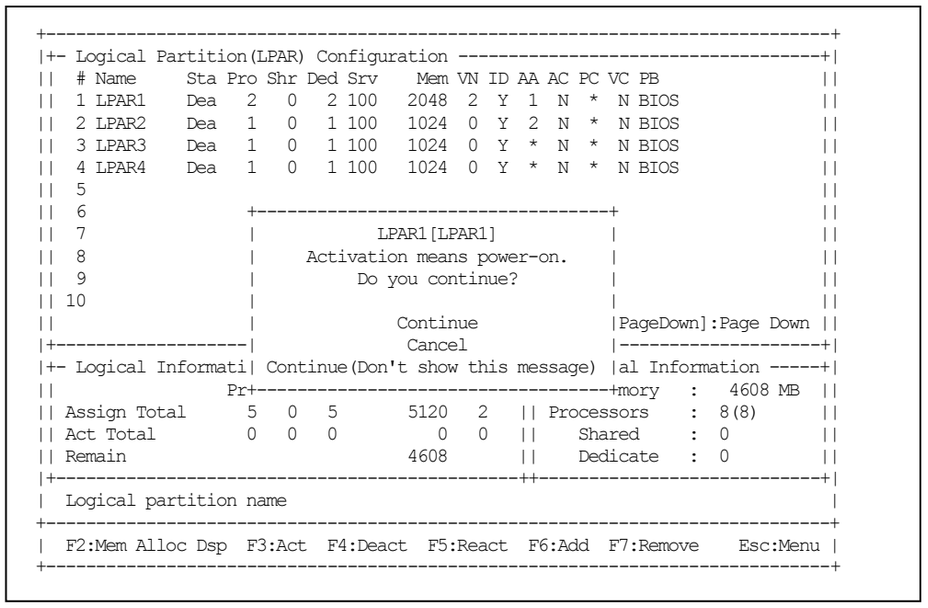
❑ Activating LPARs

1 On the **Logical Partition Configuration** screen, press **F3: Activate**.

2 On the **Activate LPAR** subscreen, select an LPAR to activate, and press **Enter**.



3 When a subscreen to confirm **Activate: power on** is displayed, select **Continue** and press **Enter**.





- The screen above might not be displayed depending on the Activation setting on the Options screen. See Options for details.
- If the guest screen is displayed improperly and freezes after the LPAR is activated, display the LP System Logs screen to check if “LP-LFW detected internal error.” exists in LP system logs. If the log exists, contact your reseller or maintenance personnel.

4 Activating the LPAR makes the USB device in use. Then connecting to the LPAR via the remote console, you can operate the guest OS. See “Remote Console Connection” for details about connection.



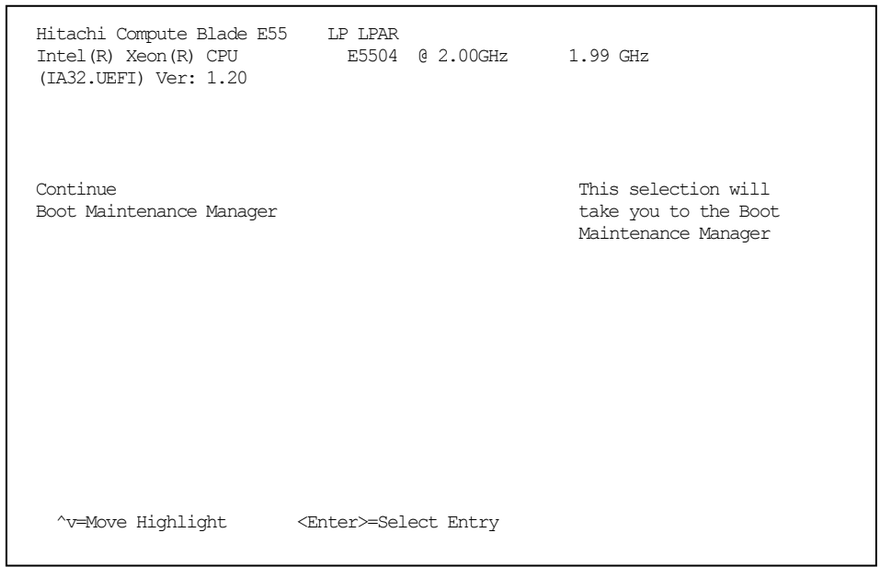
If another LPAR is using the USB device, the first activated LPAR can connect to the remote console. The latter activated LPAR cannot connect to the remote console. To allow the latter activated LPAR to connect to the remote console, it is necessary to change the USB assigned destination.

❑ Setting the extensible firmware interface (EFI) driver

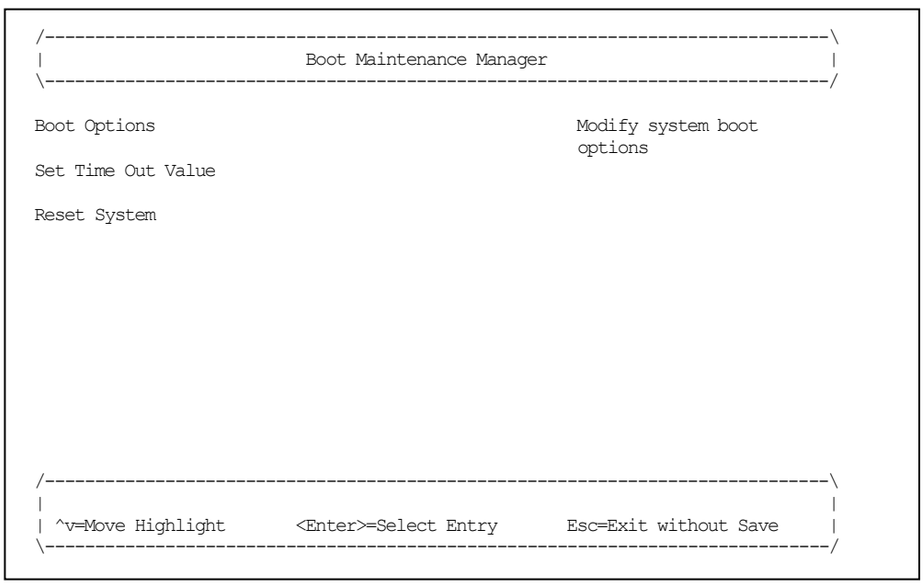
Before booting a guest OS, set the EFI driver from EFI Shell. When you have already set the EFI driver, skip this section.

Make sure to configure to boot a guest OS as follows: booting from a designated disk in normal operation; booting from the compact disc Read Only Memory (CD-ROM) in OS installation; Preboot eXecution Environment (PXE) boot (network boot) when using ServerConductor (SC)/Deployment Manager (DPM).

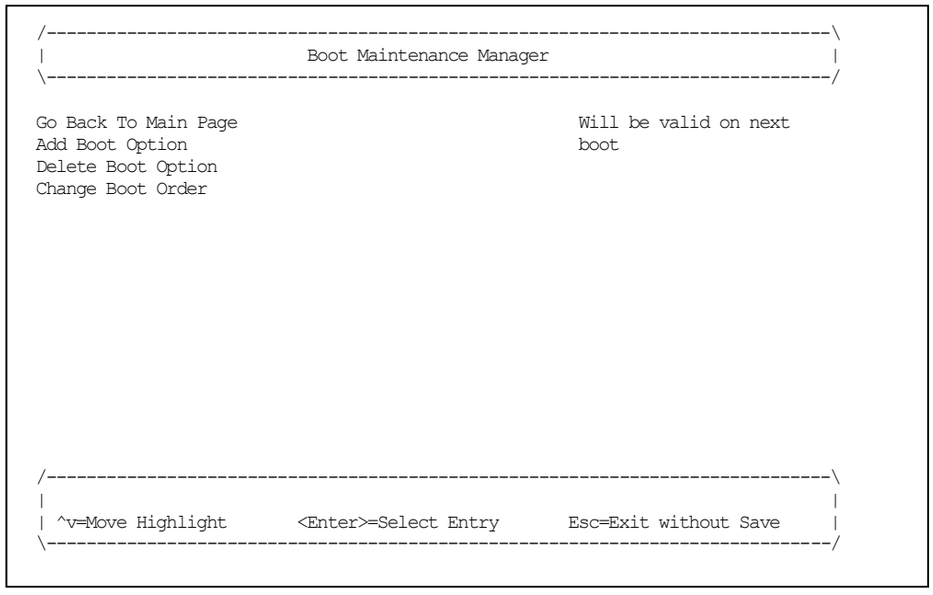
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.



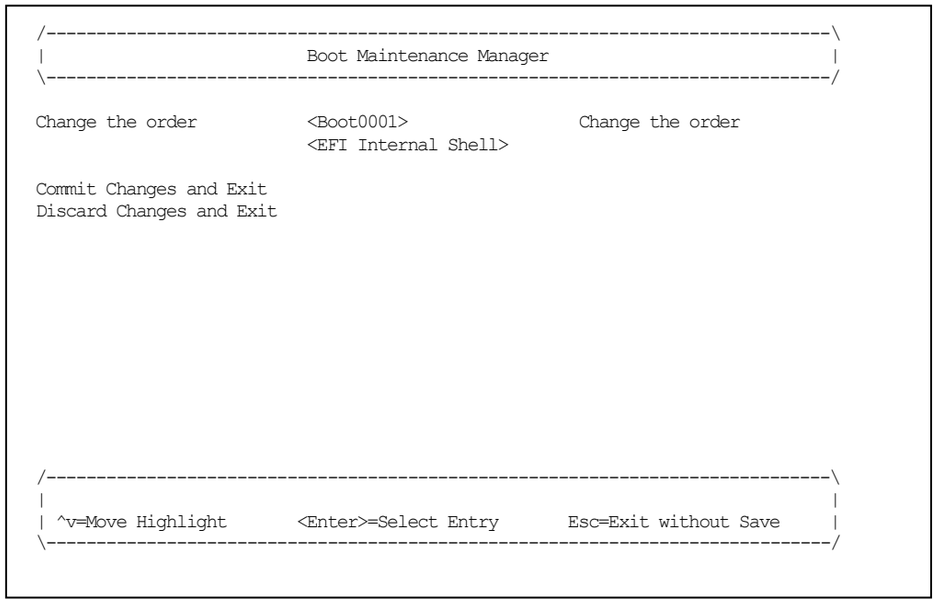
3 Select **Change Boot Order**.



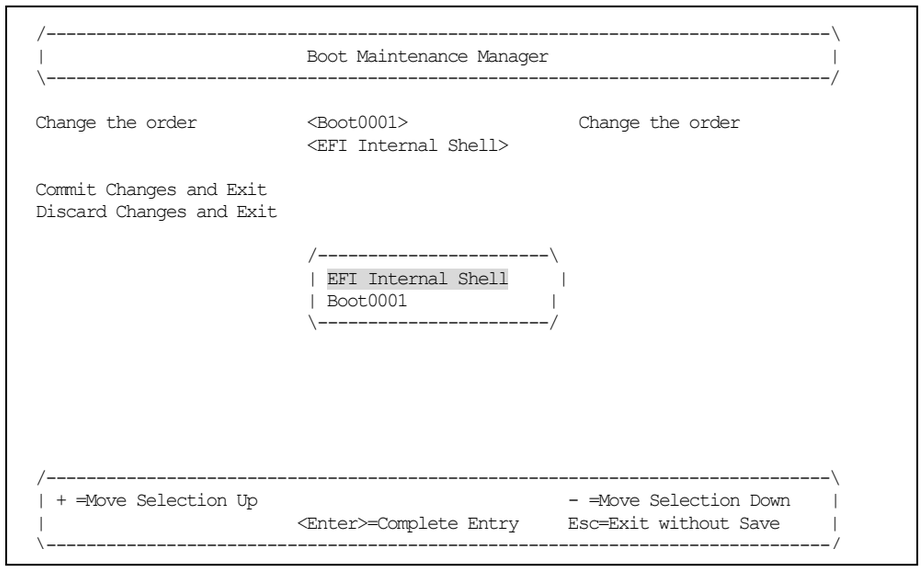
4 When **EFI Internal Shell** is displayed on the top of the boot order, **Change Boot Order** is unnecessary.

Select **Discard Changes and Exit** and then go to the step 8.

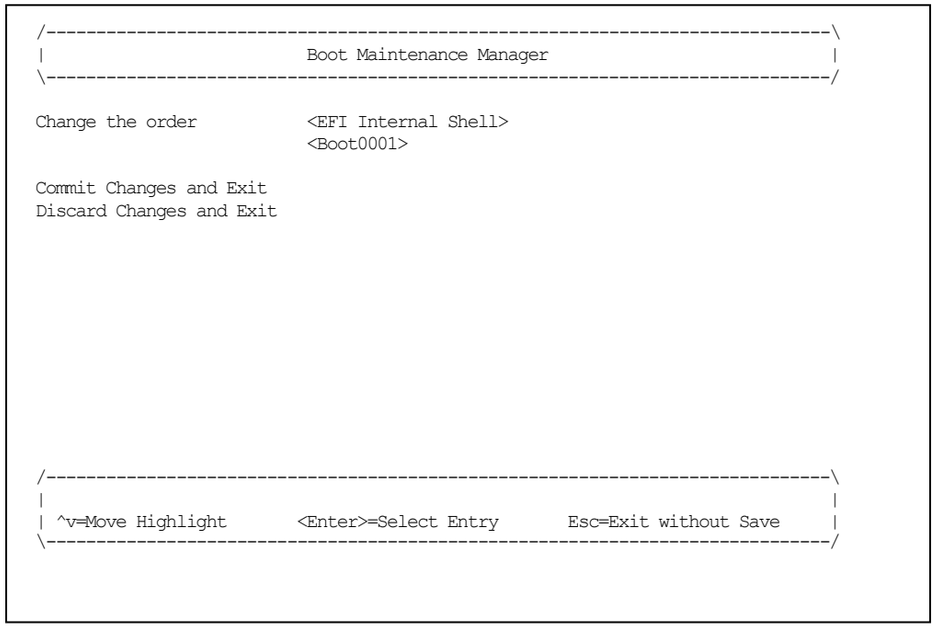
5 When **EFI Internal Shell** is not displayed on the top of the boot order, select **Change the order**.



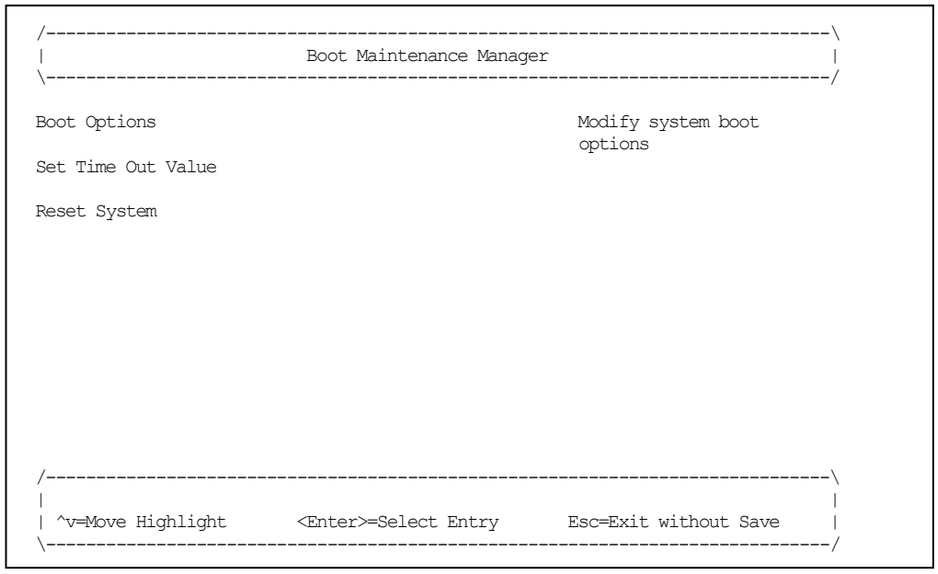
6 When a subscreen is displayed, press the **[+] or [-]** key to top the **EFI Internal Shell** in the boot order.



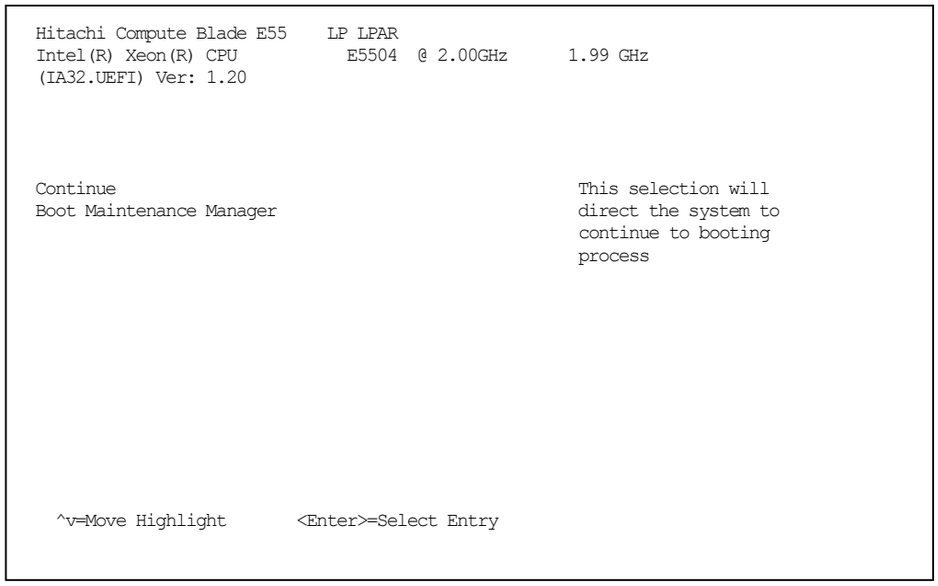
7 Select **Commit Changes and Exit**.



8 When the **Boot Maintenance Manager** screen is displayed again, press **Esc** to show the screen at the logical basic input/output system (BIOS) boot.



9 Select **Continue** on the screen displayed at the logical BIOS boot.



See ‘EFI Driver’ in the *HITACHI Gigabit Fibre-channel Board User’s Guide (BIOS/EFI Edition)*” for further details about the EFI driver.

10 Enter the **drivers** command to find out the driver handle of “HITACHI Fibre-channel Driver”

```
Shell> drivers
            T   D
D           Y C I
R           P F A
V  VERSION  E G G #D #C DRIVER NAME                    IMAGE NAME
== ======== = = = == == ================================ ==================
:
65 01010001 D X -  1  - Hitachi Fibre channel Driver    EFIdriver
:
Shell>
```

The handle is “65” in the example above.

11 Enter `drvcfg` [driver handle] to find out the controller handle.

```
Shell> drvcfg 65
Configurable Components
  Drv[65]  Ctrl[74]  Lang[eng]
Shell>
```

The controller handle is “74” in the example above.



When multiple FC ports are assigned, multiple results are displayed. There is no problem if you select a controller handle between those displayed,

12 Enter `drvcfg –s` [driver handle] [controller handle].

hfccfg> prompt is displayed.

```
Shell> drvcfg -s 65 74
Set Configuration Options
  Drv[65]  Ctrl[74]  Lang[eng]
hfccfg>
```

13 Enter the `select` command and select an adapter for booting.

```
hfccfg> select
 HBA FC Port List:
     Num  Bus  Dev Func  current WWPN      original WWPN
     ---  ---  --- ----  ----------------  --------------
       1 - 09   04   01  XXXXXXXXXXXXXXXX
       C - cancel
 Select Number ---> 1
```

Select “1” in the example above.

14 When the prompt is displayed, enter the **set** command and set each item.

Set the following items:

- Boot Function: **Enabled**
- Select Boot Device: **Enabled**
- Boot Device List: Set WWPN and LUN number, which is usually “0” because LU0 is commonly LU for booting, for ports that the target eternal disk array uses.

Set other necessary items for your system environment.

Set other necessary items for your system environment.

```
hfccfg.XXXXXXXXXXXXXXX>set
   Base Settings:
    ** Boot Function = Disabled
       change? (y/[n]) -->y
           0 - Disabled -[default]
           1 - Enabled
           c - cancel
        please select -->1
    ** Connection Type = Auto Detection
       please Enter -->
    ** Data Rate = 4Gbps
       please Enter -->
    ** Spinup Delay = Disabled
       change? (y/[n]) -->
    ** Login Delay Time = 3sec
       change? (y/[n]) -->
    ** Persistent Bindings = Enabled
       change? (y/[n]) -->
    ** Force Default Parameter for adapter driver = Disabled
       change? (y/[n]) -->
    ** Select Boot Device = Disabled
       change? (y/[n]) -->y
           0 - Disabled -[default]
           1 - Enabled
           c - cancel
        please select -->1
    ** << Boot Device List >> (LUN:decimal)
           1 - WWPN:0000000000000000  LUN:0000
           2 - WWPN:0000000000000000  LUN:0000
           3 - WWPN:0000000000000000  LUN:0000
           4 - WWPN:0000000000000000  LUN:0000
           5 - WWPN:0000000000000000  LUN:0000
           6 - WWPN:0000000000000000  LUN:0000
           7 - WWPN:0000000000000000  LUN:0000
           8 - WWPN:0000000000000000  LUN:0000
       change? (y/[n]) -->y
       please select a number(1-8,c(cancel)) -->1
      ** List#1: WWPN:0000000000000000 LUN:0000
           1 - Scan Target
           2 - Manual setup
           3 - Clear this list
           c - cancel
         please select -->1
       ===> Target port serching... please wait
       ===> Target port serch End.
         << Target Device List >>
            1 - D-ID:090C00  WWPN:XXXXXXXXXXXXXXXX  HITACHI   DF600F
            c - cancel(return to <<Boot Device List>>)
         select a Target for Boot Device. (1-xx, c): 1
         *** #1: D-ID:090C00  WWPN:XXXXXXXXXXXXXXXX is selected ***
            1 - Scan Lun
            c - cancel(return to <<Target Device List>>)
         please select -->1
         << LUN List (decimal)>>
            1 - LUN : 0000
            c - cancel(return to <<Target Device List>>)
         select a LUN for Boot Device. (1-xx, c): 1
         *** List#1 new WWPN and LUN ***
              WWPN : XXXXXXXXXXXXXXXX
              LUN  : 0000
         Update List#1 ? (y/[n]) -->y
```

```
        List#1 update end
 ** << Boot Device List >> (LUN:decimal)
         1 - WWPN:XXXXXXXXXXXXXXXX  LUN:0000
         2 - WWPN:0000000000000000  LUN:0000
         3 - WWPN:0000000000000000  LUN:0000
         4 - WWPN:0000000000000000  LUN:0000
         5 - WWPN:0000000000000000  LUN:0000
         6 - WWPN:0000000000000000  LUN:0000
         7 - WWPN:0000000000000000  LUN:0000
         8 - WWPN:0000000000000000  LUN:0000
     change? (y/[n]) -->n
Base Settings is completed
```

15 When settings are completed, enter the **save** command to save the settings.

16 Use the **exit** command to return to the EFI Shell.

17 Execute the **reconnect –r** command, and then enter the **map –r** command. Confirm that the target LU is listed next to the Fibre and its WWN is correct.

```
Shell> reconnect -r
ReconnectController(X,X,X) : Status = Success

Shell> map -r
Device mapping table
  fs0   :Removable BlockDevice - Alias XXXX blk0
  blk0  :Removable BlockDevice - Alias XXXX fs0
  blk1  :BlockDevice - Alias (null)

Acpi(PNP0A08,0)/Pci(4|0)/Pci(0|2)/Pci(4|1)/Fibre(WwnXXXXXXXXXXXXXXXX, Lun0)
  Blk2  :Removable BlockDevice - Alias XXXX fs0
    :
Shell>
```

Displayed details are different depending on the environment.

18 Confirm the settings and then enter the **exit** command.

❑ Creating Boot Options

You need to create Boot Options for your purpose. If you already created one, ignore this subsection. Boot Option of EFI Shell is created by default.

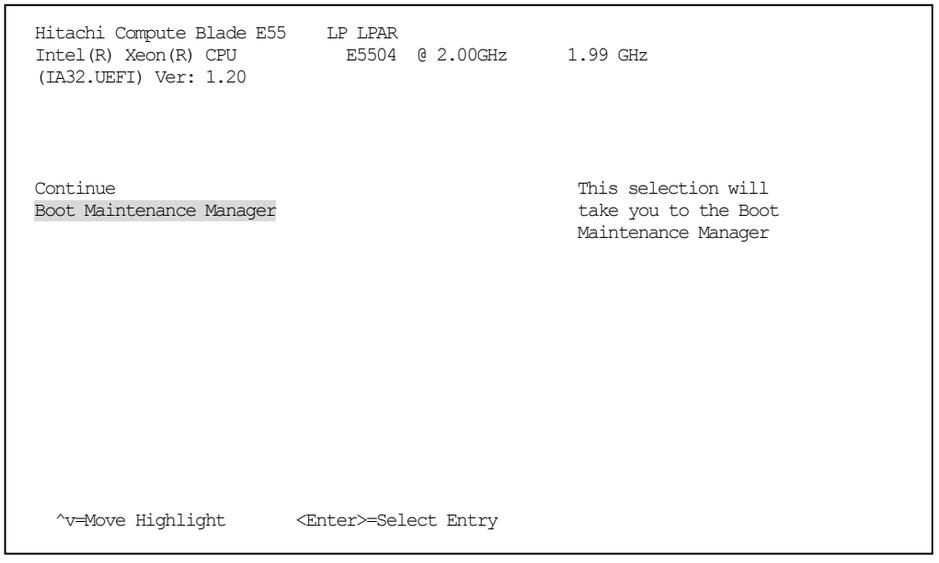
Boot option example	Device	Boot type	Application
EFI Internal Shell	-	EFI Shell boot	EFI driver settings
Windows	FC STORAGE DEVICE	Guest OS boot	Guest OS is booted.
CD/DVD	USB STORAGE DEVICE	CD/DVD boot	CD/DVD is used.
DPM	NETWORK BOOT DEVICE	PXE boot	SC/DPM is used.

Note

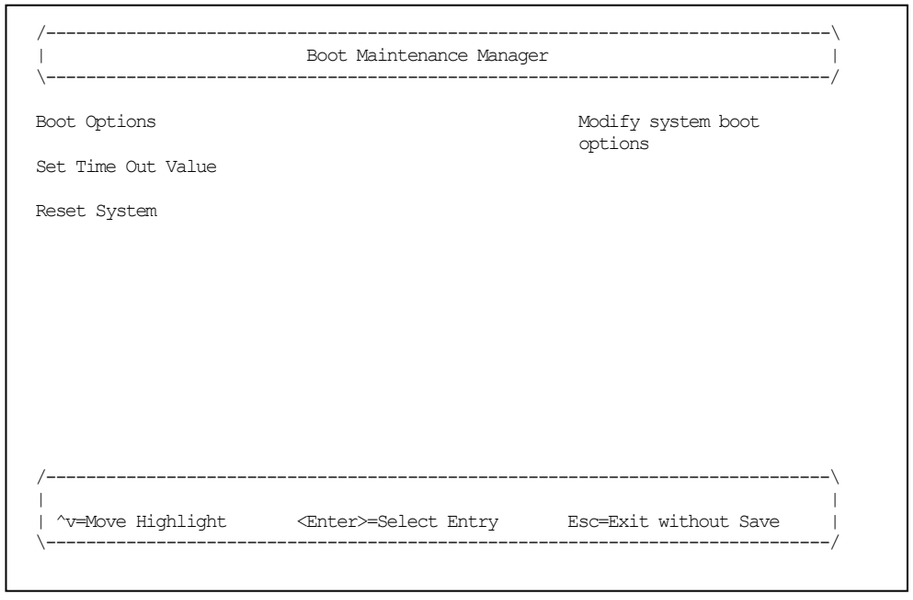
Do not create multiple boot options for a boot device. If you do, the boot device might not boot up properly.

Guest OS Setup

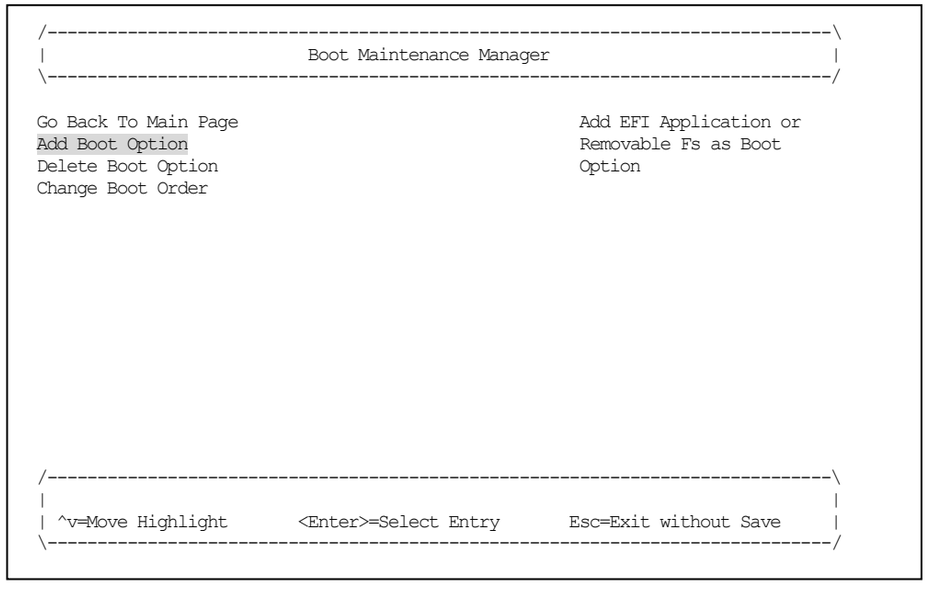
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.



3 Select **Add Boot Option**.



4 When **File Explorer** is displayed, select a device to configure**.**

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E8010433B00,0x0)]
USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x1,0x0)/MAC(00008762
F730,0x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x2,0x0)/MAC(00008762
F731,0x0)]



/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

5 Select **Input the description**.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E801025A260,0x0)]

Input the description      _
Input Optional Data        _

Commit Changes and Exit
Discard Changes and Exit

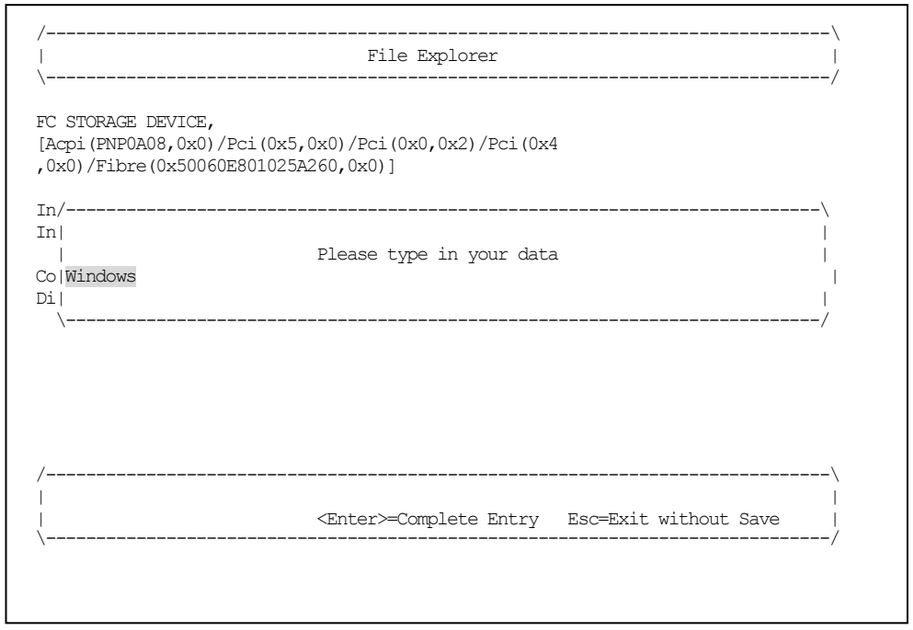






/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

6 Type the device name.

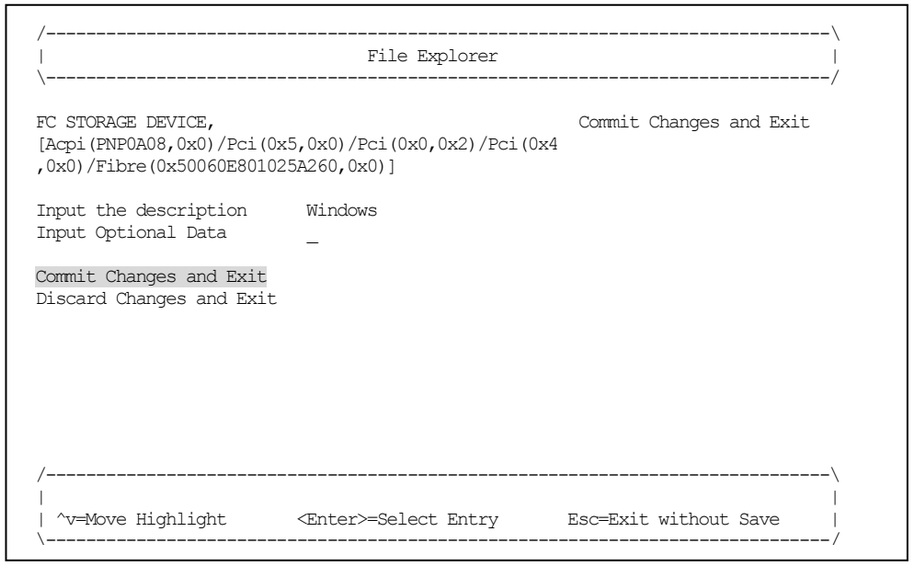


Tip

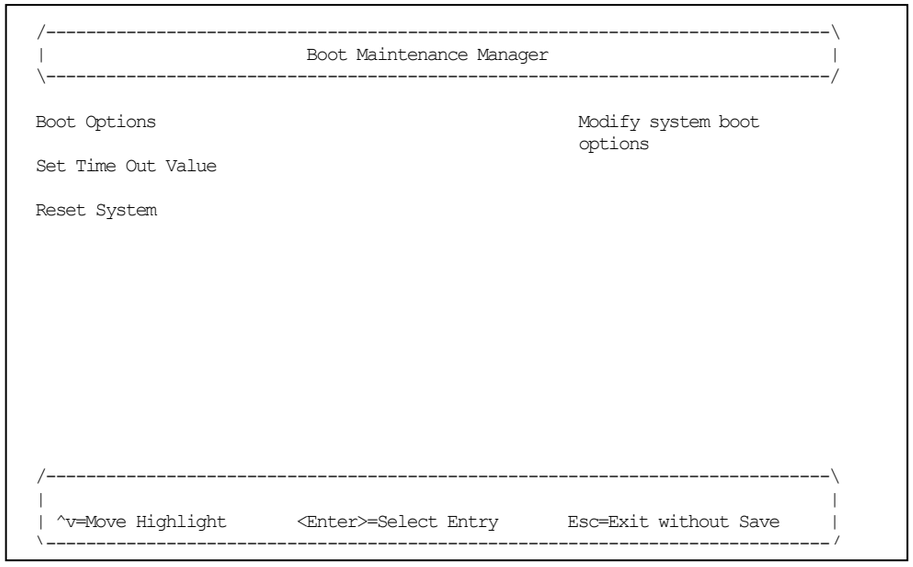
You can use the number of characters from 2 up to 75. The following characters are available.

Alphanumerics; symbols: !"#$%&'()=~|{}_?*`+><,./¥:];[@^-

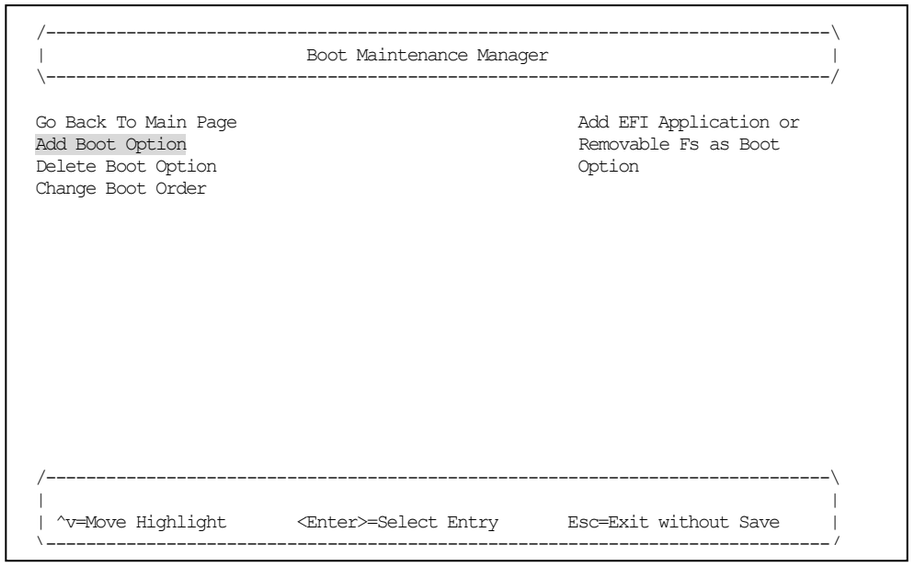
7 Select **Commit Changes and Exit**.



8 On **Boot Maintenance Manager**, select **Boot Options**.



9 Select **Add Boot Option**.



10 When **File Explorer** is displayed, select a device to create.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E8010433B00,0x0)]
USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x1,0x0)/MAC(00008762
F730,0x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x2,0x0)/MAC(00008762
F731,0x0)]




/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```



If `USB STORAGE DEVICE` is not displayed, connect a CD/DVD drive to the server blade and insert the OS media.

11 Select **Input the description**.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]

Input the description       _
Input Optional Data         _

Commit Changes and Exit
Discard Changes and Exit



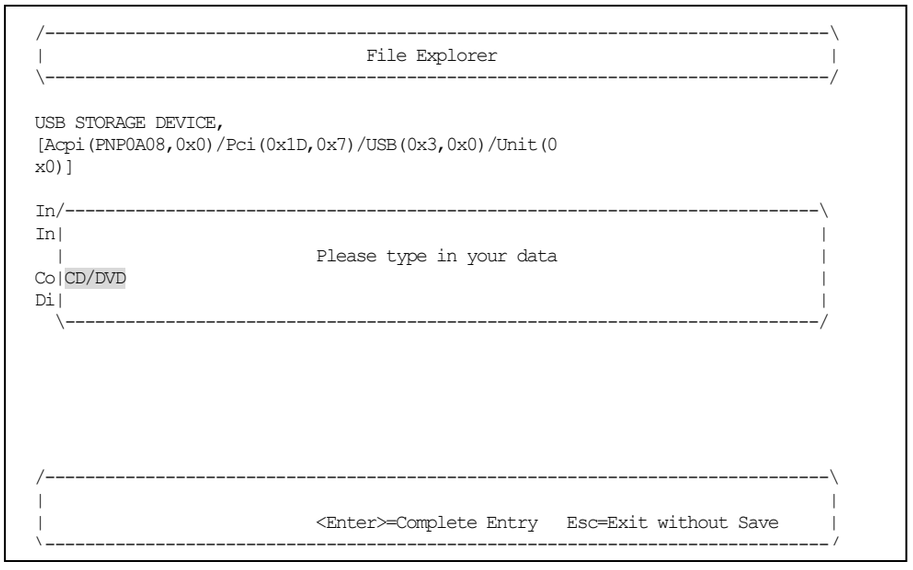






/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

12 Type the device name.

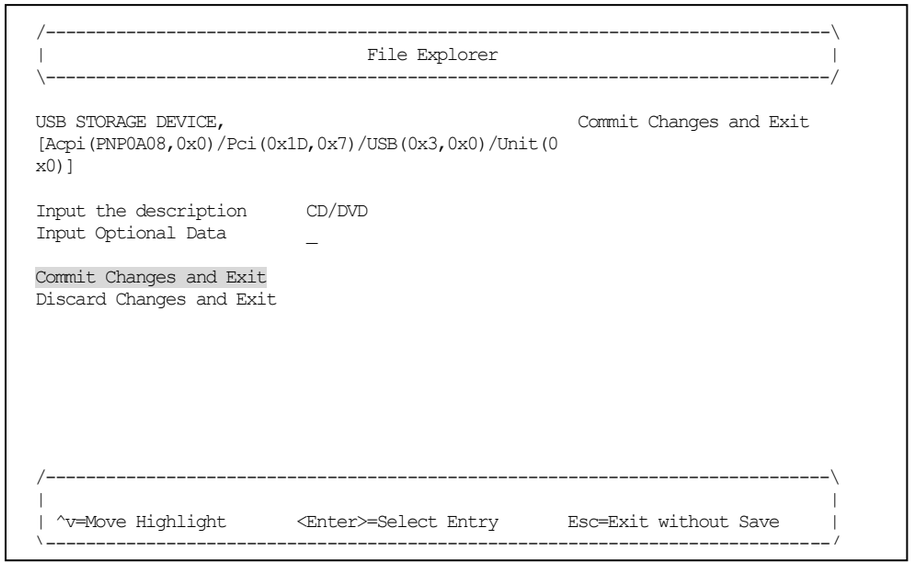


Tip

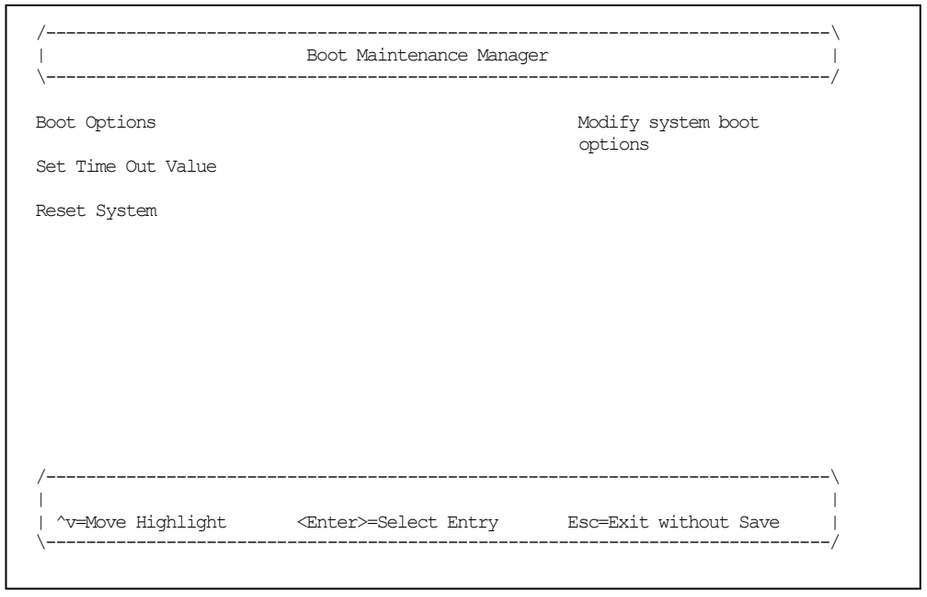
You can use the number of characters from 2 up to 75. The following characters are available.

Alphanumerics; symbols: !"#$%&'()=~|{}_?*`+><,./¥:];[@^-

13 Select **Commit Changes and Exit**.



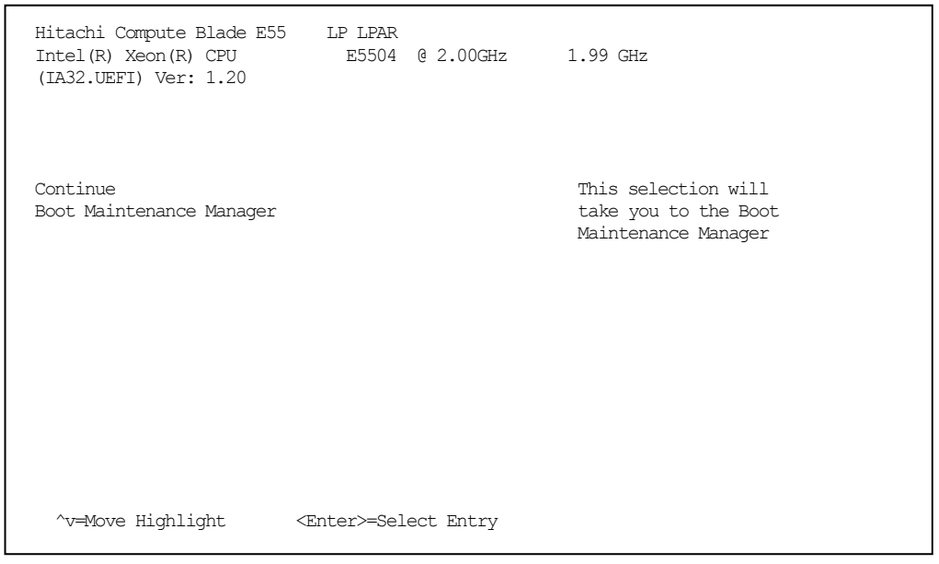
14 When **Boot Maintenance Manager** is displayed, press **Esc**.



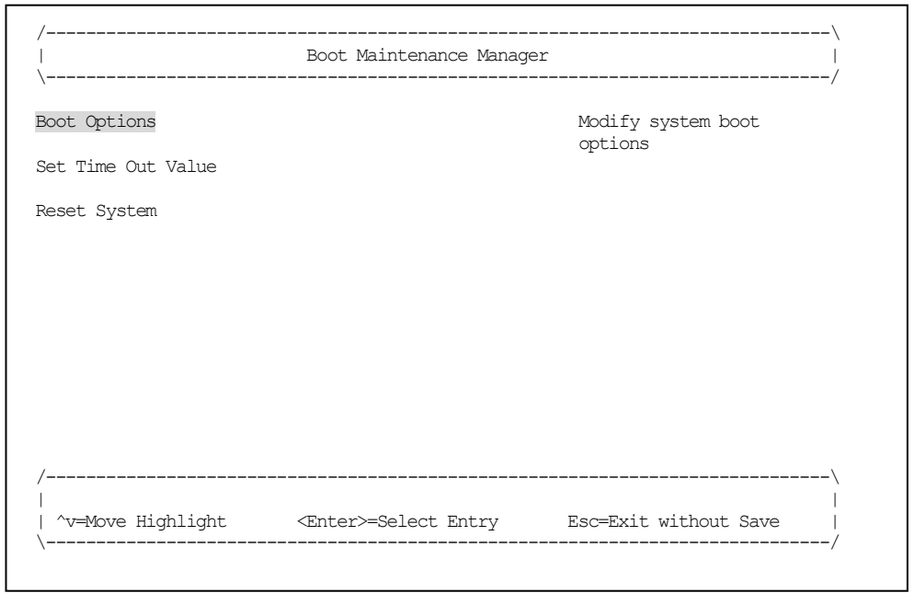
Go to Guest OS Setup in Changing Boot Orders to execute the procedure.

Guest OS Boot

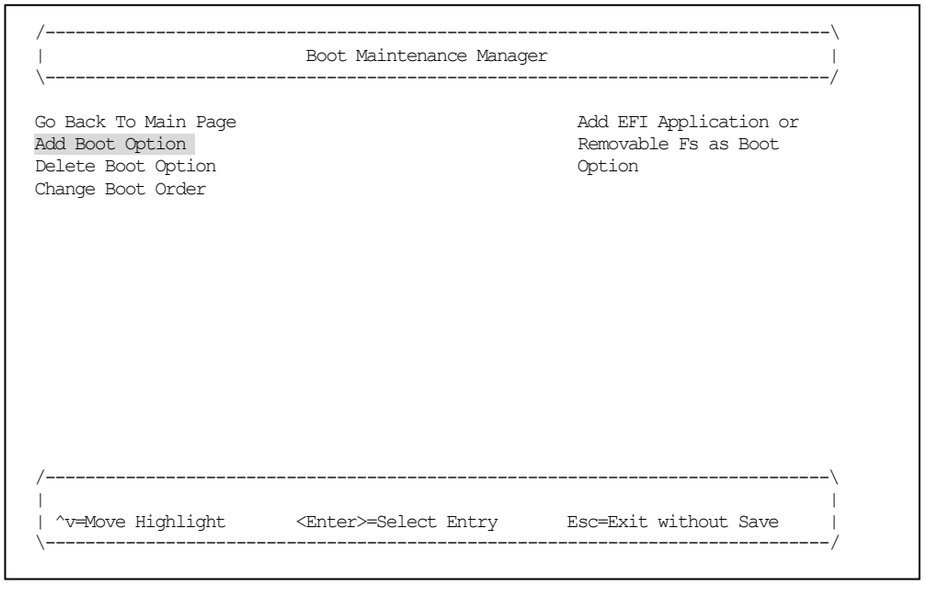
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.



3 Select **Add Boot Option**.



4 When **File Explorer** is displayed, select a device to configure.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E8010433B00,0x0)] *
USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x1,0x0)/MAC(00008762
F730,0x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x2,0x0)/MAC(00008762
F731,0x0)]




/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

5 Select **Input the description**.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E801025A260,0x0)] *

Input the description      _
Input Optional Data        _

Commit Changes and Exit
Discard Changes and Exit



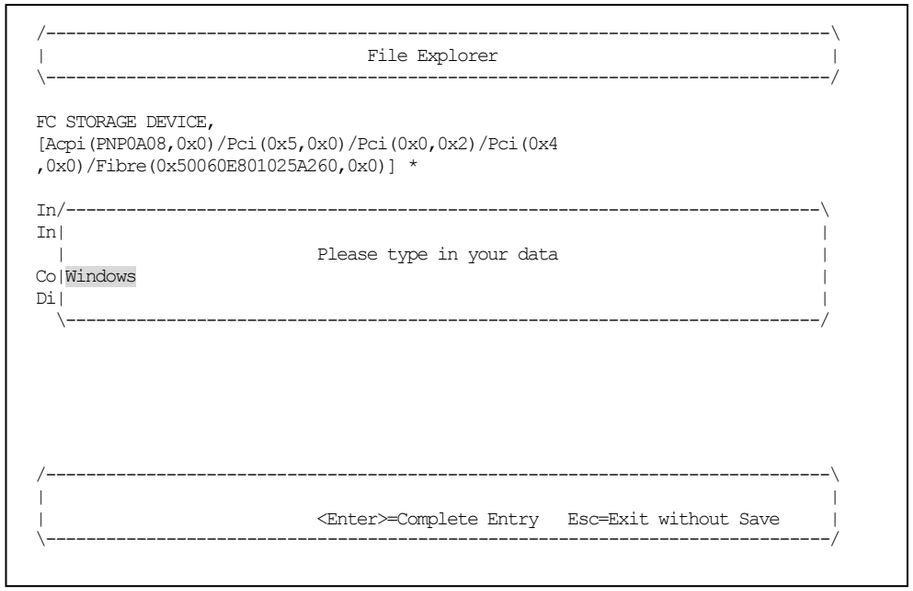






/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

6 Type the device name.

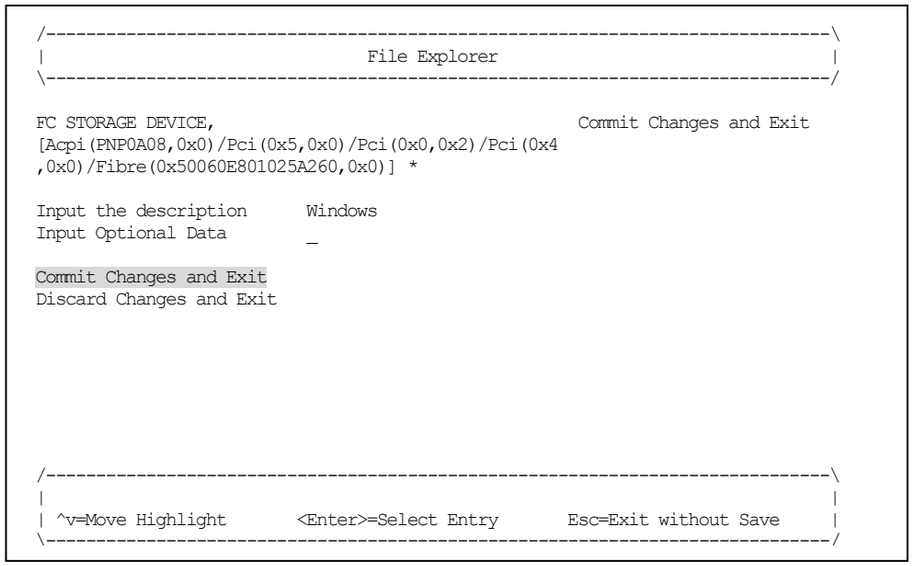


Tip

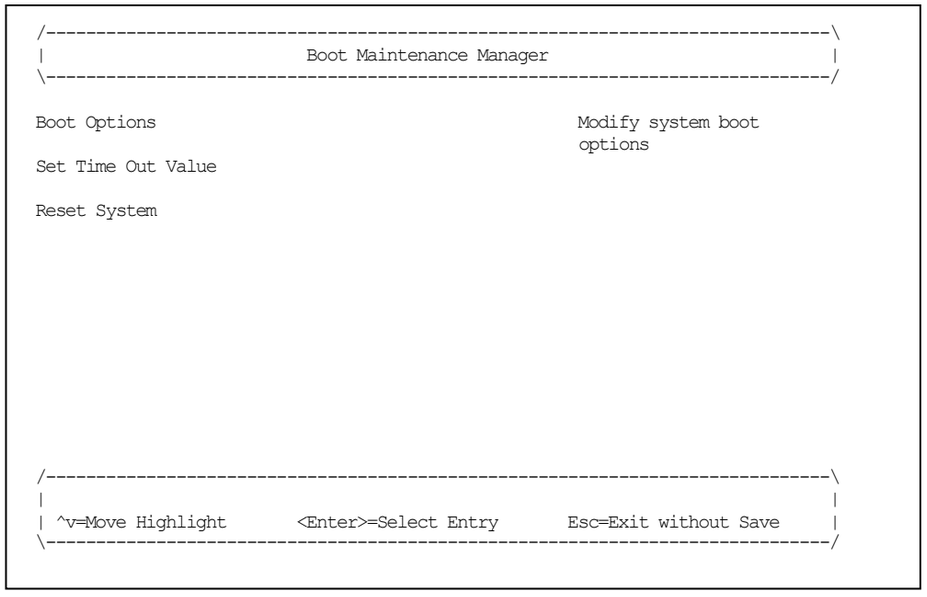
You can use the number of characters from 2 up to 75. The following characters are available.

Alphanumerics; symbols: !"#$%&'()=~|{}_?*`+><,./¥:];[@^-

7 Select **Commit Changes and Exit**.



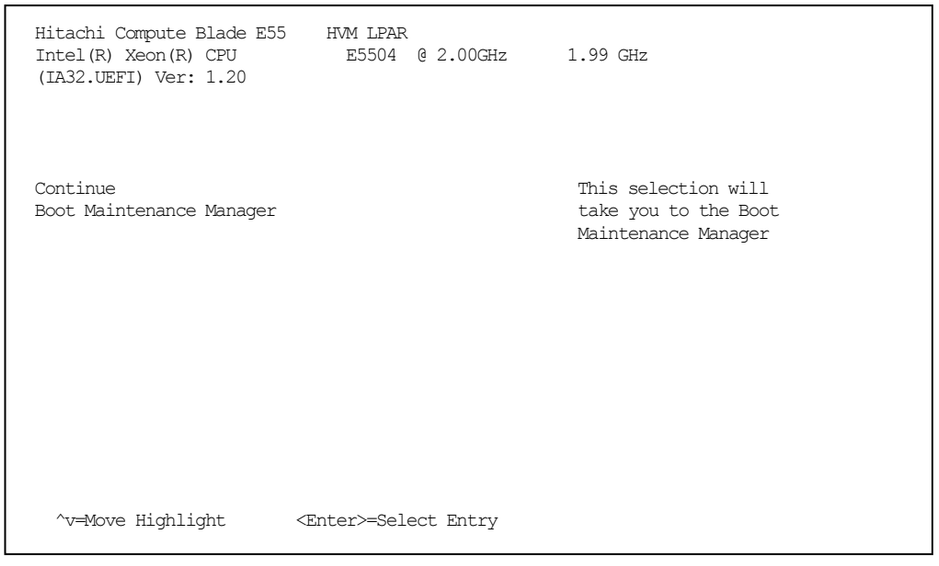
8 When **Boot Maintenance Manager** is displayed, press **Esc**.



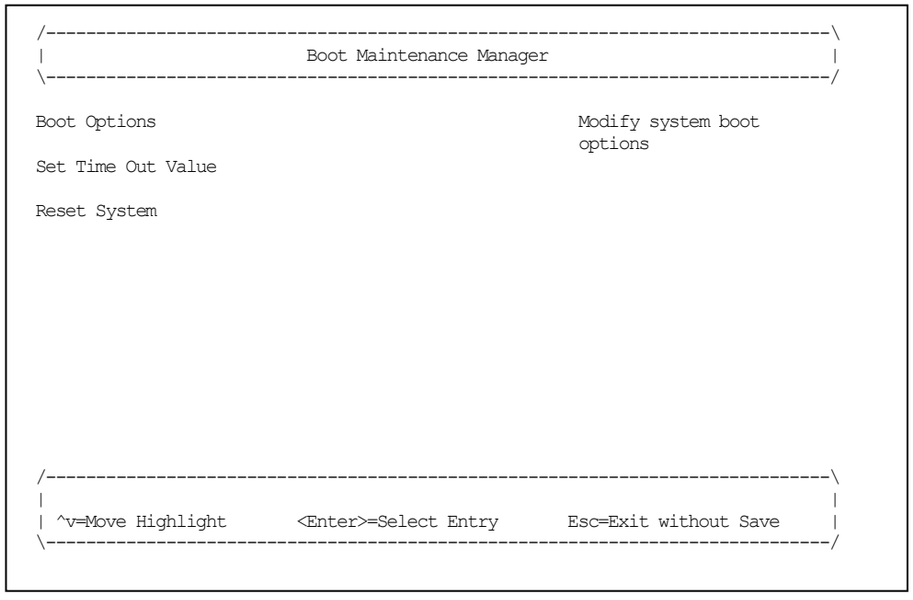
Go to Guest OS Boot in Changing Boot Orders to execute the procedure.

PXE Boot (network boot)

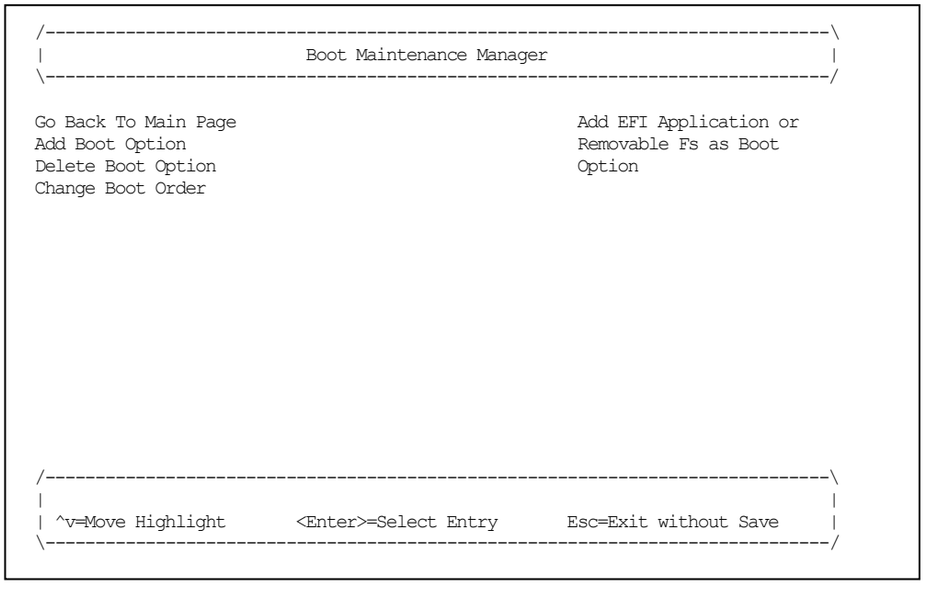
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



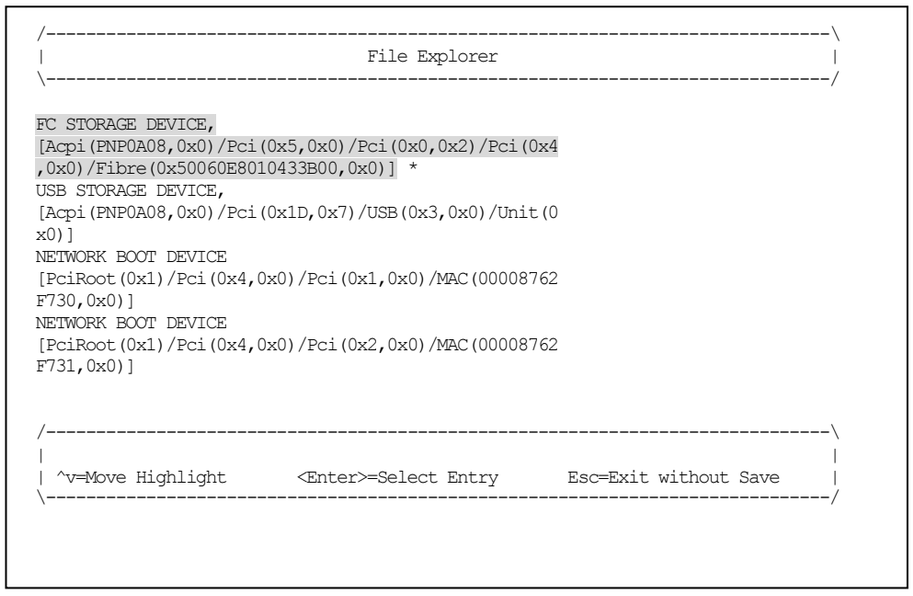
2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.



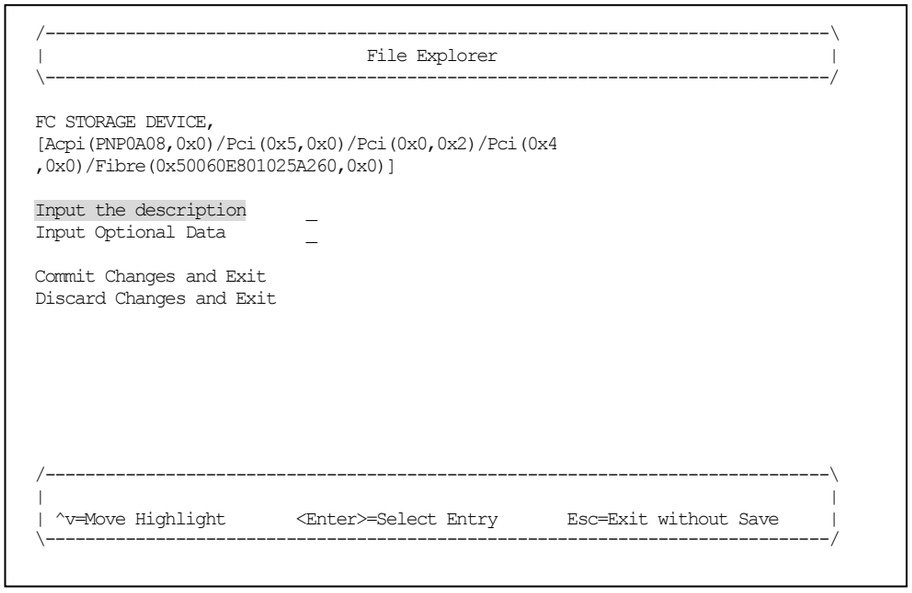
3 Select **Add Boot Option**.



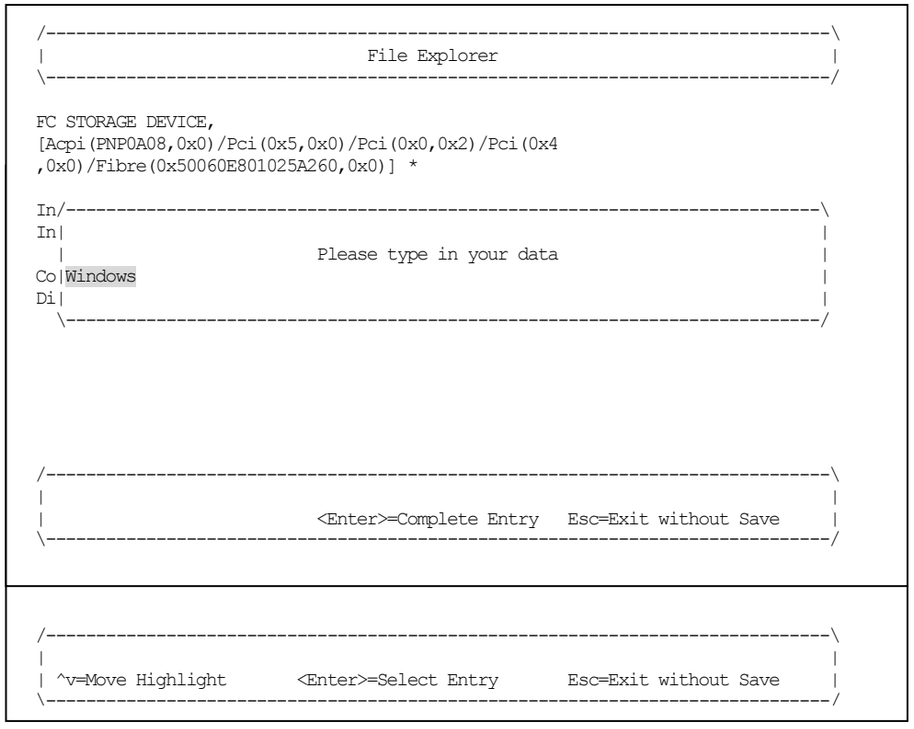
4 When **File Explorer** is displayed, select a device to configure.



5 Select **Input the description**.



6 Type the device name.

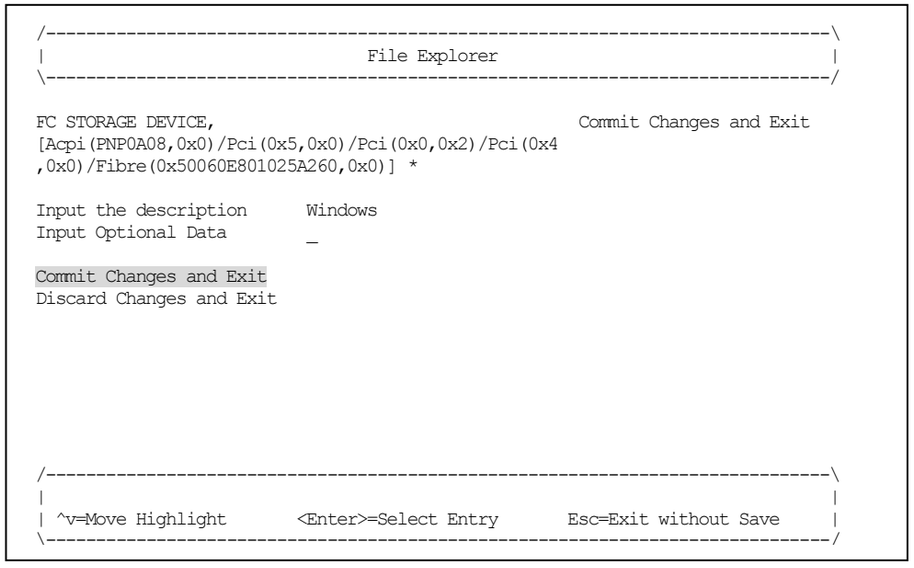


Tip

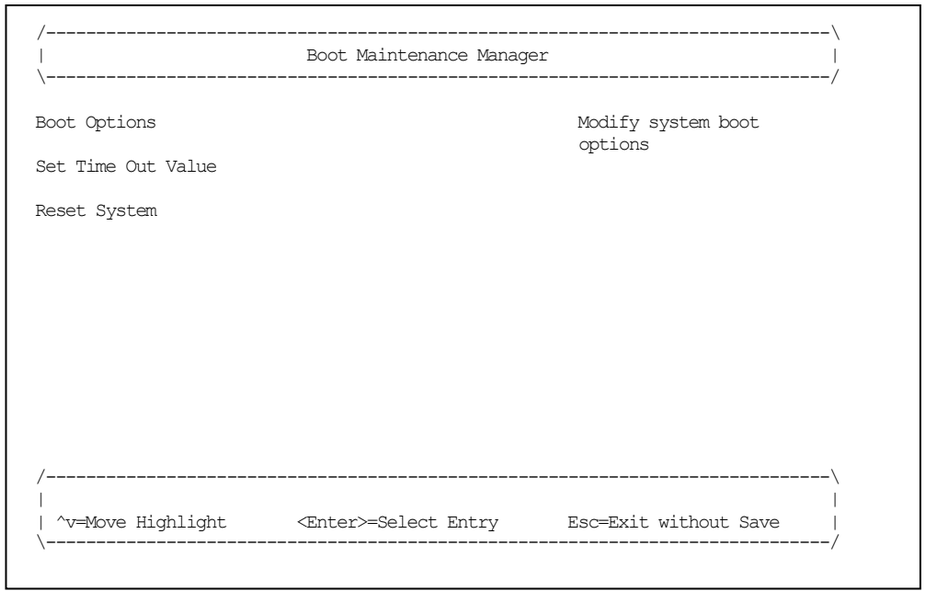
You can use the number of characters from 2 up to 75. The following characters are available.

Alphanumerics; symbols: !"#$%&'()=~|{}_?*`+><,./¥:];[@^-

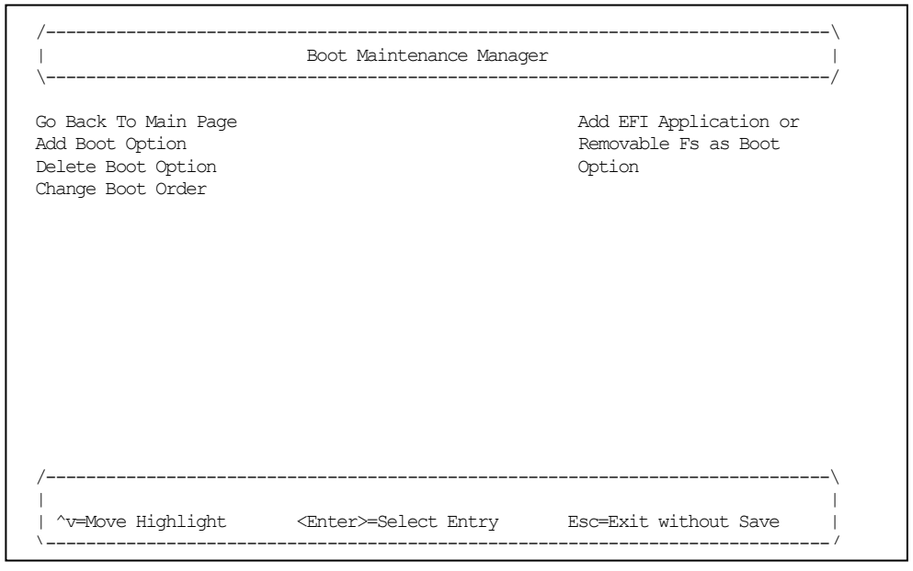
7 Select **Commit Changes and Exit**.



8 When **Boot Maintenance Manager** is displayed, press **Esc**.



9 Select **Add Boot Option**.



10 When **File Explorer** is displayed, select a device to create.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

FC STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x5,0x0)/Pci(0x0,0x2)/Pci(0x4
,0x0)/Fibre(0x50060E8010433B00,0x0)]
USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x1,0x0)/MAC(00008762
F730,0x0)]
NETWORK BOOT DEVICE
[PciRoot(0x1)/Pci(0x4,0x0)/Pci(0x2,0x0)/MAC(00008762
F731,0x0)]




/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

11 Select **Input the description**.

```
/-------------------------------------------------------------------------------\
|                               File Explorer                                   |
\-------------------------------------------------------------------------------/

USB STORAGE DEVICE,
[Acpi(PNP0A08,0x0)/Pci(0x1D,0x7)/USB(0x3,0x0)/Unit(0
x0)]

Input the description      _
Input Optional Data        _

Commit Changes and Exit
Discard Changes and Exit



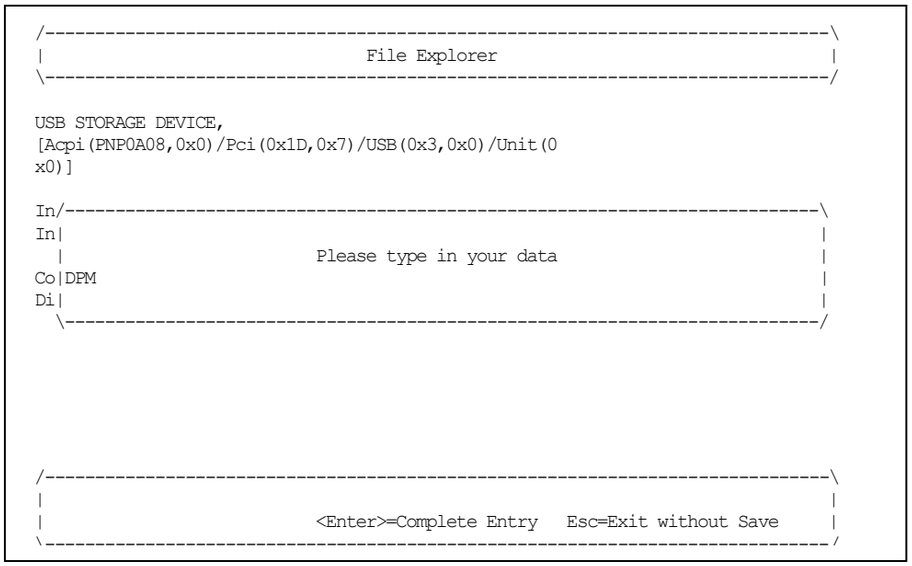






/-------------------------------------------------------------------------------\
|                                                                               |
| ^v=Move Highlight       <Enter>=Select Entry       Esc=Exit without Save      |
\-------------------------------------------------------------------------------/
```

12 Type the device name.

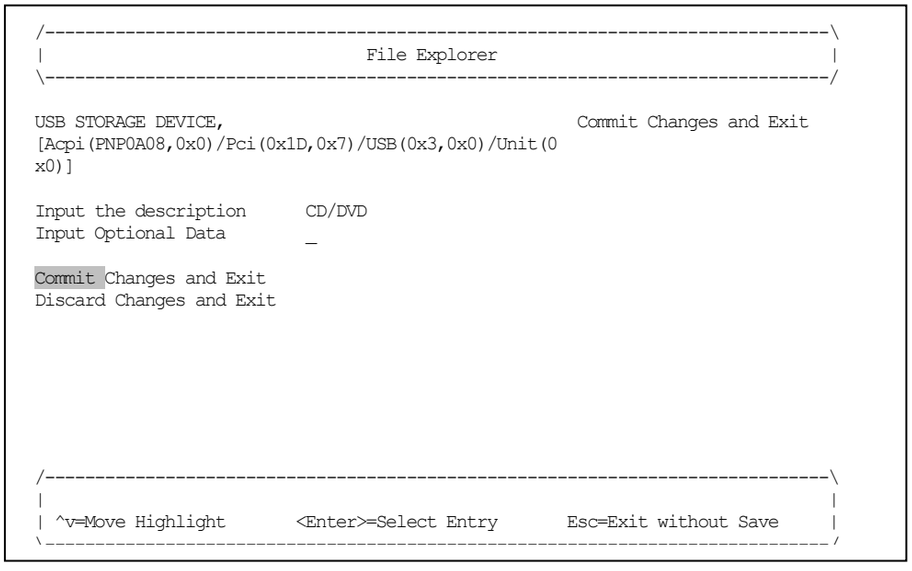


Tip

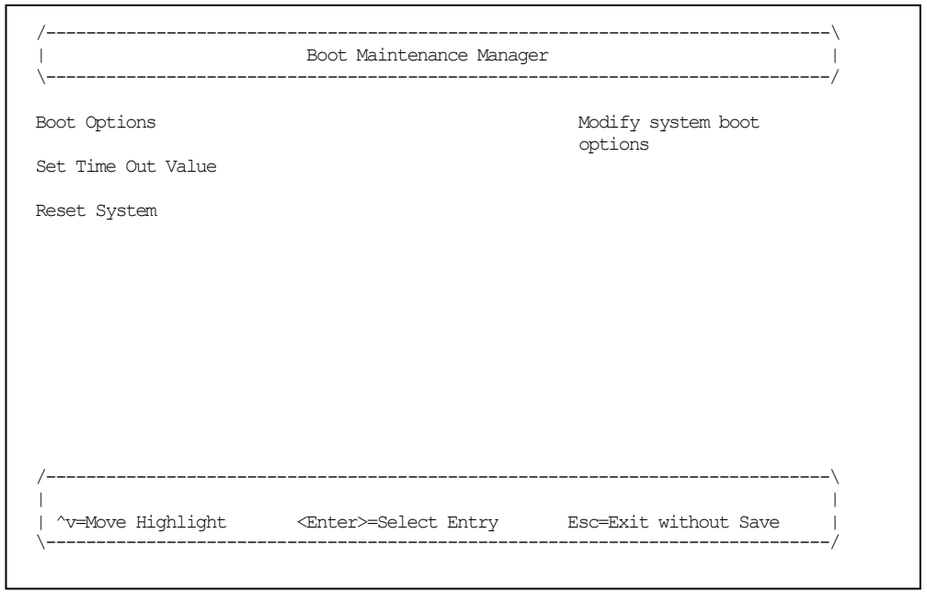
You can use the number of characters from 2 up to 75. The following characters are available.

Alphanumerics; symbols: !"#$%&'()=~|{}_?*`+><,./¥:];[@^-

13 Select **Commit Changes and Exit**.



14 When **Boot Maintenance Manager** is displayed, press **Esc**.



Go to PXE Boot (network boot) in Changing boot orders to execute the procedure.

❑ Changing boot orders

You can specify the boot order of devices by changing the boot order.

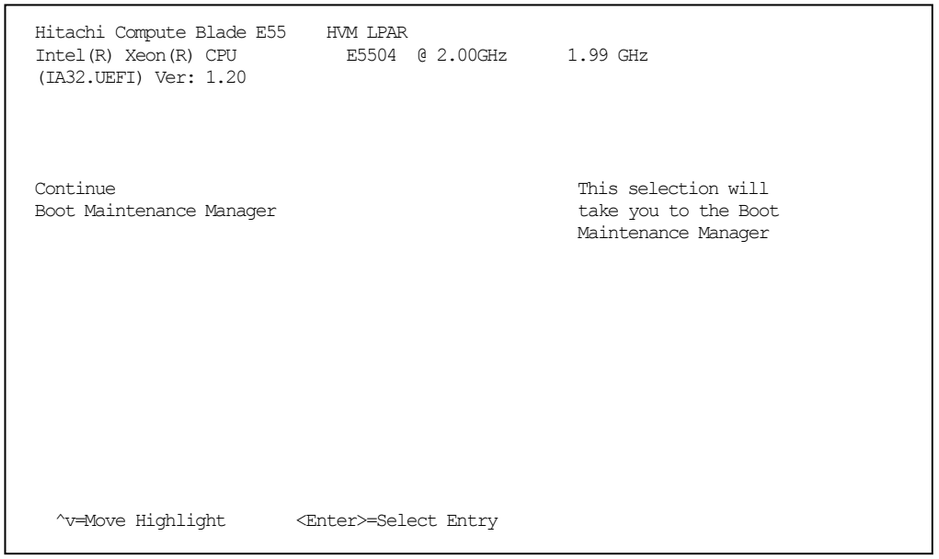
.

When already having configured the order of boot devices, ignore this subsection.

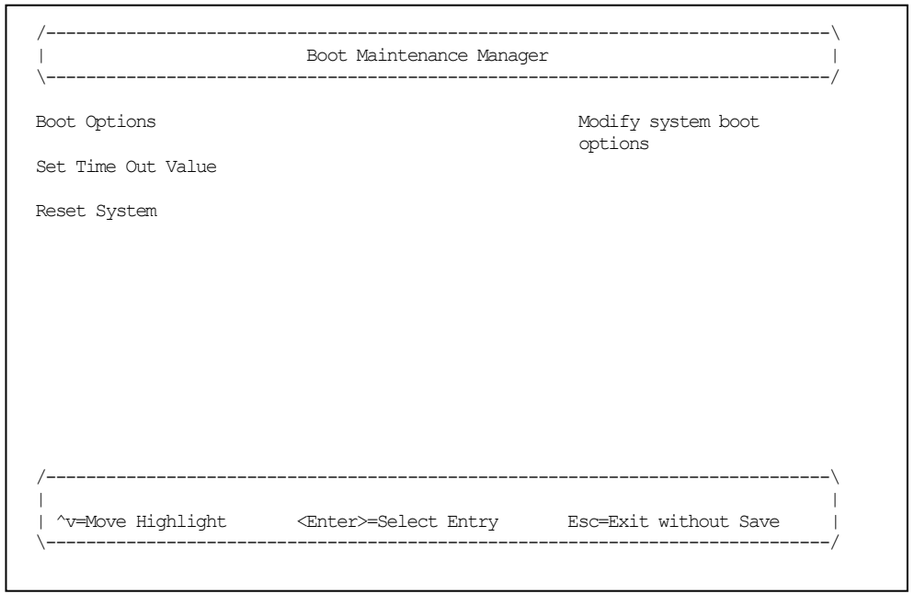
Boot option example	Device	Boot type	Application
EFI Internal Shell	-	EFI Shell boot	EFI driver settings
Windows	FC STORAGE DEVICE	Guest OS boot	Guest OS is used
CD/DVD	USB STORAGE DEVICE	CD/DVD boot	CD/DVD is used.
DPM	NETWORK BOOT DEVICE	PXE boot	SC/DPM is used

Booting EFI Shell

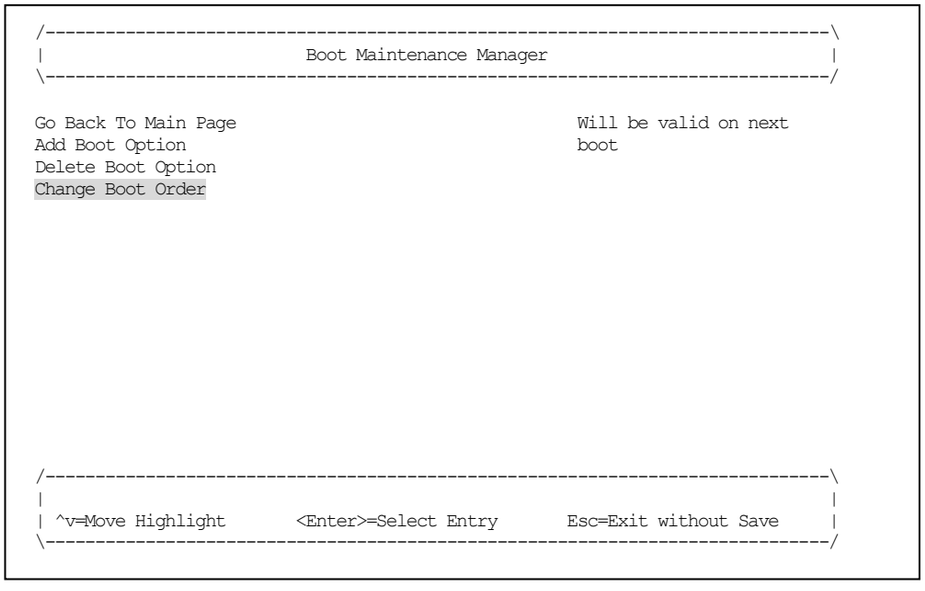
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.

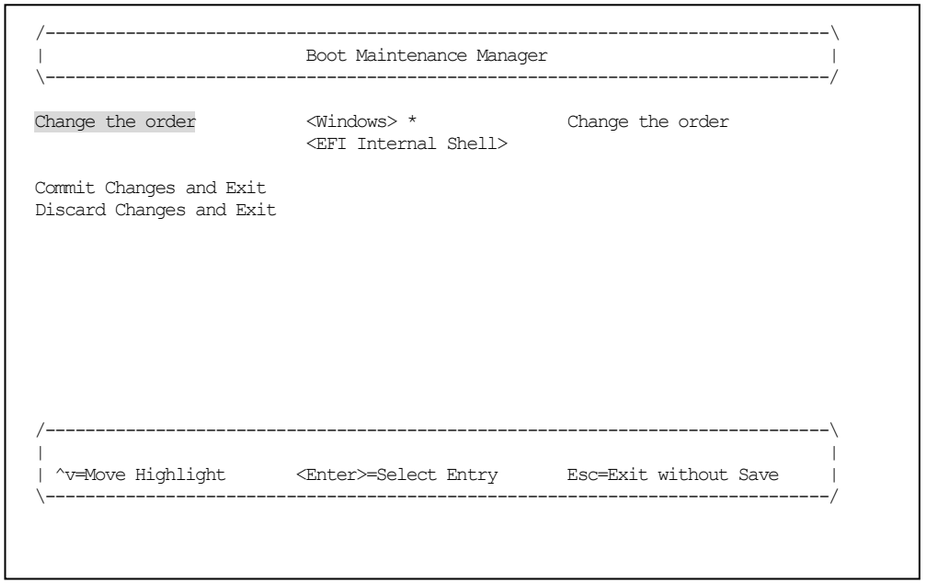


3 Select **Change Boot Order**.

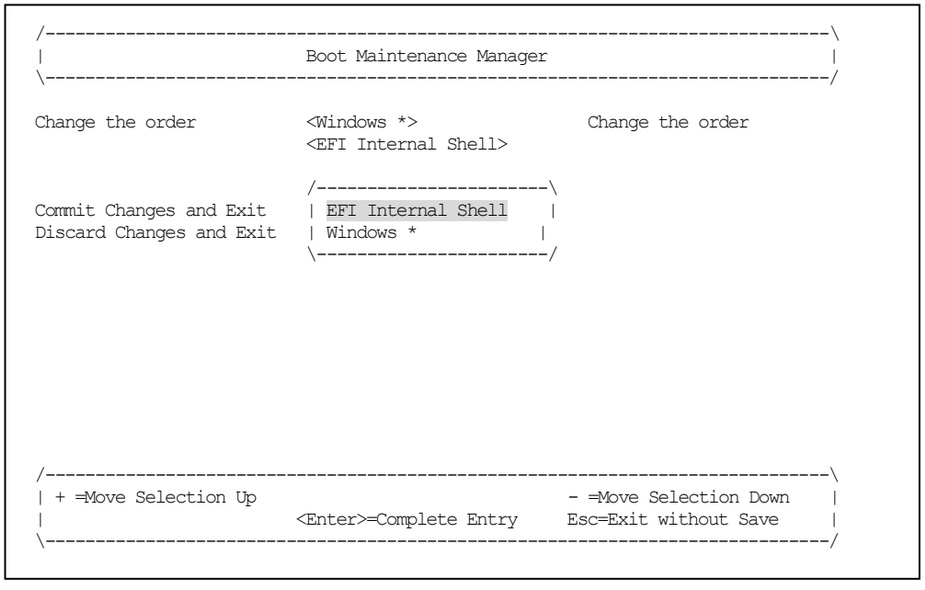


4 If **EFI Internal Shell** is displayed on the top of the boot order, Change Boot Order is not needed. Select **Discard Changes and Exit**, and then go to Step 8.

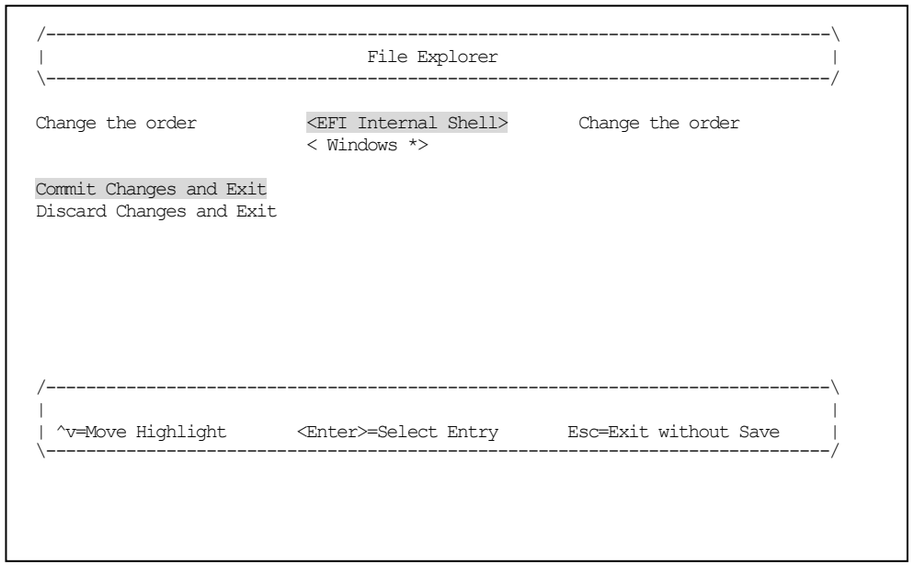
If not, select **Change the order**.



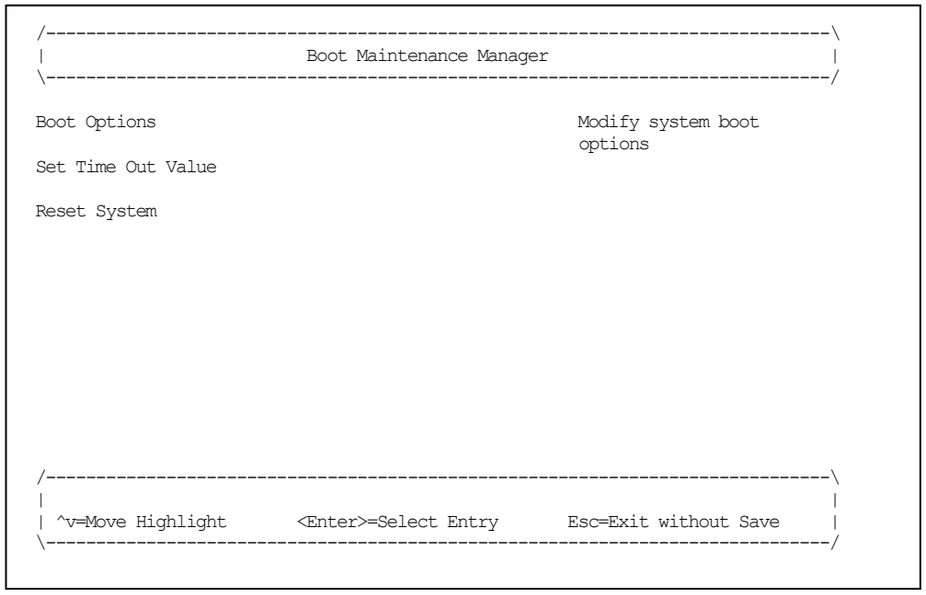
5 When the subscreen is displayed, move **EFI Internal Shell** to the top of the boot options using a key, [+] or [-].



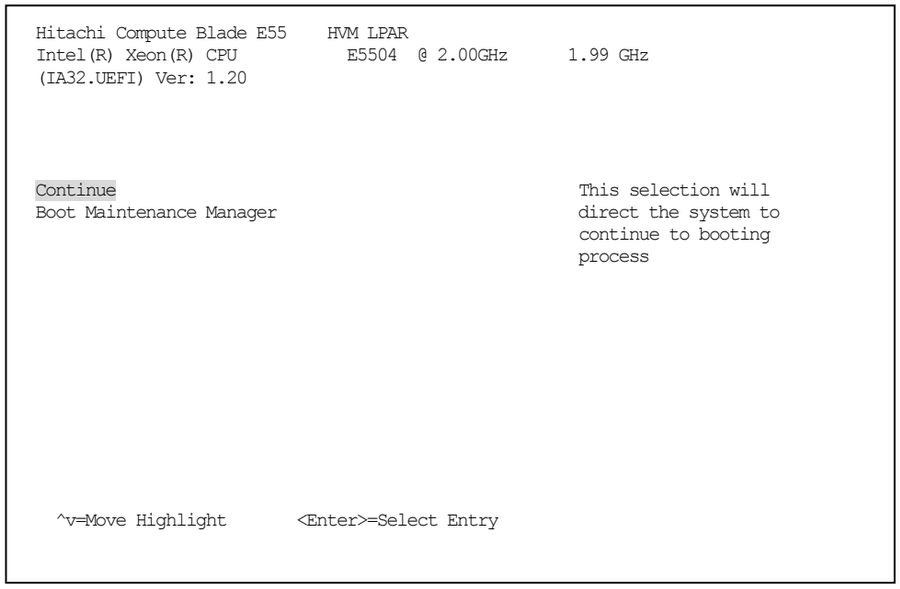
6 Select **Commit Changes and Exit**.



7 When **`Boot Maintenance Manager`** is displayed again, press **Esc**.

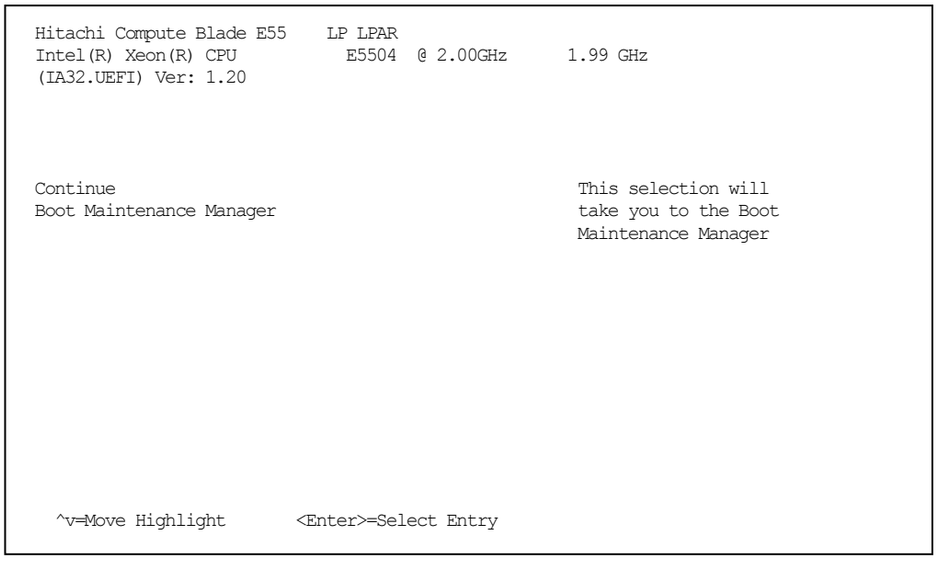


8 On the screen displayed at the logical BIOS boot, select **Continue**.

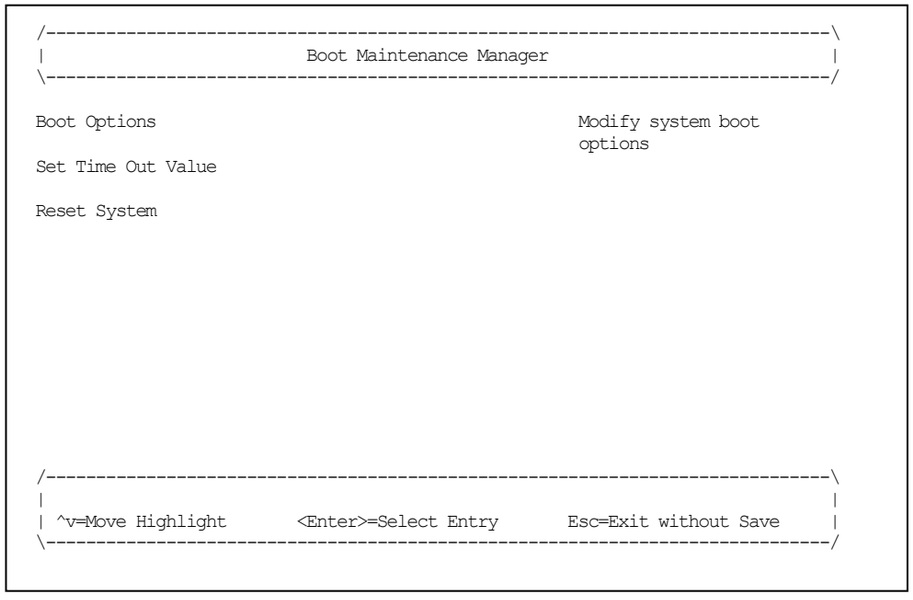


Guest OS Setup

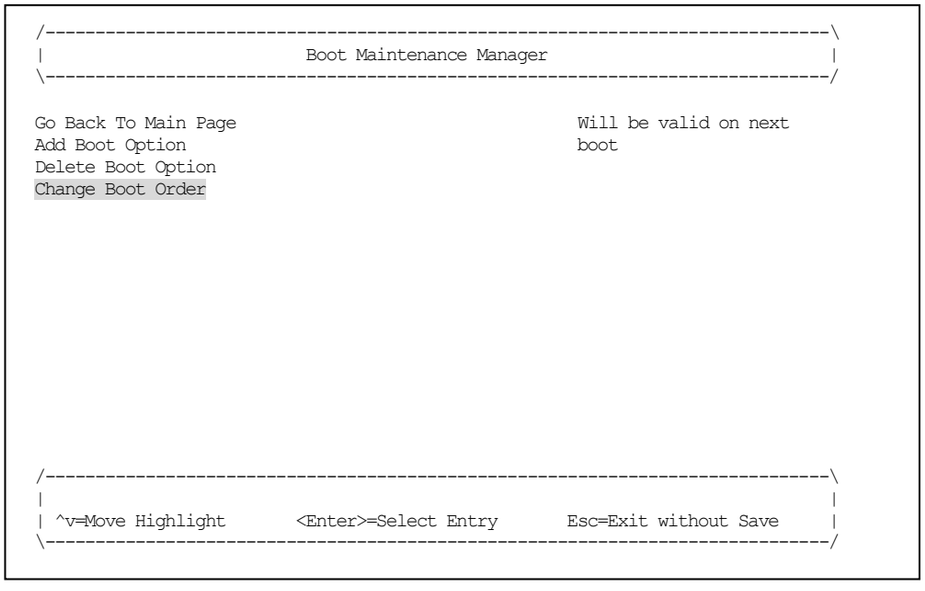
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.

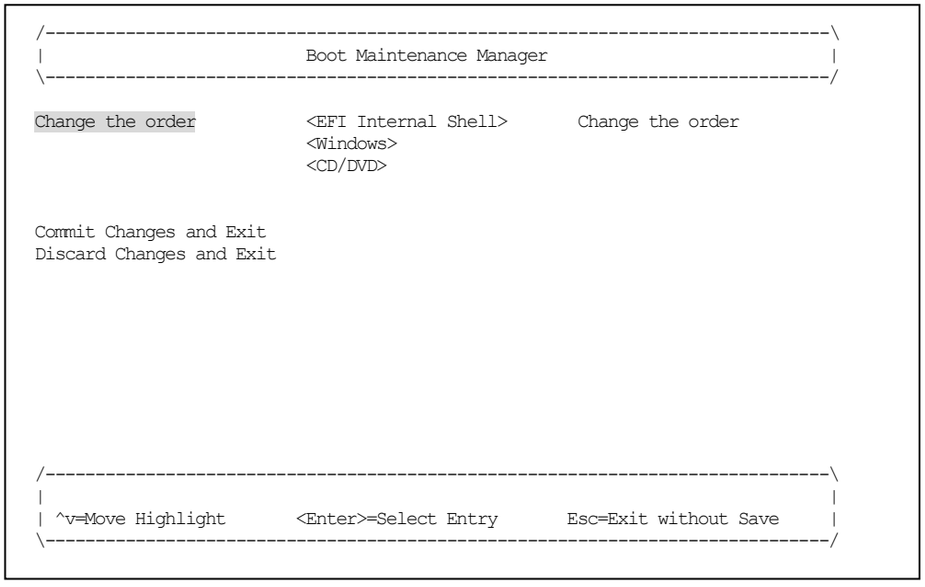


3 Select **Change Boot Order**.

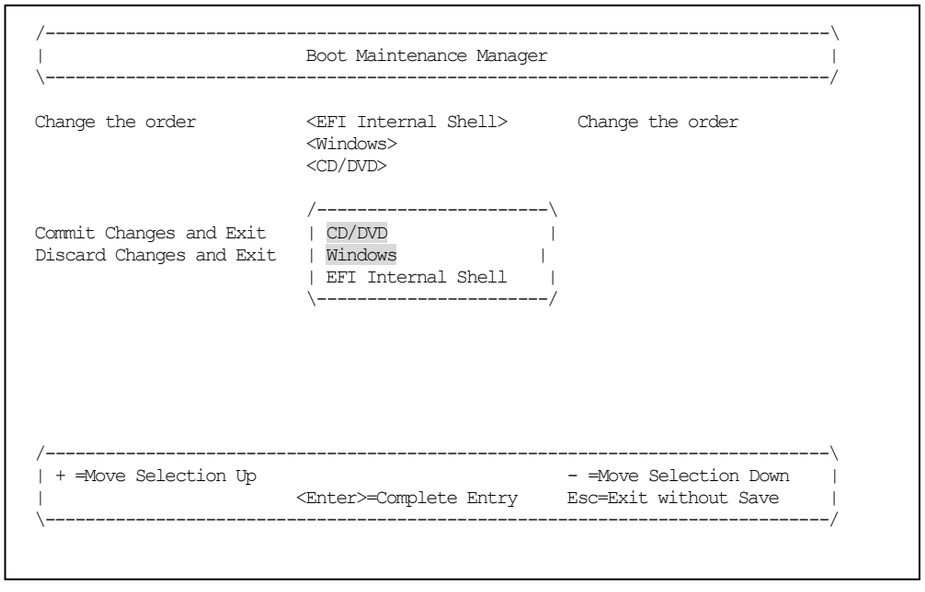


4 If **CD/DVD** then **Windows** are displayed in the boot order, Change Boot Order is not needed. Select **Discard Changes and Exit**, and then go to Step 8.

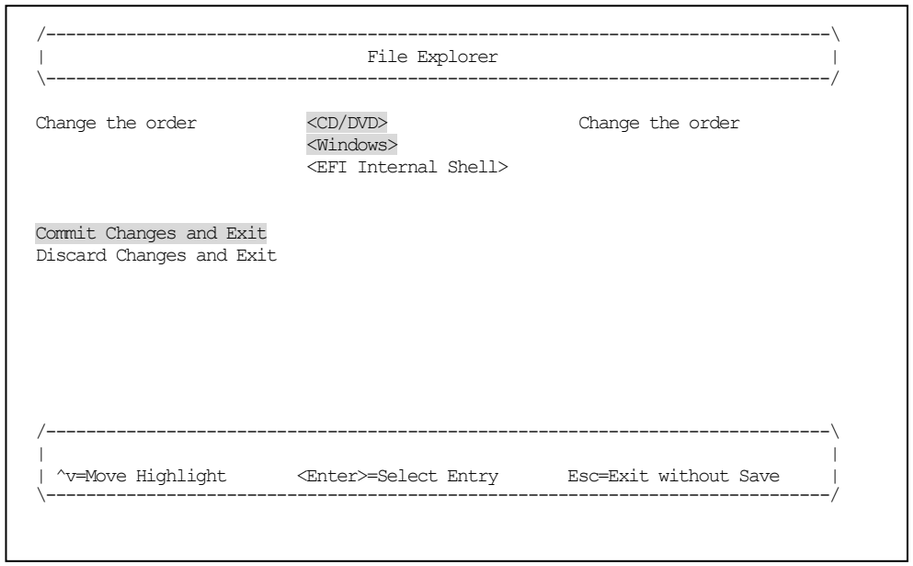
If not, select **Change the order**.



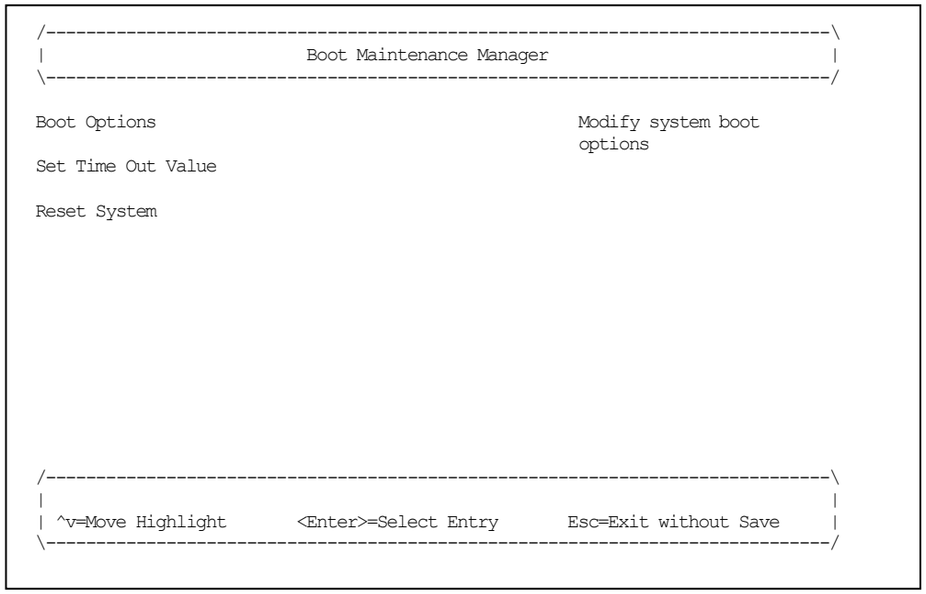
5 When the subscreen is displayed, move **CD/DVD** to the top and **Windows** to the second of the boot options using a key, [+] or [-].



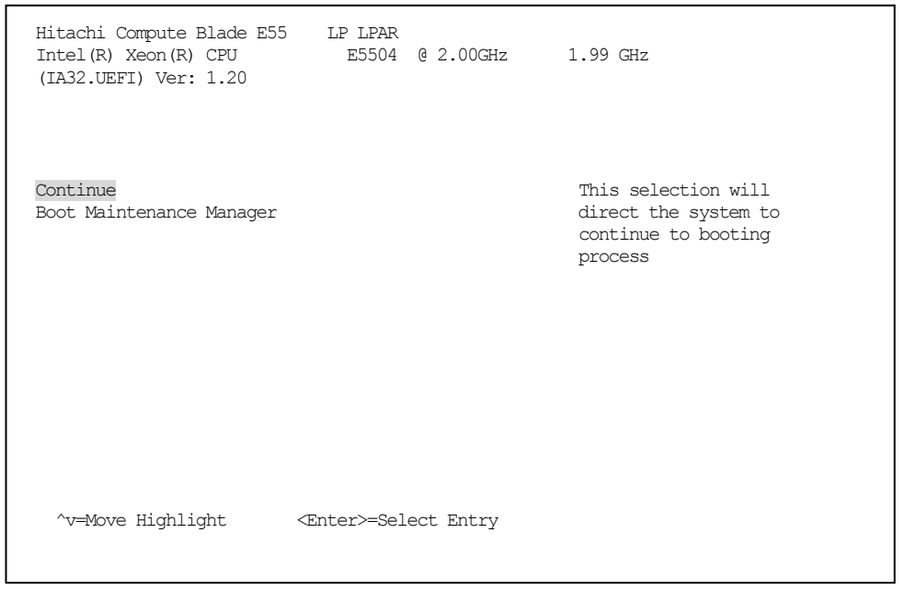
6 Select **Commit Changes and Exit**.



7 When **Boot Maintenance Manager** is displayed again, press **Esc**.

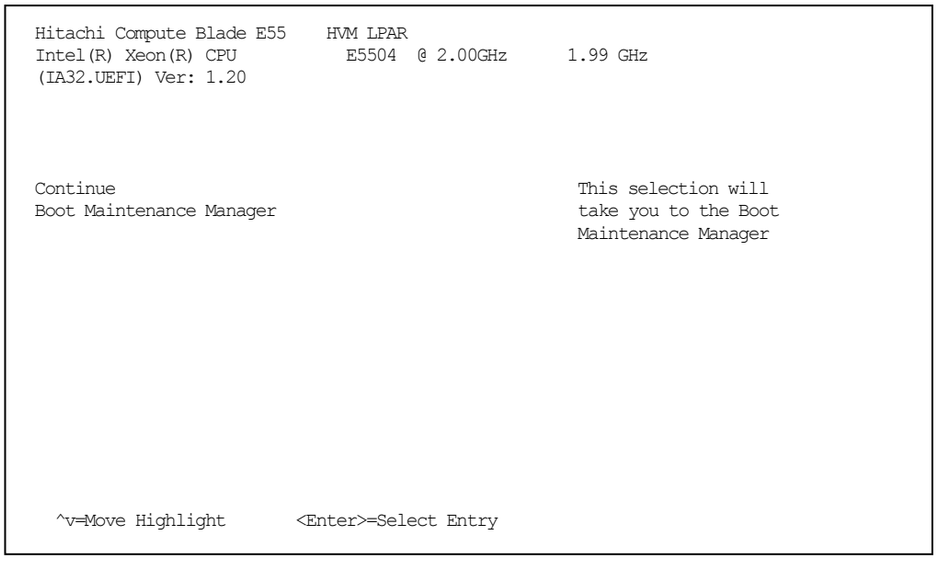


8 On the screen displayed at the logical BIOS boot, select **Continue**.

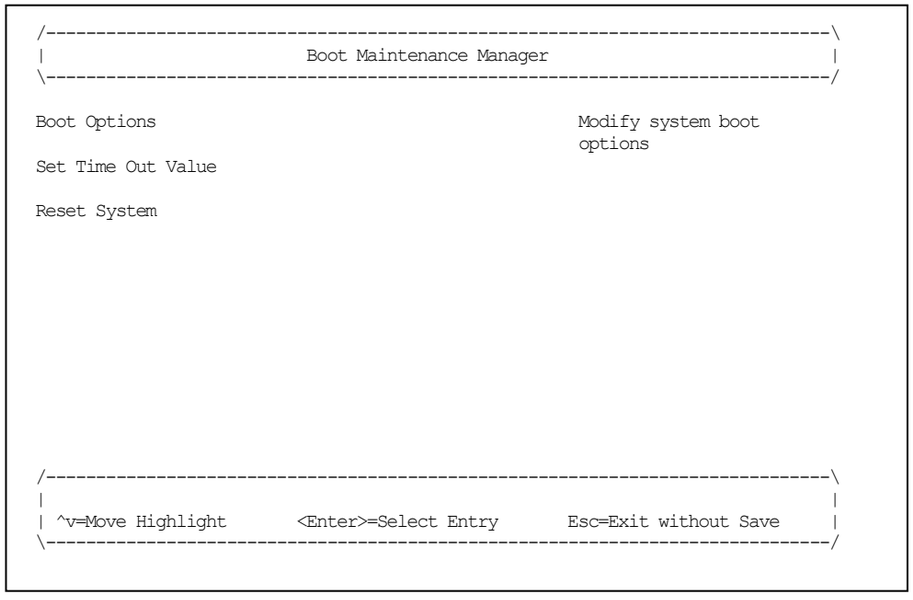


Guest OS Boot

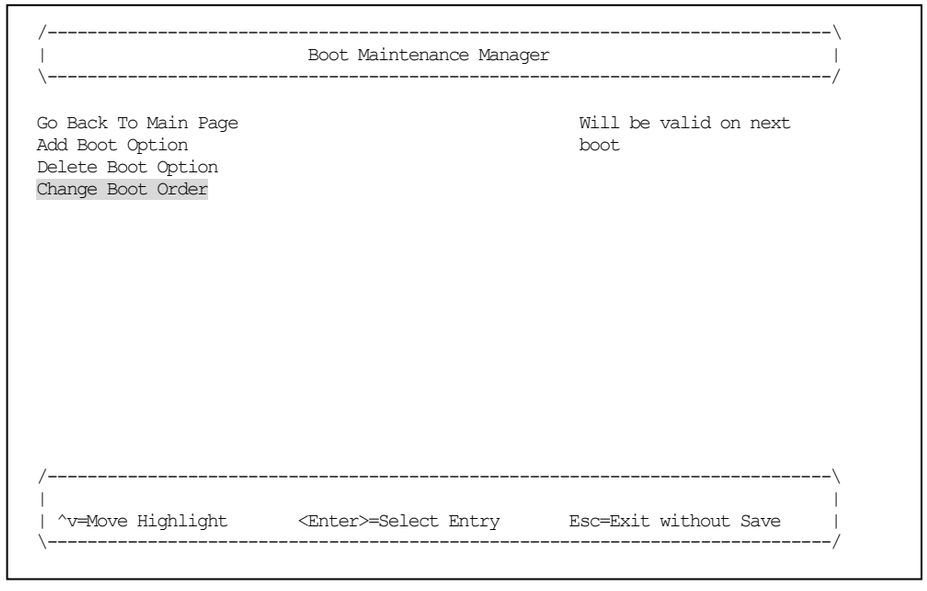
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.

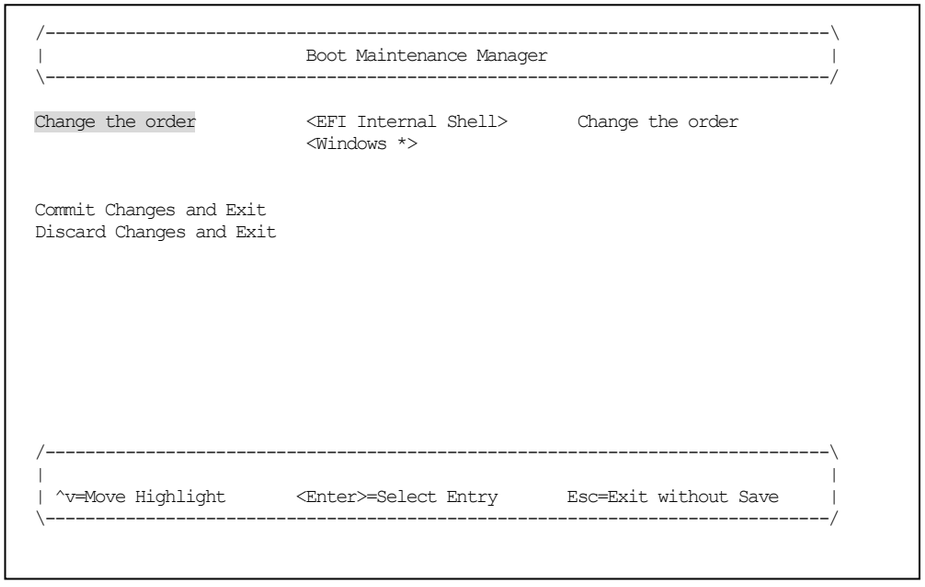


3 Select **Change Boot Order**.

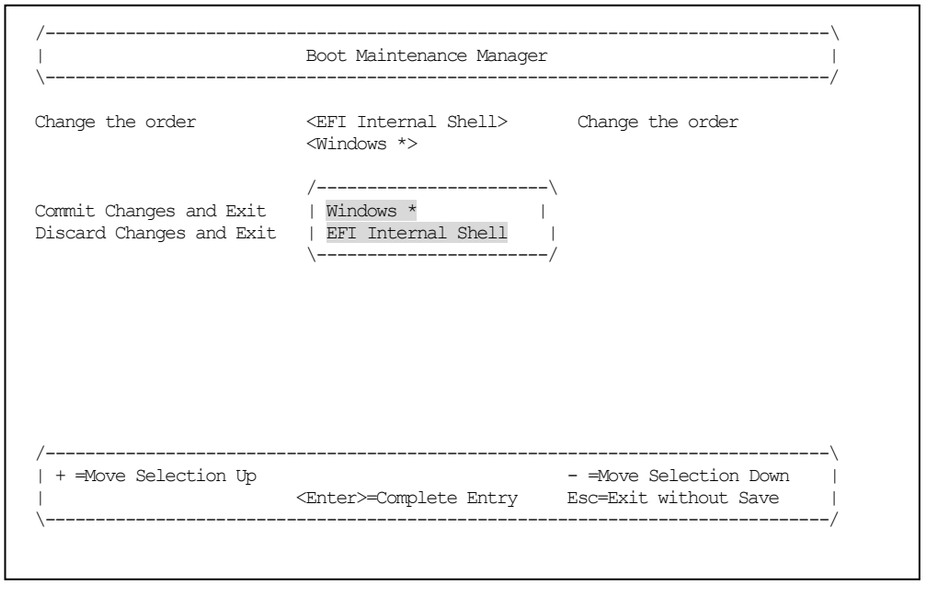


4 If **Windows** is displayed on the top of the boot order, Change Boot Order is not needed. Select **Discard Changes and Exit**, and then go to Step 8.

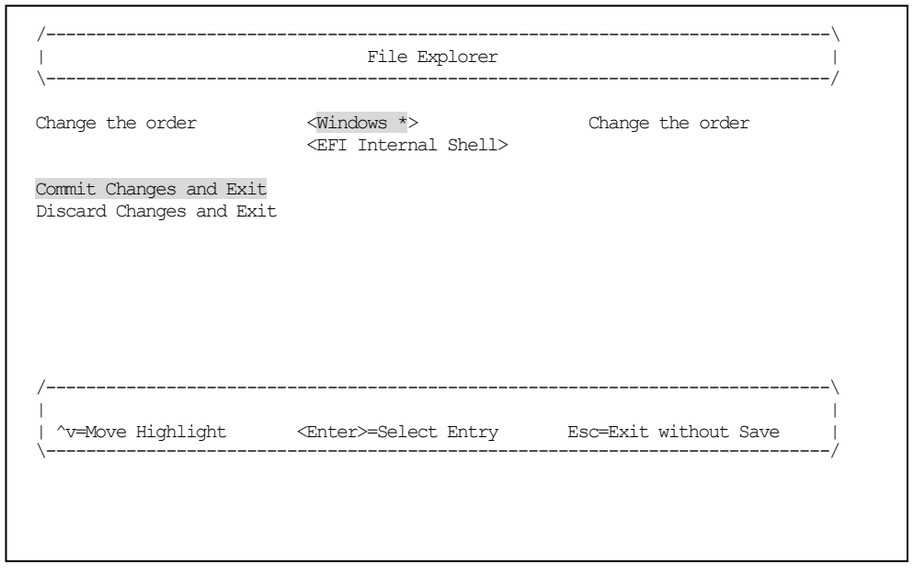
If not, select **Change the order**.



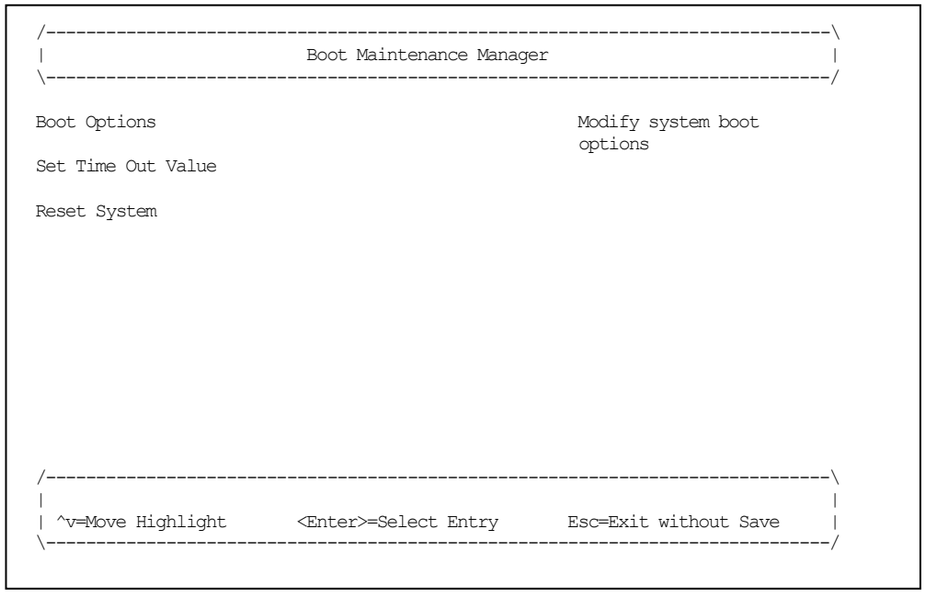
5 When the subscreen is displayed, move **Windows *** to the top of the boot options using a key, [+] or [-].



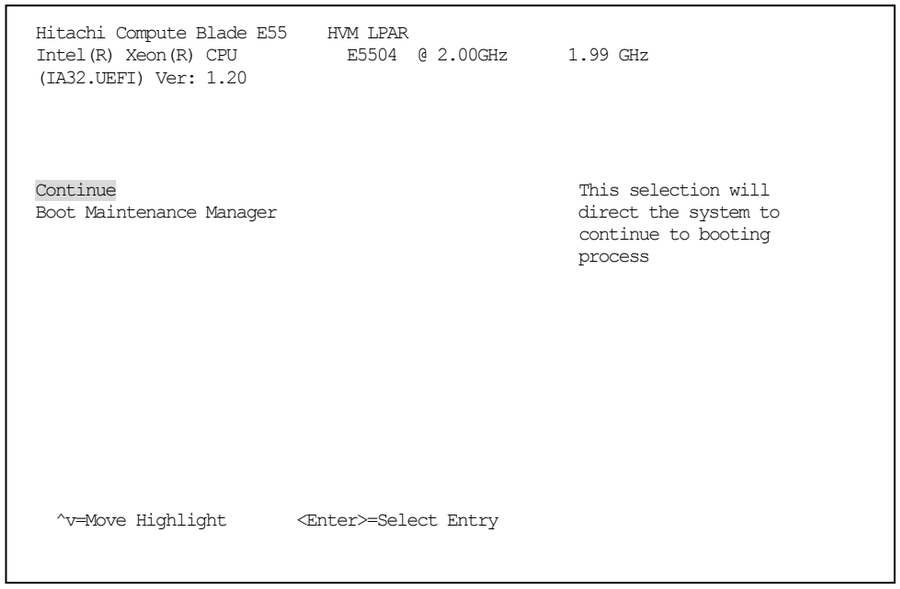
6 Select **Commit Changes and Exit**.



7 When **Boot Maintenance Manager** is displayed again, press **Esc**.

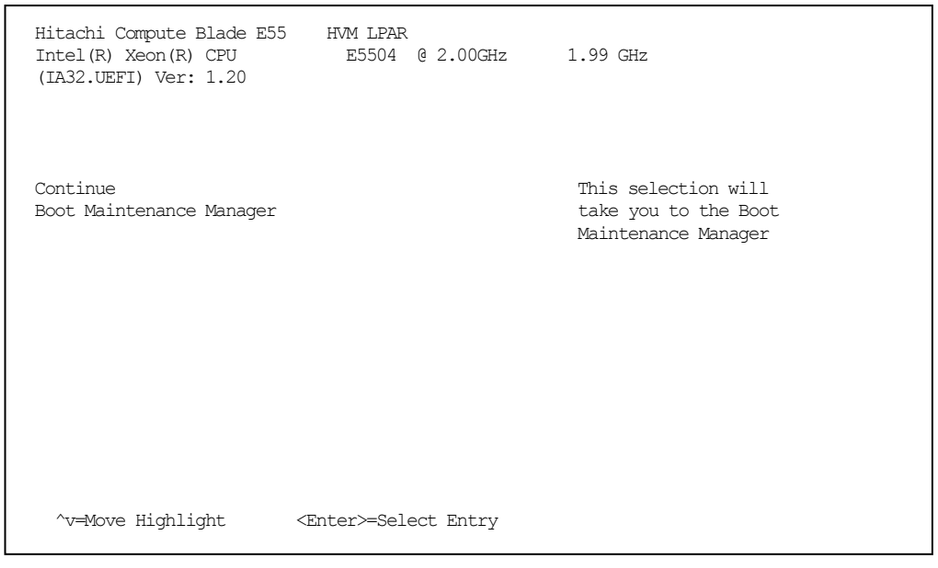


8 On the screen displayed at the logical BIOS boot, select **Continue**.

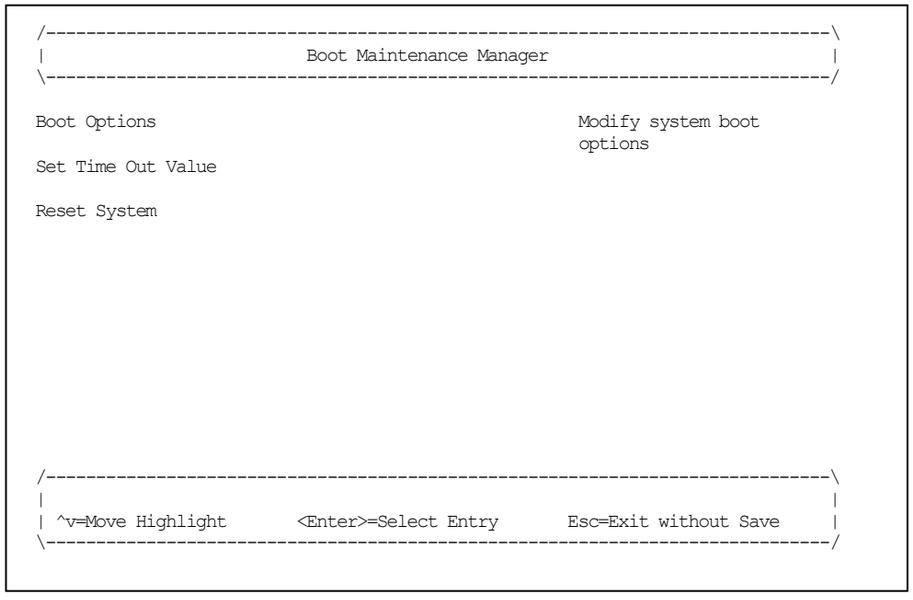


PXE Boot (network boot)

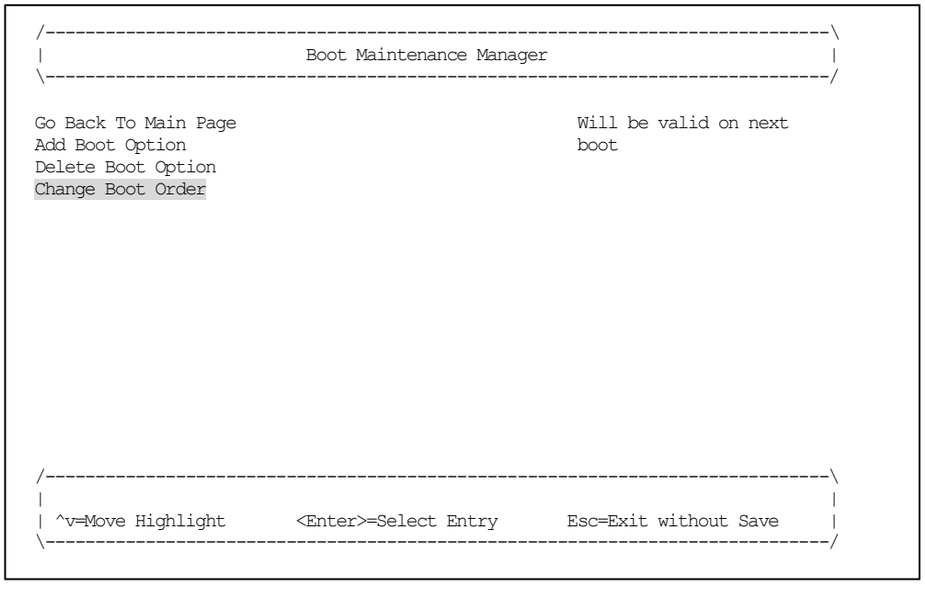
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.

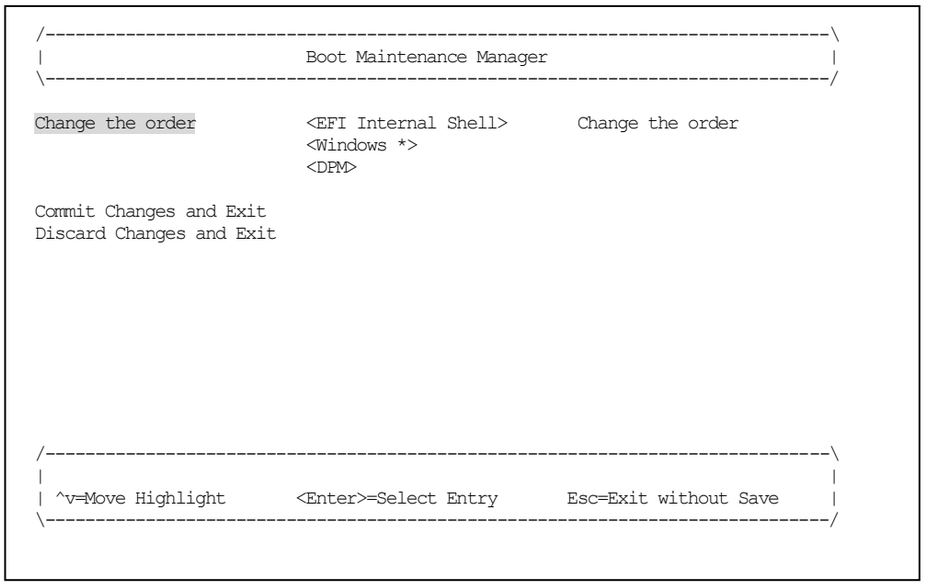


3 Select **Change Boot Order**.

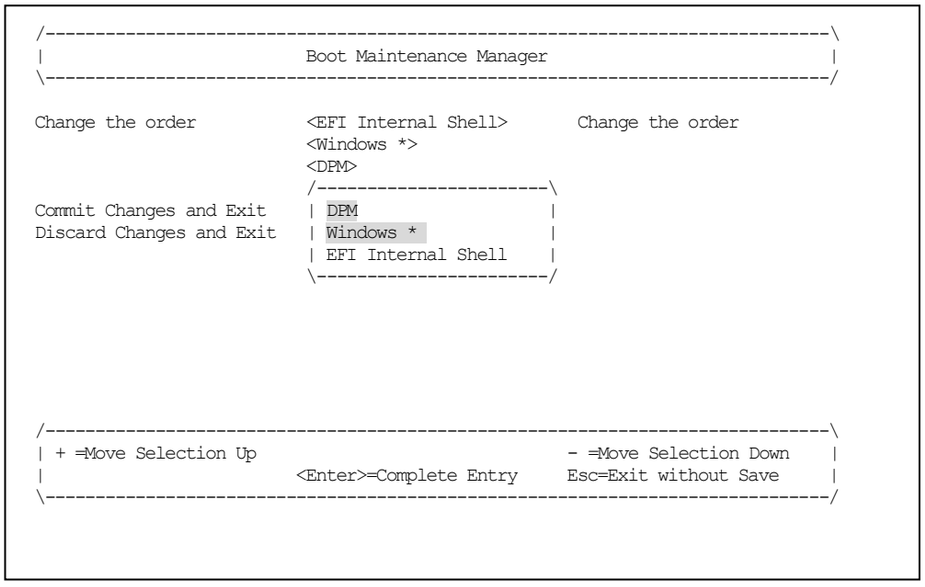


4 If **DPM** and **Windows** are displayed at the top and the second respectively, Change Boot Order is not needed. Select **Discard Changes and Exit**, and then go to Step 8.

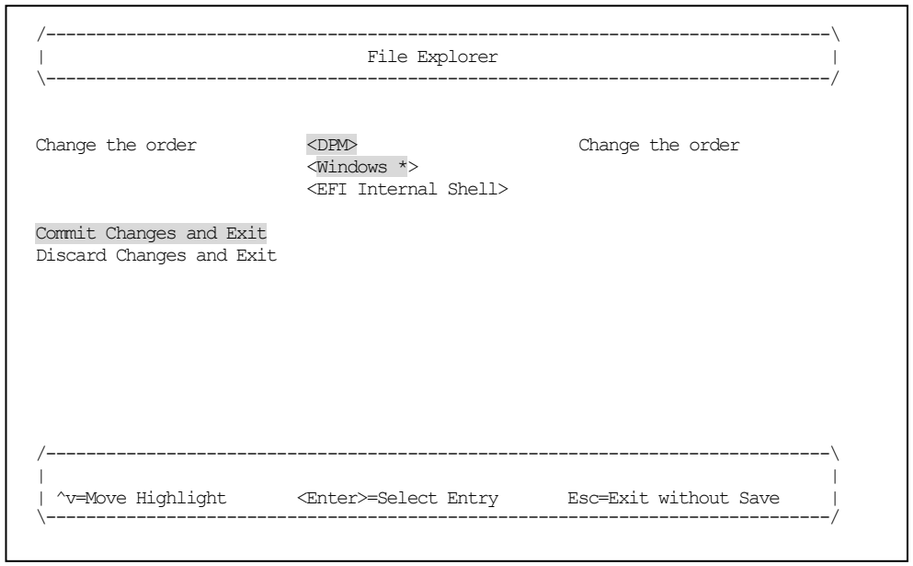
If not, select **Change the order**.



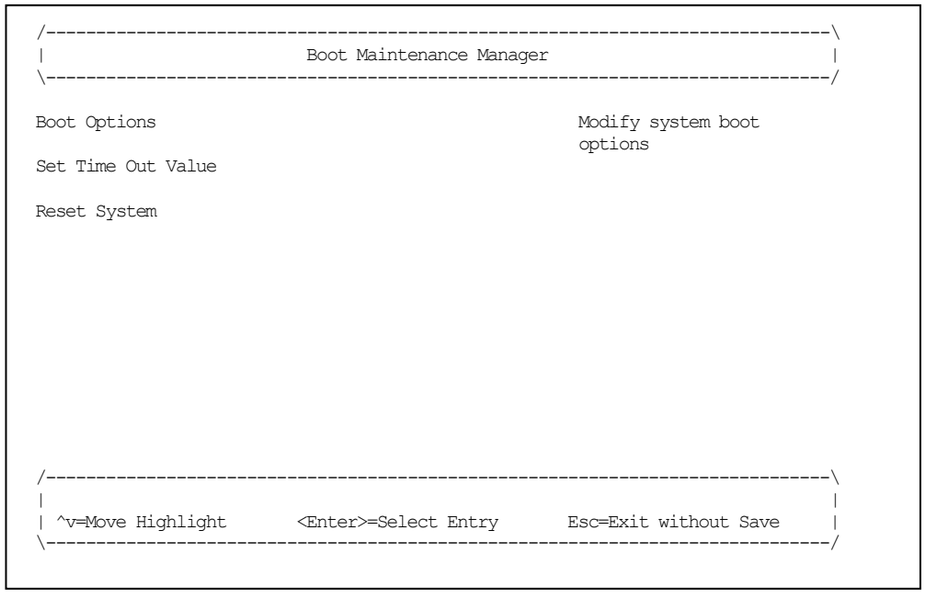
5 When the subscreen is displayed, move **DPM** and **Windows** to the top and the second respectively using a key, [+] or [-].



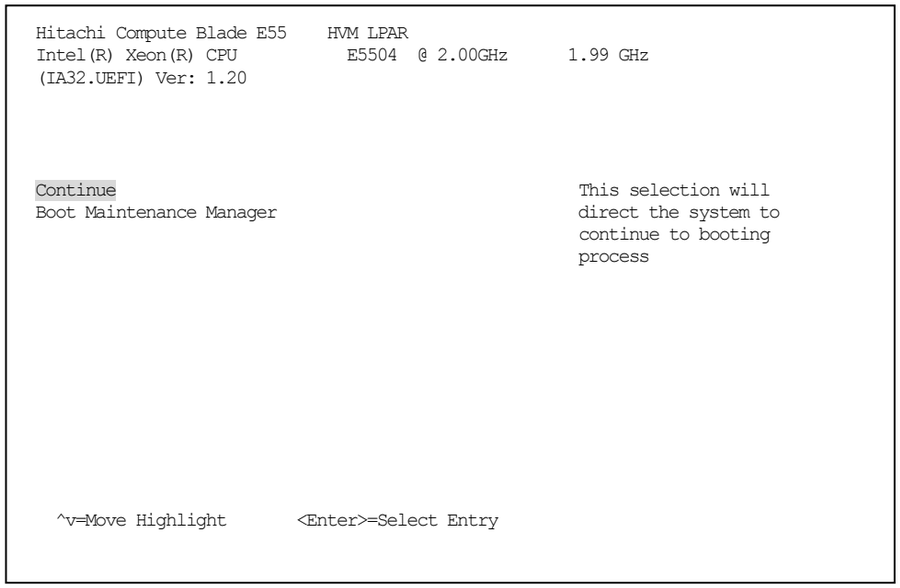
6 Select **Commit Changes and Exit**.



7 When **Boot Maintenance Manager** is displayed again, press **Esc**.



8 On the screen displayed at the logical BIOS boot, select **Continue**.



Tip

- The operation after OS booting is basically the same as that for Basic.
- Be sure to allocate adequate resources to the LPARs to operate the OS, middleware, and applications used. For details, see the *Hitachi Compute Blade 2000 Software Guide* and the manuals for each product.
- Make sure to reset **Boot Order** after booting the EFI Shell. Otherwise the OS will not boot. Especially when booting the OS after the LPAR Auto Activate, sure to check if the guest OS boots up.
- When multiple devices installing the OS in the File Explorer are displayed, find out the target device from WWN or LUN on the display. WWN is 0x50060E801025A260 for Fibre (0x50060E801025A260, 0x0); 0x0 for LUN.



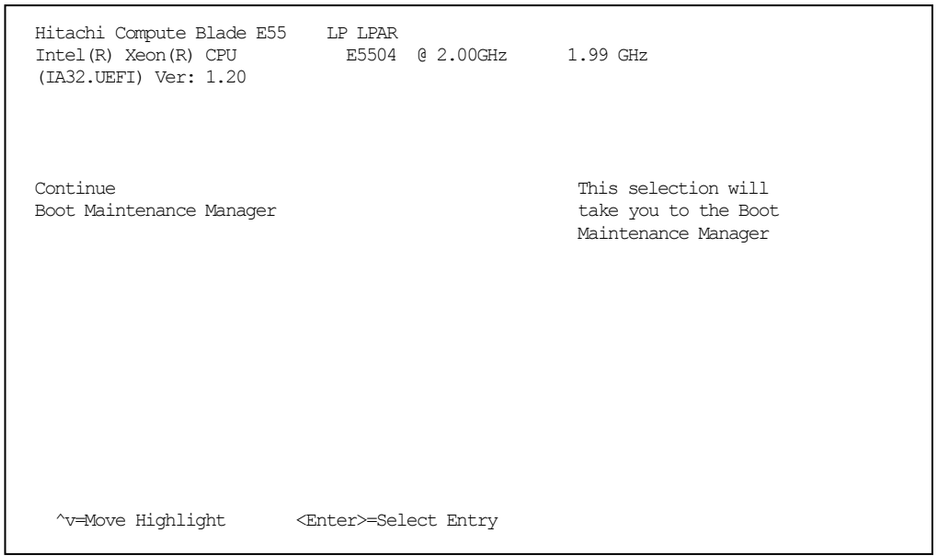
Action for the guest OS incomplete boot

- When using a shared FC as a boot device, boot might fail to finish depending on the number of LPARs assigned to the shared FC. In such a case, you can avoid the problem by extending the LOGIN DELAY time in the operation parameters for the FC adapter. For details, see the *HITACHI Gigabit Fibre Channel Board User's Guide (BIOS/EFI Edition)*.
- If rebooting suddenly occurs during OS boot, the service ratio allocated to LPAR might be low so that time-out requirements for the OS are not satisfied. If sudden rebooting occurs frequently, display the **LP System Logs** screen and check whether the LP system log contains "LP detects AP initialization timeout." If it is contained, review the service ratio allocated to the LPAR.
- If actions above cannot complete the guest OS boot, LPAR settings might cause the problem. Check the settings once more. Deactivate the LPAR, review and set the proper values, reactivate it, and boot the guest OS. If the symptom still remains, contact our technical personnel.

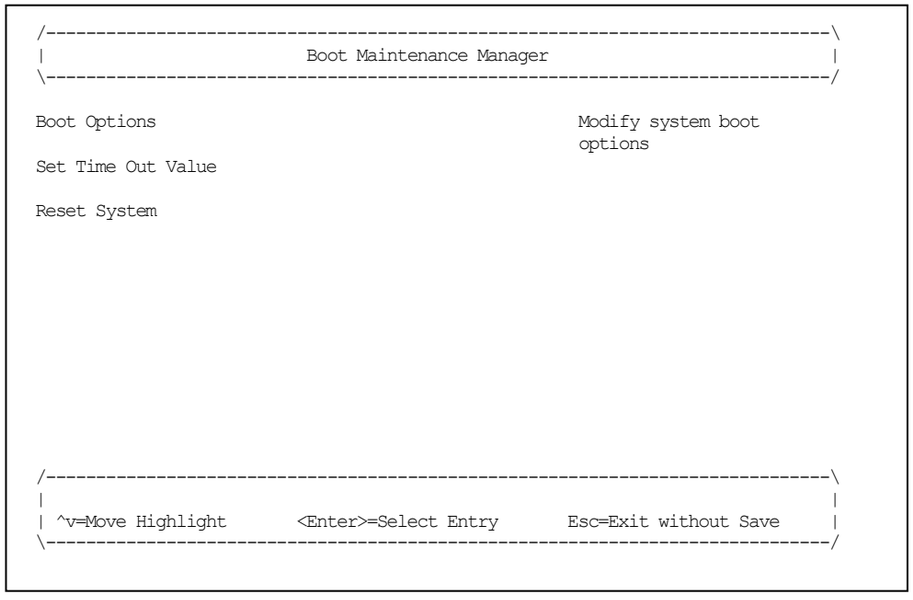
❑ Deleting Boot Options

You can prevent unrequired boot device from booting by deleting them. The following procedure is an example for deleting CD/DVD boot option.

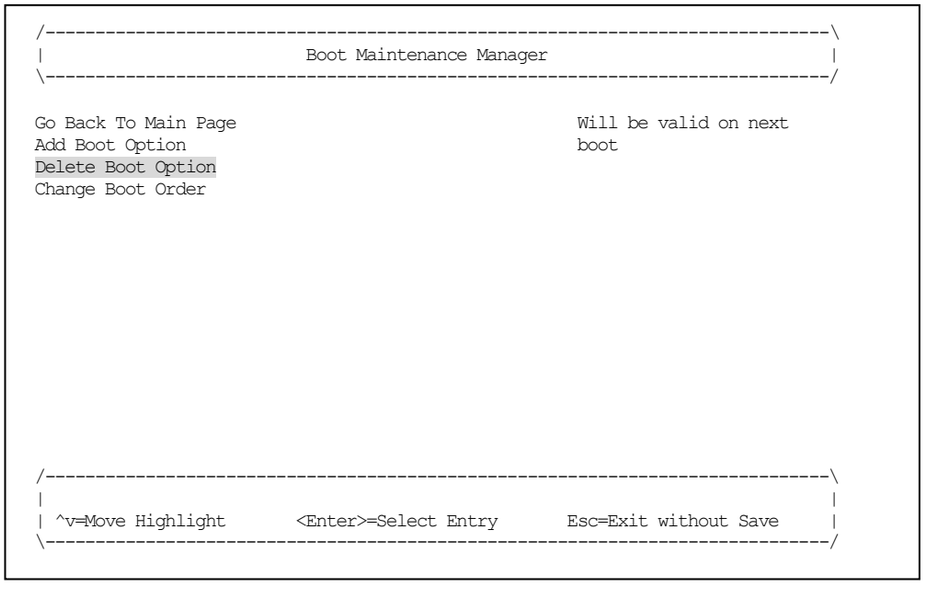
1 On the screen displayed at the logical BIOS boot, select **Boot Maintenance Manager**.



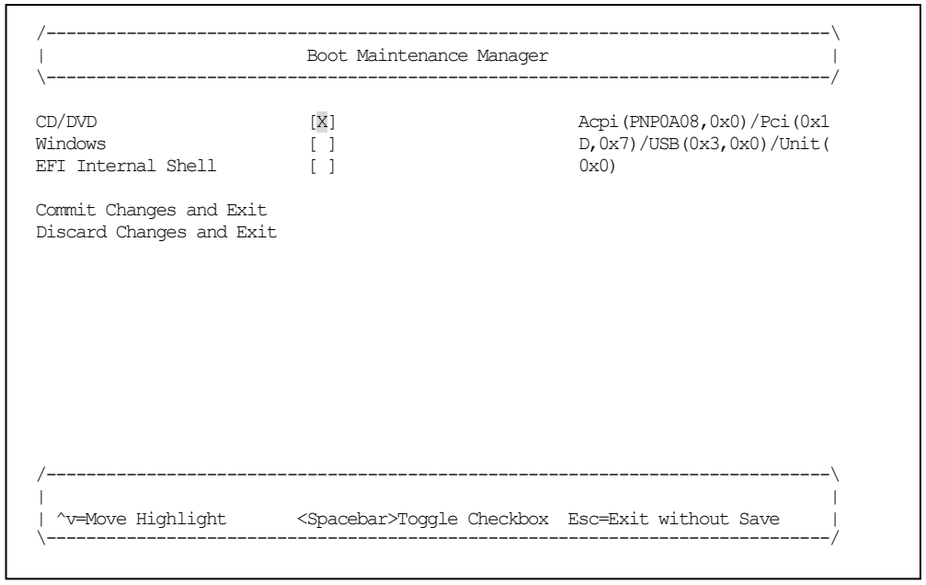
2 When the **Boot Maintenance Manager** screen is displayed, select **Boot Options**.



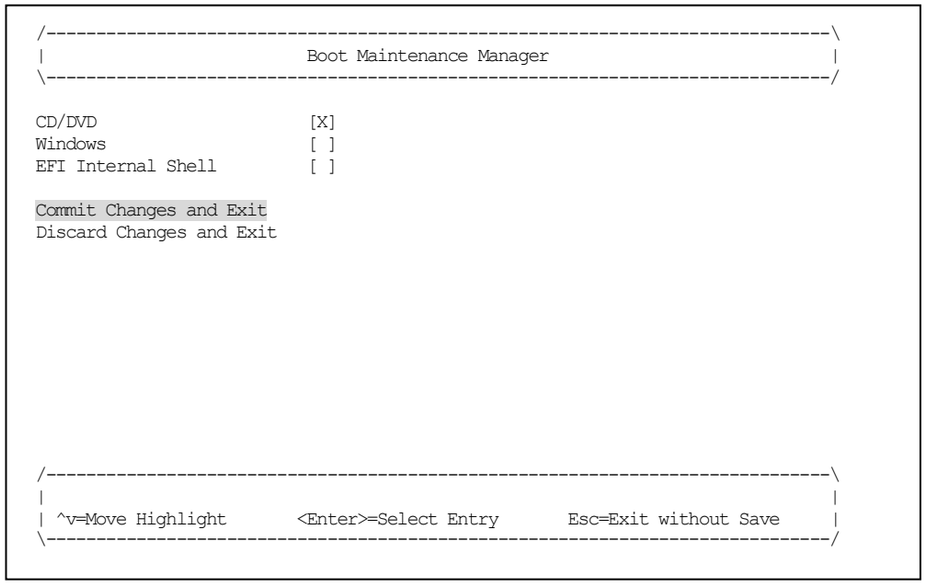
3 Select **Delete Boot Option**.



4 Select a boot option to delete by pressing the space key.



5 Select **Commit Changes and Exit**.



Guest OS display setting

It is recommended that the guest OS display should be set as described below when using the remote console. Set the display from the remote console. For maximum performance, the following display settings are recommended.

LPAR manager firmware version 59-4X/79-4X or earlier

Guest OS	Resolution (pixel)	Number of bits for colors
Windows	1024 x 768	16
Linux	1024 x 768	16

LPAR manager firmware version 59-5X/79-5X or later

Guest OS	Resolution (pixel)	Number of bits for colors
Windows	1024 x 768	32
Linux	1024 x 768	24

The following describes how to set resolution to 1024 x 768 pixels and 16-bit color. If setting other bits for color, replace the16-bit with bits you want to set.

❑ Windows display setting

It is recommended that the resolution should be set to 1024x768 pixel and 16-bit per color using the standard VGA driver.

Windows Server 2008/Windows Server 2008 R2 as the guest OS

Set the OS following the steps below.

Set 1024x768 pixels for the screen resolution setting, and medium 16-bit for color. Click **OK**.

When the confirmation dialog appears, click **Yes**.

Here completed the display setting for Windows Server 2008/Windows Server 2008 R2.

Windows Server 2003 R2 as the guest OS

Set the OS following the steps below.

Set 1024x768 pixels for resolution of screen setting, medium 16-bit for color. Click **OK**.

When the confirmation dialog appears, click **Yes**.

Here completed the display setting for Windows Server 2003 R2.

❑ Linux display setting



If you click GUI: System > Management > Display or System > Preferences > Screen Resolution to set the screen resolution, the setting values might not properly take effect or the screen might be disturbed after the setting. If so, open /etc/X11/xorg.conf in a text editor to edit the resolution.

The Setting procedure for Red Hat Enterprise Linux 5 is as follows.

Open “/etc/x11/xorg.conf” using the editor, and set the following.

1 In /etc/X11/xorg.conf, select **Section “Device” > Driver**, and confirm that **Driver** is **vesa**. If not, change it to **vesa**.

Setting example: **Section “Device”**

```
Section “Device”
    Identifier      “Videocard0”
    Driver          “vesa”
EndSection
```

2 /etc/X11/xorg.conf has not **Section “Monitor or Section “Screen” – Monitor** line, create a new one referring to the examples described below.

Section “Screen” > SubSection ”Display” > Modes, and set **Modes** to “1024x763”. If **Modes** does not exist, create a new one.

Select **Section “Screen” – DefaultDepth** or **Section “Screen” > SubSection “Display” > Depth**, and set “16”, which is our recommended value, to each of them. If setting 24 bits, set “24”.

Setting example: **Section “Monitor”**

```
Section “Monitor”
    Identifier      “Monitor0”
    ModelName       “LCD Panel 1024x768”
    HorizSync 31.5 – 48.0
    VertRefresh     56.0 – 65.0
    Option          “dpms”
EndSection
```

Setting example: **Section “Screen”**

```
Section “Screen”
    Identifier “ Screen0”
    Device          “Videocard0”
    Monitor         “Monitor0”
    DefaultDepth    16 <<< If setting 24 bits, replace 16 with 24.
    Subsection “Display”
        Viewport: 0 0
        Depth: 16 <<< If setting 24 bits, replace 16 with 24.
        Modes: “1024x768”
    EndSubSection
EndSection
```

Here completed the Linux display setting.

Reboot the X server to reflect the resolution setting.

Set the resolution and pixel with “/etc/x11/xorg.conf”. If using GUI **System-Management-Display** or **System-Setting-Resolution**, the setting of resolution or pixel might not be reflected correctly or the screen might be disturbed after the setting.

Shutdown guest OS and deactivate LPAR

1 Use the **Shutdown** command from the operating system command line.

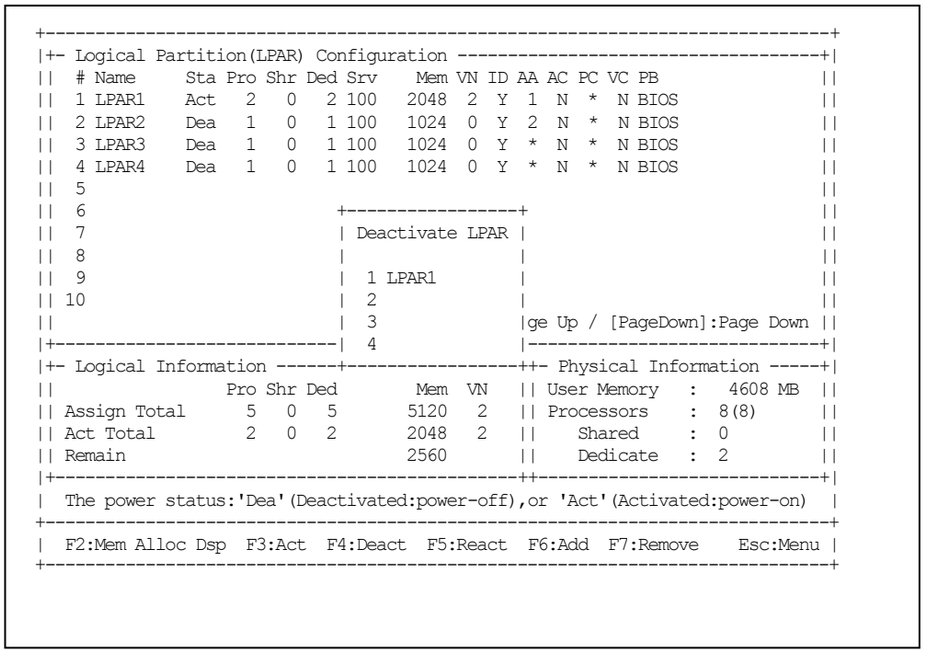
Execute (Enter) the **Shutdown** command from the OS command line or GUI.

Once the Shutdown processing is finished, the LPAR is deactivated.

2 Deactivate a LPAR from the LPAR manager screen.

On the **LP Menu** or LP Menu or **Logical Partition Configuration** screen, press **F4: Deact**.

On the subscreen, select the LPAR to deactivate using the cursor and press **Enter**.



When a subscreen to confirm Deactivate: power-off appears, select **Yes**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta Pro Shr Ded Srv    Mem VN ID AA AC PC VC PB                ||
||  1 LPAR1    Act   2   0   2 100   2048  2  Y  1  N  *  N BIOS              ||
||  2 LPAR2    Dea   1   0   1 100   1024  0  Y  2  N  *  N BIOS              ||
||  3 LPAR3    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS              ||
||  4 LPAR4    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS              ||
||  5                                                                         ||
||  6                +-------------------------------+                      ||
||  7                |         LPAR1[LPAR1]          |                      ||
||  8                | Deactivation means power-off. |                      ||
||  9                |        Do you continue?       |                      ||
|| 10                |                               |                      ||
||                   |             Yes               | [PageDown]:Page Down ||
|+-------------------|              No               |----------------------+|
|+- Logical Information|     Yes(Don't ask anymore)    |ical Information -----+|
||                Pro +-------------------------------+Memory   :   4608 MB  ||
|| Assign Total     5   0   5       5120   2   || Processors    :  8(8)      ||
|| Act Total        2   0   2       2048   2   ||    Shared     :  0         ||
|| Remain                           2560       ||    Dedicate   :  2         ||
|+-------------------------------------------++-----------------------------+|
|  The power status:'Dea'(Deactivated:power-off),or 'Act'(Activated:power-on)  |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```

■ Example of Logical Partition Configuration display after deactivating LPAR1

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta Pro Shr Ded Srv    Mem VN ID AA AC PC VC PB                ||
||  1 LPAR1    Dea   2   0   2 100   2048  2  Y  1  N  *  N BIOS              ||
||  2 LPAR2    Dea   1   0   1 100   1024  0  Y  2  N  *  N BIOS              ||
||  3 LPAR3    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS              ||
||  4 LPAR4    Dea   1   0   1 100   1024  0  Y  *  N  *  N BIOS              ||
||  5                                                                         ||
||  6                                                                         ||
||  7                                                                         ||
||  8                                                                         ||
||  9                                                                         ||
|| 10                                                                         ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down ||
|+-------------------------------------------------------------------------------+|
|+- Logical Information ------------------------++- Physical Information -----+|
||                Pro Shr Ded        Mem  VN    || User Memory   :   4608 MB  ||
|| Assign Total     5   0   5       5120   2   || Processors    :  8(8)      ||
|| Act Total        0   0   0          0   0   ||    Shared     :  0         ||
|| Remain                           4608       ||    Dedicate   :  0         ||
|+-------------------------------------------++-----------------------------+|
|  Logical partition name                                                      |
+-------------------------------------------------------------------------------+
|  F2:Mem Alloc Dsp  F3:Act  F4:Deact  F5:React  F6:Add  F7:Remove    Esc:Menu |
+-------------------------------------------------------------------------------+
```



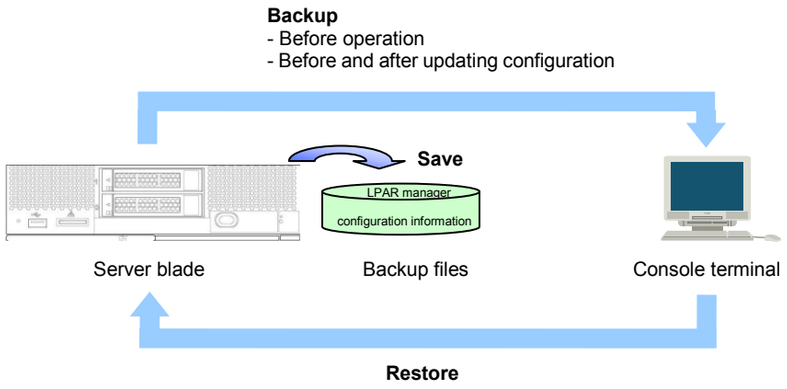
- Deactivating a LPAR is equivalent to turning off the power supply of the LPAR, so due care should be taken when performing this operation. In particular, the hard disk might get damaged if you perform this operation while data is being accessed on the LPAR such as booting the guest OS. We strongly recommend that you shutdown the guest operating system before deactivating it.
- If LP auto shutdown is set, the LPAR manager system will automatically shutdown once all the LPARs have been deactivated. See Options for more on LP auto shutdown.

Backup of LPAR manager

This section describes backing up the LPAR manager configuration.

Backup Files for LPAR manager

- Create a backup file for LPAR manager before starting operations after setting up the LPAR manager or performing Operations in need to back up files.
- When in failure, backup files of LPAR manager configuration information allow you to rapidly recover the system. It is recommended that you back up LPAR manager configuration information on a regular basis in case you need to restore the LPAR manager configuration in normal operation.
- Hardware failure may cause a device to be degenerated or isolated. LPAR manager cannot recognize degenerated or isolated devices, and a part of LPAR manager configuration information related to the devices will be deleted or reconfigured. If this happens, restore the backup files after hardware is replaced by service personnel. For notes and restrictions on degeneration and isolation, see Degeneration/Isolation of Processors, Memories, and PCI Devices and Degeneration of Processor Cores.



❑ Operations in need to back up files

Create backup files before the following operations

- Changing hardware configuration or settings
  - Adding or removing processors, changing settings for hyper-threading, or changing settings for planned degeneration;
  - Adding or removing memory or changing settings for planned degeneration;
  - Adding or removing a mezzanine card or PCI card, or changing card types;
  - Adding or removing an I/O slot expansion unit, or changing operating modes
  - Changing SMP configurations between server blades

Create backup files after the following operations

- Changing LPAR manager configurations
  - Changing LPAR manager system settings;
  - Adding, removing, or reconfiguring LPAR;
  - Changing settings for LPAR manager boot order
  - Changing settings for LPAR manager EFI driver

❑ Methods for saving, backing up, and restoring LPAR manager configuration

You can save, back up, and restore LPAR manager configuration information using the following methods.

Operation status	Method	Save	Back up	Restore
Not in operation	LPAR manager screen	N/A	N/A	N/A
	HVM Navigator	N/A	N/A	N/A
	System Web console System console	N/A	✓	✓
	SC/BSM	N/A	✓	✓
In operation	LPAR manager screen	✓	N/A	N/A
	HVM Navigator	✓	N/A	N/A
	System Web console System console	N/A	✓	✓
	SC/BSM	✓	✓	✓

(✓): Available

(N/A): Not available

❑ Creating backup files

Save LPAR manager configuration information to create backup files and keep them safe from loss.

For detailed operation information, see the *HVM Navigator User's Guide - LPAR Configuration* or *ServerConductor/Blade Server Manager Series Administration Guide*.

❑ Restoring backup files

Restore backup files of LPAR manager configuration information created in Creating backup files.

Check the LPAR manager system time and OS system time. If with a time lag between them, set the time.

For detailed operation information, refer to this manual or see the *ServerConductor/Blade Server Manager Series Administration Guide*.

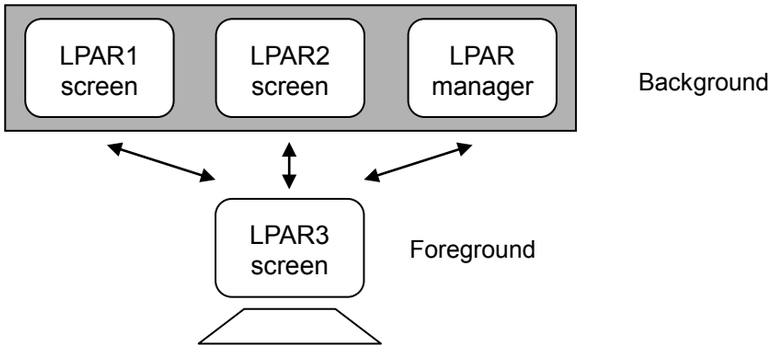
LPAR manager screen operations

This section describes LPAR manager operations using terminal software.

LPAR manager screen display

Using terminal software, you can perform LPAR manager operations and operations on each guest OS. You cannot perform LPAR manager operations and operations on multiple guest OSes at the same time. You must switch the LPAR manager or guest OS in order to perform operations.

The LPAR manager or guest screen that is displayed is said to be in the *foreground*. Other screens are in the *background*. When you move a LPAR manager or guest screen into the foreground, the screen in the foreground then will automatically move to the background.



The display of the guest screen in the background is saved by LPAR manager in the internal buffer. When that screen becomes the foreground, it reflects to its most recent state on the serial terminal. Even when a guest screen is in the background, it does not lose any of the displayed information.

The following table describes main uses of each screen.

Screen	Function
LPAR manager screen	Set the LPAR manager system configuration Define the LPAR configuration Activate/Deactivate LPAR
Guest screen	Boot the guest OS Execute the guest OS command
	Transmit the Break signal (*1)

*1 When enterirng the Break signal of IAC (Interpreted As Command) escape code defined in the telnet protocol from the OS console, the Break singnal is transmitted to the serial port of the LPAR whose guest screen is displayed.

The following table shows how to switch between screens.

Switch Direction	Key Operations	Description
From guest to LPAR manager	Ctrl + l	Press the **Ctrl** and **l** keys simultaneously on the guest screen to switch to the LPAR manager menu. The combination of keys used for screen switching can be changed on the Options screen.
From LPAR manager to guest	F8	When you press **F8** on the LPAR manager Menu screen or the Logical Partition Configuration screen, the activated LPARs become selectable. Select the LPAR that you would like to switch to the foreground and press **Enter**.

If you shut down a guest OS when its LPAR is in the foreground, the LPAR manager screen automatically returns to the foreground after the guest OS has finished shutting down.

When displaying the guest screen by using the virtual COM console, screens can be operated simultaneously without switching between the LPAR manager screen and guest screen.
See Virtual COM console function for how to use the virtual COM console.

Tip

- While you are using LPAR manager, garbage might remain on the screen and part of the screen is missing. If you switch to the SMP command mode with **Ctrl+B** and display the LPAR manager screen again, it is not displayed correctly. In this case, press **Alt+t** simultaneously to refresh the screen. The screen refreshing operation (**Alt+t** works on all HVM screens).
- If you continuously press an arrow key or a function key, the screen might switch as pressing **Esc**). If this occurs, display the previous screen once again and continue operations.
- If you activate or deactivate all LPARs from the ServerConductor/Blade Server Manager at a time, LPAR manager screen operations might become temporarily unavailable and the screen might look as if it has frozen. If this happens, wait for one minute or two and try the operation again.
- When any of the following symptoms occurs, press **Alt+t** simultaneously to refresh the screen.

  (1) The cursor remains rooted to **Esc:Menu** in the bottom right-hand corner of the screen, and cannot move by the arrow keys, even though there are selectable items in the screen.

  (2) The cursor remains over an item that is not selectable and cannot move by the arrow keys, even though there are other selectable items in the screen.

  (3) The cursor is not displayed, even though there are selectable items in the screen.

❑ Serial setting when using the guest screen

When using a guest screen, execute the following serial settings. When you have done the serial settings, skip these settings.

Windows Server 2003 R2

1 Execute the following command from the command prompt.

bootcfg /ems EDIT /port COM1
bootcfg /ems ON /baud 115200 /id 1

Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2012 R2

1 Execute the following command from the command prompt.

bcdedit/ems ON

bcdedit/emssettings EMSPORT:1 EMSBAUDRATE:115200

Red Hat Enterprise Linux 5

1 /boot/grub/grub.conf setting

1) Comment out the line “spashimage=(hd0,0)/grub/splash.xpm.gz”.
2) Add the following two lines between lines of hiddenmenu and title.
“serial --unit=0 --speed= 115200
“terminal --timeout=10 serial console”.
3) Add the following line at the end of the kernel line.
“console=tty0 console=ttyS0,115200”

2 /etc/sysconfig/init setting

Change “BOOTUP=color” to “BOOTUP=serial”.

3 /etc/sysconfig/kudzu setting

Change “SAFE=no” to “SAFE=yes”.

4 /etc/inittab setting

Add “co:2345:respawn]/sbin/agetty 115200 ttyS0vt100” to the bottom line.

5 /etc/securetty setting

1) Add ttyS0 at the bottom line.

Red Hat Enterprise Linux 6

1 /boot/grub/grub.conf setting

1) Comment out the line “spashimage=(hd0,0)/grub/splash.xpm.gz”.
2) Add the following two lines between lines of hiddenmenu and title.
serial --unit=0 --speed= 115200
terminal –timeout=10 serial console”.
3) Add the following line at the end of the kernel line.
console=ttyS0,15200” .

2 /etc/sysconfig/init setting

Change “BOOTUP=color” to “BOOTUP=serial”.

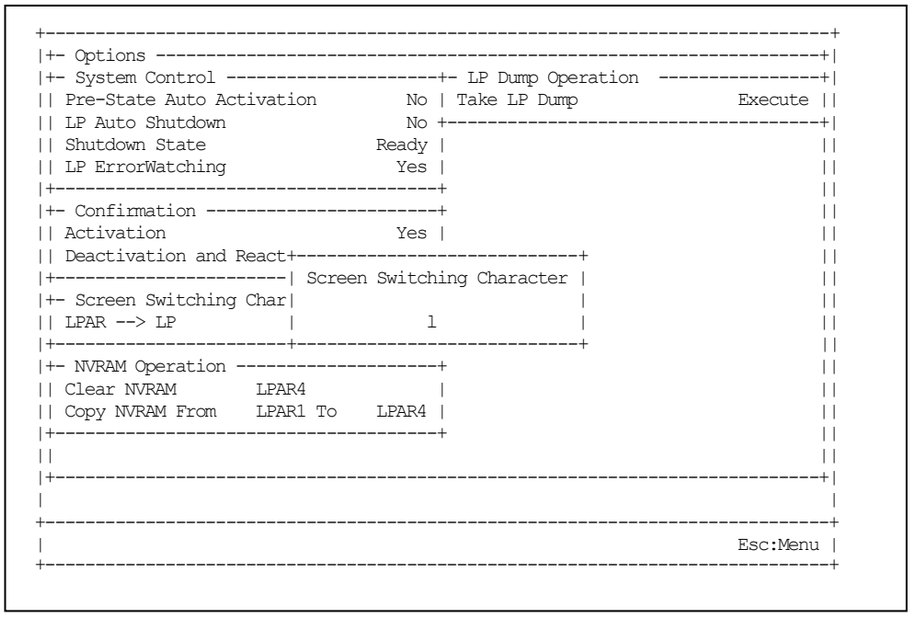
Move between guest and LPAR manager screens

❑ Moving from a guest screen to an LPAR manager screen

1 Press and hold the **Ctrl** key, and press the switching character.

The default switching character is "l" (lower case "L").

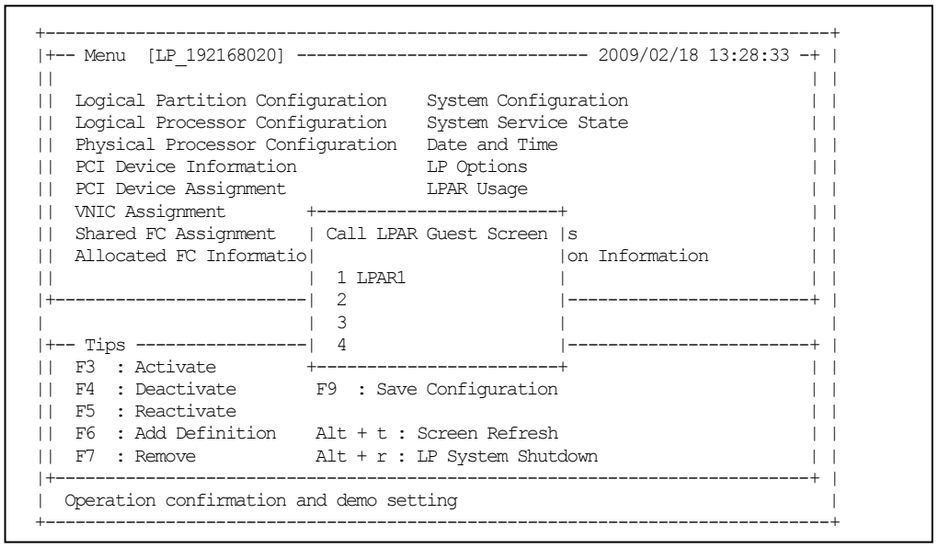
* You can change the switching character by changing the Screen Switching Character in Options. However, you cannot use b, h, i, j, m, q, s, and z, since these characters are reserved for the SVP console.



* If the LPAR has the virtual COM console enabled from which connected to the LPAR guest screen, you can operate the LPAR manager screen without this procedure.
See Virtual COM console function for how to use the virtual COM console.

❑ Moving from an LPAR manager screen to a guest screen

1. Press the **F8** key on the **LPAR manager Menu** screen.
2. On the subscreen, use the cursor to select the LPAR you wish to display the guest screen and press **Enter**.



* If the LPAR has the virtual COM console enabled, you can access the LPAR manager screen from the virtual COM console.
See Virtual COM console function for how to use the virtual COM console.

LPAR manager key operations

You can change or perform operations on any selected item on the LPAR manager screen by pressing **Enter**. Use the arrow keys to move the cursor.

The following table shows main keys and their functions.

#	Key	Operation/Role	Screen on which operation is performed
1	Arrow ([↑], [→], [↓], [←])	Moves the cursor to a selectable item. Used to increase or decrease the memory allocated to an LPAR or to set the time.	All screens
2	Tab	Moves the cursor to a selectable item.	All screens
3	Enter	Executes or changes the settings of the selected item. Sets the value in the subscreen for selecting (setting) values, and closes the subscreen.	All screens
4	Esc	Press Esc on any LPAR manager screen other than the LPAR manager Menu screen to display the LPAR manager Menu screen. Nothing will happen if you press Esc in the LPAR manager Menu screen. Cancels the selection in the subscreen, and closes the subscreen.	All screens other than the LPAR manager menu screen
5	Page Up	Scrolls the displayed page up. Selects the largest value in the subscreen for selecting values.	Screens that can be moved up or down Subscreens with which selects a value
6	Page Down	Scrolls the displayed page down. Selects the smallest value in the subscreen for selecting values.	Screens that can be moved up or down Subscreens with which selects a value
7	F1	Used to specify the size of the memory to be allocated to LPAR in GB units.	Memory allocation subscreen for LPAR Configuration screen
		Standard sever blades with LPAR manager firmware 58-4X or later versions/High-performance server blades with LPAR manager firmware 78-4X or later versions. Used to select a VC number and display VC numbers/Transmission Checksum Protocol (TCP)-port assignment.	LPAR Configuration subscreen to assign virtual COM for LPAR configuration screen
		Standard sever blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions Adds processor groups: Press the F1 key to display a subscreen where you can add a processor group. Select a target group number and press Enter	Physical Processor Configuration
8	F2	Displays the memory allocation status on a subscreen in the LPAR Configuration screen. For more about this function, see "(14) How to display memory allocation" under "Logical Partition Configuration" in "Summary of LPAR manager Screens".	LPAR Configuration

#	Key	Operation/Role	Screen on which operation is performed
		Displays the VLAN ID assignment and promiscuous mode setting list on a subscreen in the VNIC Assignment screen. For more about this function, “(5) How to display VLAN ID assignment list” under “VNIC Assignment and Promiscuous mode” in "Summary of LPAR manager Screens".	VNIC Assignment
		Standard sever blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions Deletes processor groups: Press the F2 key to display a subscreen where you can delete a processor group. Select a target processor number and press Enter.	Physical Processor Configuration
		Standard server blades with LPAR manager firmware version 58-7X or later/High-performance server blades with LPAR manager firmware version 78-7X or later Displays a subscreen of PCI device mapping information.	PCI Device Information
9	F3	Activates (powers on) an LPAR. When you press the F3 key, a subscreen where you can select the LPAR that you want to activate is displayed. Select the LPAR and press Enter. The subscreen will not be displayed if the LPARs are entirely undefined. If an LPAR is in an Activate state or a Failure state, its name will not be displayed and it cannot be selected by the cursor. When the number of defined LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
10	F4	Deactivates (powers off) an LPAR. When you press the F4 key, a subscreen where you can select the LPAR that you want to deactivate is displayed. Select the LPAR and press Enter. The subscreen will not be displayed if the LPARs are entirely undefined. If an LPAR is in a Deactivate state, its name will not be displayed and it cannot be selected by the cursor. When the number of defined LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
11	F5	Reactivates (restarts) an LPAR. When you press the F5 key, a subscreen where you can select the LPAR that you want to reactivate is displayed. Select the LPAR and press Enter. The subscreen will not be displayed if the LPARs are entirely undefined. If an LPAR is in a Deactivate state, its name will not be displayed, and it cannot be selected by the cursor. When the number of defined LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
		Switches USB devices assignment. When you press the F5 key, a subscreen where you can select the LPAR to attach the USB devices is displayed. Select the LPAR and press Enter.	PCI Device Assignment
		Sets the promiscuous mode. When you press the F5 key, a subscreen where you can select the promiscuous mode is displayed. Select the promiscuous mode and press Enter.	VNIC Assignment

#	Key	Operation/Role	Screen on which operation is performed
12	F6	Adds (defines) an LPAR. When you press the F6 key, a subscreen where you can select the LPAR that you want to add is displayed. Select the LPAR and press Enter. When the number of definable LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
		LPAR manager firmware version 59-0X/79-0X or later Changes USB automatic Attach settings. Point the cursor on A or R for USB assignment status, and press the F6 key to toggle between Set and Reset.	PCI Device Assignment
		Changes the MAC address. When you press the F6 key, a subscreen where you can select the MAC address that you want to change is displayed. Enter the new MAC address and press Enter.	VNIC Assignment
		Changes the LPAR manager display time. When you press the F6 key, a subscreen where you can change the LPAR manager display time is displayed. Enter the new LPAR manager display time, and press Enter.	Date and Time
13	F7	Deletes an LPAR. When you press the F7 key, a subscreen where you can select the LPAR that you want to delete is displayed. Select the LPAR and press Enter. The subscreen will not be displayed if the LPARs are entirely undefined. If an LPAR is in the Activate state or the Failure state, its name will not be displayed, and it cannot be selected by the cursor. When the number of defined LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
		Sets the VLAN mode. When you press the F7 key, a subscreen where you can select the VLAN mode that you want to add is displayed. Select the VLAN mode and press Enter.	VNIC Assignment
		Changes the time zone on the LPAR manager system. When you press the F7 key, a subscreen where you can select a time zone on the LPAR manager system is displayed. Select a new time zone and press Enter.	Date and Time
14	F8	Switches to display of a guest screen. When you press the F8 key, the activated LPARs become selectable. To switch screens, select the LPAR that you would like to move to the foreground and press Enter. The subscreen will not be displayed if the LPARs are entirely undefined. If an LPAR is in a Deactivate, its name will not be displayed and it cannot be selected by the cursor. When the number of defined LPARs is 18 or larger, arrow keys [←] or [→] are displayed.	LPAR manager Menu, LPAR Configuration
		For LPAR manager firmware 57-30 or later versions: Sets Inter-LPAR packet filtering. When you press the F8 key, a subscreen for packet filter selection is displayed. Select the Inter-LPAR Packet Filtering and press Enter.	VNIC Assignment
15	F9	LPAR manager firmware version 59-70/79-70 or later Sets transmission bandwidth limitation for VF NIC.	VNIC Assignment

#	Key	Operation/Role	Screen on which operation is performed
16	F10	Used to change the schedule mode for the PCI device.	PCI Device Assignment
		Used to reflect specific settings, such as logical partitioning manager (LP) identifier (ID) and VNIC System Number, in the LPAR manager system.	System Configuration
17	F11	Scrolls the displayed page to the left.	Any screen that can move to the left or right
18	F12	Scrolls the displayed page to the right.	Any screen that can move to the left or right
19	Alt + t	Refreshes the LPAR manager screen. ・ Resets the cursor position in the following screens: - Logical Partition Configuration, - Logical Processor Configuration, - PCI Device Assignment, - VNIC Assignment, - Shared FC Assignment - Date and Time, - Front Panel (Note) When the cursor position is reset, it is repositioned over the item with the lowest LPAR number defined in the above screens and at the far left within the selectable row. However, the cursor position is not set again even if Alt+t is executed while the subscreen is displayed during the LPAR setting or the like. ・ Forcibly displays the cursor. (Note) If there are no selectable items on the subscreen that is displayed by F3 ~ F8, the cursor will be hidden (positioned in the bottom left corner of the screen). This key operation forcibly displays the cursor. This might lead to a confusing screen display with the main screen and the subscreen overlapping.	All screens
20	Alt+r	Shutdown the LPAR manager system. After the shutdown process completed, the power of the server blade will turn off.	All screens
21	Ctrl+b	Returns to the system console of the management module.	All screens

Summary of LPAR manager screens

The following table shows the summary of the LPAR manager screens.

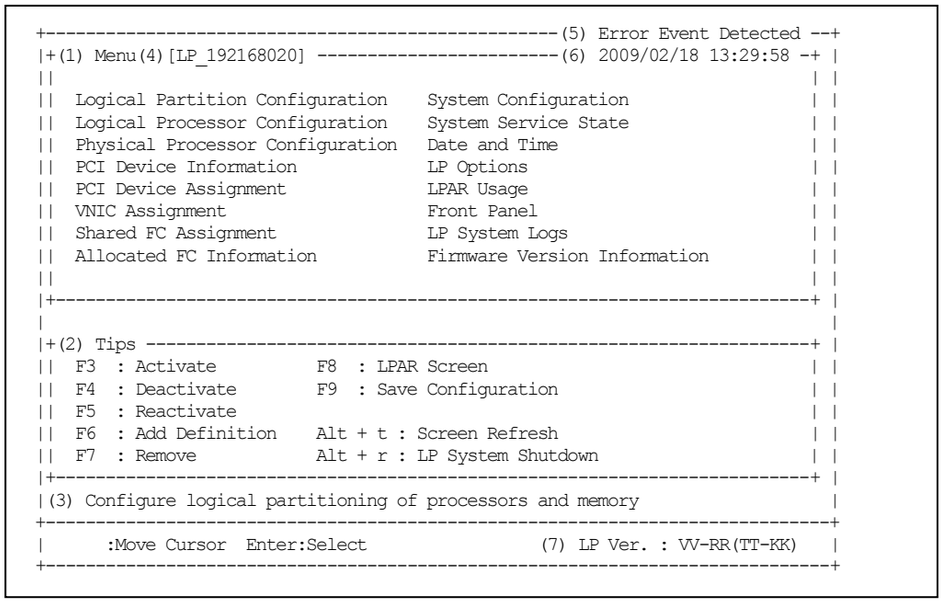
LPAR manager screens different from those in this manual might be displayed depending on LPAR manager firmware versions.

#	Screen Name	Main Use
1	LPAR manager menu	Displays the index screen of other LPAR manager screens.
2	Logical partition configuration	Sets the LPAR name, number of processors, and memory size. Also provides the switching function to the LPAR guest screens, and sets the LPAR activated (power-on) and deactivated (power-off).
3	Logical partition configuration	Configures the logical processors for the LPARs. Displays the name of the defined LPARs and their power status.
4	Physical processor configuration	Displays the configuration and status of the physical processors. Adds, deletes, or changes a processor group.
5	PCI device information	Displays the PCI device information.
6	PCI device assignment	Assigns PCI devices to the LPARs. Displays the name of the defined LPARs and their status.
7	Virtual NIC (VNIC) assignment	Assigns virtual NICs to the LPARs. The name and status of the defined LPAR are displayed.
8	Shared FC assignment	Assigns the shared mode Hitachi 4Gbps Fibre-channel adapter to the LPARs. The name and status of the defined LPAR are displayed.
9	Allocated FC information	Displays the configuration (WWN) of the FCs installed in LPAR manager.
10	System configuration	Sets the LPAR manager system configuration.
11	System service state	Displays the service status of the LPAR manager system.
12	Date and time	Sets the LPAR's SEL (System Event Log) time. Sets the LPAR's RTC (Real Time Clock) time. Sets the time zone. Sets the LPAR manager display time. Sets the time zone in the LPAR manager system. Adjusts the SEL time and RTC time to the LPAR manager system time or UTC time. The name and status of the defined LPAR are displayed.
13	Options	Sets the LPAR manager optional functions.
14	LPAR usage	Displays the usage status of the LPAR manager system and the LPARs.
15	Front panel	Collects guest dumps and guest screen data. The name and status of the defined LPAR are displayed.
16	LPAR manager system logs screen messages	Displays the various events that occurred in LPAR manager.
17	Firmware version information	Displays the firmware version of each component.

In addition, the relevant subscreen might be displayed when you select the setting items (by pressing Enter).

❑ LPAR manager menu

- Displaying the LPAR manager screen
- Switching to other LPAR manager screens



The following table describes all of the items displayed in the LPAR manager Menu screen.

#	Title	Description
(1)	Menu	Displays the title of the screen that can be displayed by the LPAR manager. In addition, select the title of each screen using ([↑], [→], [↓] or [←]),and press Enter. The display changes into the selected screen.
(2)	Tips	Lists the function keys and the shortcut keys available in this screen. F3: Activates an LPAR. F4: Deactivates an LPAR. F5: Reactivates an LPAR. F6: Adds an LPAR definition. F7: Removes an LPAR definition. F8: Switches from the LPAR manager screen to an LPAR screen. F9: Saves the LPAR manager configuration. Alt+t: Refreshes the LPAR manager screen display. Alt+r: Shutdown the LPAR manager system. Note: F3, F5, F6, and F7 are not available on the LPAR where LPAR migration has failed.
(3)	Comments	Displays a brief description of the selected item.
(4)	LPAR manager identifier	Displays ID to identify LPAR manager configured in the system configuration screen. See System configuration for the details of LPAR manager identifier
(5)	Error event detected	Displays that LP system logs at the error level are detected. When this is displayed, check the contents of the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, click the Esc button on this screen, or open the system logs screen.
(6)	System time	Displays the LPAR manager display time configured in the Date and Time screen. Not updated regularly. Updated when the screen is operated, or the screen requires Refresh in the LPAR manager. Use this as an approximate time.
(7)	LPAR manager firmware version	Displays the LPAR manager firmware version and the LPAR manager firmware internal version.

(1) How to Return to the LPAR manager Menu from Each LPAR manager screen

Press **Esc** on each **LPAR manager** screen. If there are no settable items on the displayed screen, the cursor is always positioned on the Esc:Menu display. Pressing Enter in this status returns to the LPAR manager Menu screen.

(2) How to Activate (turn on) an LPAR

Press **F3: Act** in this screen to display a subscreen, place the cursor on an LPAR to activate on the subscreen, and press **Enter**. You can perform “Activate” only to deactivated LPARs.

(3) How to Deactivate (Turn off) an LPAR

Press F4: Deact in this screen to display a subscreen, place the cursor on an LPAR to deactivate on the subscreen, and press **Enter**. You can perform “Deactivate” only to activated LPARs.

Always perform “Deactivate” carefully because it is equivalent to turning off an LPAR. It can damage the disk on which “Deactivate” is performed especially during data access such as guest OS boot. Thus, we recommend shutting down the OS instead of deactivating.



- When shutting down the guest OS in operation on an LPAR, the guest OS might hang up in the final process. If the guest OS hangs up, deactivate the LPAR. The disk will not be damaged because the LPAR has been disconnected from the disk.

(4) How to Reactivate an LPAR

Press F5: React in this screen to display a subscreen, place the cursor on an LPAR to reactivate on the subscreen, and press **Enter**. You can perform “Reactivate” only to activated LPARs.

Always perform “Reactivate” carefully because it is equivalent to rebooting the server blade. It can damage the disk on which “Reactivate” is performed especially during data access such as guest OS boot. We recommend that you reboot the OS instead of reactivating.



- When rebooting the guest OS in operation on an LPAR, the guest OS might hang up in the final process. If the guest OS hangs up, reactivate the LPAR. The disk will not be damaged because the LPAR has been disconnected from the disk.

(5) How to Add an LPAR

Press **F6: Add** in this screen to display a subscreen, place the cursor on an LPAR to add on the subscreen, and press **Enter**.

(6) How to Delete an LPAR

Press **F7: Remove** in this screen to display a subscreen, place the cursor on an LPAR to delete on the subscreen, and press **Enter**. You can delete only a deactivated LPAR. When an LPAR is deleted, all resources assigned to the LPAR will be unassigned

(7) How to Migrate from the LPAR manager screen to an LPAR screen

Press **F8: LPAR Screen** in this screen to display a subscreen, place the cursor on an LPAR which you migrate on the subscreen, and press **Enter**. You can select only an activated LPAR to migrate to the screen.

(8) How to Save configuration

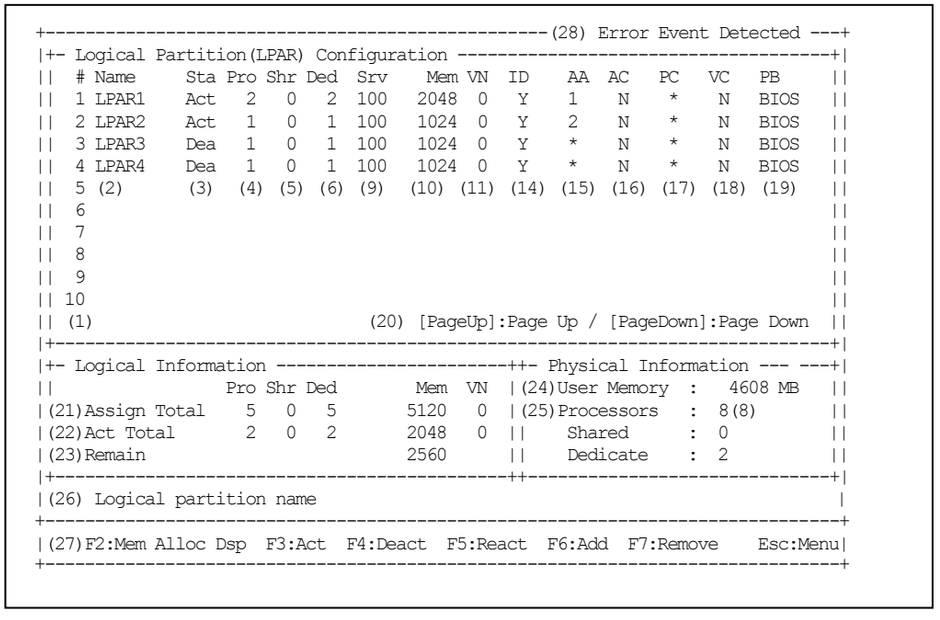
Press **F9: Save Configuration** in this screen.

❑ Logical partition configuration

Use the Logical Partition Configuration screen to do the followings.

- Add and remove a LPAR.
- Rename a LPAR.
- Set the number of processors, allocated memory size, service ratio, etc.
- Activate (power-on) and deactivate (power-off) LPARs.
- Display the system information, such as the configurable memory capacity, and the number of processors.
- Display the total amount of the memory capacity, the number of processors and virtual NIC assigned to LPAR
- Display the total capacity of memory, the number of processors, and number of virtual NICs of active LPARs.
- Displays the configurable memory capacity left to be used by LPAR

For: Standard server blades with LPAR manager firmware version 58-2X or earlier versions;
High-performance server blades with LPAR manager firmware version 78-2X or earlier veriosns



For: Standard server blades with LPAR manager firmware version 58-3X or later versions;
High-performance server blades with LPAR manager firmware version 78-3X or later versions

```
+-------------------------------------------------(28) Error Event Detected -----+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta  Scd  Pro  Grp Srv   Mem  VN  PN  MN  ID  AA  AC  PC  VC  PB  ||
||  1 LPAR1    Act    D    2    0 100   2048  0   A   A   Y   *   N   *   N BIOS ||
||  2 LPAR2    Dea    D    1    0 100   1024  0   A   A   Y   *   N   *   N BIOS ||
||  3 LPAR3    Dea    D    1    0 100   1024  0   A   A   Y   *   N   *   N BIOS ||
||  4 LPAR4    Dea    D    1    0 100   1024  0   A   A   Y   *   N   *   N BIOS ||
||  5 (2)      (3)   (7)  (4)  (8) (9)  (10) (11)(12)(13)(14)(15)(16)(17)(18)(19)||
||  6                                                                            ||
||  7                                                                            ||
||  8                                                                            ||
||  9                                                                            ||
|| 10                                                                            ||
|| (1)                              (20) [PageUp]:Page Up / [PageDown]:Page Down  ||
|+-----------------------------------------------------------------------------+|
|+- Logical Information ----------------------++- Physical Information ---------+|
||                Pro Shr Ded        Mem  VN  |(24)User Memory  :   4608 MB --  ||
|(21)Assign Total   5   0   5       5120   0  |(25)Processors   :  8(8)     --  ||
|(22)Act Total      2   0   2       2048   0  ||    Shared      :  0        --  ||
|(23)Remain                         2560      ||    Dedicate    :  2       --  ||
|+-----------------------------------------++-----------------------------------+|
|(26) Logical partition name                                                    |
+-------------------------------------------------------------------------------+
|F1:VCAssign F2:MemAllocDsp F3:Act F4:Deact F5:React F6:Add F7:Remove  Esc:Menu  |
+(27)-----------------------------------------------------------------------------+
```

For: Standard server blades with LPAR manager firmware version 59-5X or later versions;
High-performance server blades with LPAR manager firmware version 79-5X or later versions

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Configuration ------------------------------------+|
||  # Name     Sta   OSType                                                    ||
||  1 LPAR1    Act  Solaris                                                    ||
||  2 LPAR2    Dea  Default                                                    ||
||  3 LPAR3    Dea  Default                                                    ||
||  4 LPAR4    Dea  Default                                                    ||
||  5              (29)                                                       ||
||  6                                                                         ||
||  7                                                                         ||
||  8                                                                         ||
||  9                                                                         ||
|| 10                                                                         ||
||                                  [PageUp]:Page Up / [PageDown]:Page Down   ||
|+- Logical Information ---------------------++- Physical Information --+|
||                 Pro  Shr  Ded         Mem  VN || User Memory  : 15104    ||
||  Assign Total     5    0    5        5120   8 || Processors   : 16(16)   ||
||  Act Total        2    0    2        2048   2 ||    Shared    : 0        ||
||  Remain                            13056     ||    Dedicate  : 2        ||
|+-----------------------------------------++-------------------------+|
|  OS Type                                                                  |
+-------------------------------------------------------------------------------+
|F1:VCAssign F2:MemAllocDsp F3:Act F4:Deact F5:React F6:Add F7:Remove           |
|F8:LPARScreen  F9:SaveConfig  F11:Left  F12:Right                   Esc:Menu|
+-------------------------------------------------------------------------------+
```

The following table describes items in the Logical Partition Configuration screen.

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(1)	#	LPAR Number	Displays LPAR numbers.	-
(2)	Name	LPAR Name	Sets the LPAR name.	NO_NAME
(3)	Sta	Status	Displays the LPAR status. Act (Activated): The LPAR is powered on. Dea (Deactivated): The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot LPAR manager when this happens. Activate, deactivate and reactivate the LPAR.	Dea
(4)	Pro	Logical Processors	LPAR manager firmware 58-2X/78-2X or lower Displays the number of logical processors allocated to the LPAR.	1
			LPAR manager firmware 58-3X/78-3X or later Sets the number of logical processors to allocate to the LPAR.	
(5)	Shr	Shared Processors	LPAR manager firmware 58-2X/78-2X or lower Sets the number of shared processors allocated to the LPAR.	0
(6)	Ded	Dedicated Processors	LPAR manager firmware 58-2X/78-2X or lower Sets the number of dedicated processors allocated to the LPAR.	1
(7)	Scd	Scheduling Mode	LPAR manager firmware 58-3X/78-3X or later Sets a scheduling mode. S: Shared mode D: Dedicated mode	D
(8)	Grp	Processor Group	LPAR manager firmware 58-3X/78-3X or later Sets a processor group number.	D
(9)	Srv	Service Ratio	Set a value between 1 and 999 as the relative allocation of the time (Service ratio) an LPAR uses a physical processor (Service-time). This item is only for shared mode LPARs. It is not for dedicated mode LPARs and cannot be set for them.	100
(10)	Mem	Memory	Sets the memory size allocated to a LPAR in units of MB. This is always a multiple of 256.	1024
(11)	VN	Virtual Network Interface Card	Displays the number of virtual NICs allocated to the LPAR.	0

<table>
<tr><th>#</th><th>Title</th><th>Official Name</th><th>Description</th><th>Initial Value (When LPAR is added)</th></tr>
<tr><td>(12)</td><td>PN</td><td>Processor Node</td><td>LPAR manager firmware version 59-2X/79-2X or later
<NUMA: disabled>
Displays the processor node assigned to the LPAR. Processor node cannot be set.
・ Deactivate
A: Node will be automatically selected when the LPAR is activated.
・ Activate
A: Node is automatically selected.
<NUMA: enabled>
Displays the processor node assigned to the LPAR. Processor node cannot be set.
・ Deactivate
A: Node will be automatically selected when the LPAR is activated.
・ Activate
0 to the maximum node number: Node numbers displayed are assigned.
M: Multiple nodes are assigned.
The following table shows displayed processor node.
<table>
<tr><th>NUMA setting</th><th>Deactivate</th><th>Activate</th></tr>
<tr><td>Disabled</td><td>A</td><td>A</td></tr>
<tr><td>Enabled</td><td>A</td><td>0 to the max # or M</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr><th>#</th><th>Title</th><th>Official Name</th><th>Description</th><th>Initial Value (When LPAR is added)</th></tr>
<tr><td>(13)</td><td>MN</td><td>Memory Node</td><td>LPAR manager firmware version 59-2X/79-2X or later
<NUMA: disabled>
Displays the memory node assigned to the LPAR. Memory node cannot be set.
・ Deactivate
A: Node will be automatically selected when the LPAR is activated. Blank memories are assigned in ascending order.
・ Activate
A: Node is automatically selected. Blank memories are assigned in ascending order.
<NUMA: enabled>
Sets memory node to be assigned to the LPAR.
・ Deactivate
A: Node will be automatically selected. Blank memories are assigned in ascending order.
0 to the maximum node number: Blank memories of the node will be assigned automatically in ascending order when the LPAR is activated are assigned. Memories of nodes other than those not set are not assigned.
・ Activate
0 to the maximum node number: Only nodes displayed are assigned.
M: Multiple nodes are assigned.
The following table shows displayed memory items.<table><tr><th>NUMA setting</th><th>Deactivate</th><th>Activate</th></tr><tr><td>Disabled</td><td>A</td><td>A</td></tr><tr><td>Enabled</td><td>A or 0 to the max #</td><td>0 to the max # or M</td></tr></table></td><td></td></tr>
<tr><td>(14)</td><td>ID</td><td>Idle Detection</td><td>Enables/disables the function that detects the idle state of the logical processors.
Y: Enables Idle Detection.
N: Disables Idle Detection.
Set Y (default value) to an LPAR in dedicated mode.</td><td>Y</td></tr>
<tr><td>(15)</td><td>AA</td><td>Auto Activation Order</td><td>Sets the automatic activation of a LPAR when LPAR manager boots.
*: Auto Activate is not set.
1-99: Enables Auto Activate. The number represents the order in which the LPARs are activated. Small number is given priority.</td><td>*</td></tr>
<tr><td>(16)</td><td>AC</td><td>Auto Clear</td><td>Enables/disables the function that automatically clears the logical SEL.
Y: Enables Auto Clear.
N: Disables Auto Clear.</td><td>N</td></tr>
</table>

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(17)	PC	Processor Capping	Enables/disables the Processor Capping function. Y: Enables the Processor Capping when using shared logical processors N: Disables the Processor Capping when using shared logical processors *: For logical processors in dedicated mode, the processor capping function is invalid. This item is available only for shared mode LPARs. It is not for dedicated mode LPARs and cannot be set for them.	*
(18)	VC	Virtual Console	Enables/disables the virtual COM console function, or specifies a VC number. Y: Enables the virtual COM console. N: Disables the virtual COM console. High-performance server blades with LPAR manager firmware 78-4X or later versions LPAR manager firmware 58-4X/78-4X or later versions 1-16: Specify a VC number of the virtual COM console with the F1 key.	N
(19)	PB	Pre-boot Firmware	Specify the Pre-boot firmware. BIOS:Start the logical BIOS by activating LPAR.	BIOS
(20)	Page Up / Page Down key	Page Up / Page Down	Page Up: Scrolls a page of the screen upwards. Page Down: Scrolls a page of the screen downwards.	-
(21)	Assign Total	Total resources allocated to LPAR	Displays the total resources on all the LPARs. Pro: Displays the total number of logical processors. Shr: Displays the total number of logical processors in the sharing mode. Ded: Displays the total number of logical processors in the occupation mode. Mem: Displays the total memory amount in megabytes. VNI: Displays the total number of virtual NICs.	-
(22)	Act Total	Total resources used by LPARs	Displays the total resources on all the LPARs which are activated. Pro: Displays the total number of logical processors. Shr: Displays the total number of logical processors in the sharing mode. Ded: Displays the total number of logical processors in the occupation mode. Mem: Displays the total memory amount in megabytes. VNI: Displays the total number of virtual NICs.	-
(23)	Remain	Configurable memory	Displays the remains of configurable memory to be used by LPARs in MB: Total memory for LPAR minus total memory currently used by LPAR. Memory, isolated due to failure detected, will not affect this item to display.	-

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(24)	User Memory	User memory	Displays the total amount of memory that can be allocated to the LPARs in units of MB. Displays the memory capacity installed in the server blade minus the amount used by LPAR manager. Memory, isolated due to failure detected, will not affect this item to display.	-
(25)	Processors	Number of processors	Displays the total number of physical processors. The format is "n(m)". n: Displays the total number of physical processors that are normally active. m: Displays the total number of physical processors installed in the server blade. Displays the total number of physical processors per mode. Shared: Displays the total number of physical processors in the shared mode. Dedicate: Displays the total number of physical processors in the dedicated mode. When SMT is enabled, the number of threads is displayed. When SMT is disabled, the number of cores is displayed.	-
(26)	Comment	Comments	Displays a brief description of the selected item.	-
(27)	Function Key	Function key	Displays the function keys that can be used on this screen. F1: Specifies the size of the memory to be allocated to LPAR in GB units, to specify a VC number, or to display assignments of VC number/TCP port. F2: Displays the memory allocation status. F3: Activates a LPAR. F4: Deactivates a LPAR. F5: Reactivates a LPAR. F6: Adds a LPAR definition. F7: Removes a LPAR definition. In addition, the following function keys can be used in this screen, although they are not shown due to the amount of display space available. F8: Switches from the LPAR manager screen to a Guest screen. F9: Saves the LPAR manager configuration. F11: Scrolls the screen to the left to display the area. F12: Scrolls the screen to the right to display the area. Note: F3, F5, F6, and F7 are not available on the LPAR where LPAR migration has failed.	-
(28)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the contents of the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the ESC key with this screen or open the system logs screen.	

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(29)	OSType	OS Type	LPAR manager firmware version 59-5X/79-5X or later Sets an OS type to boot on an LPAR. Default: Boots Linux or Windows. Solaris: Boots Solaris.	

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	✓	-	
(3)	Sta	✓	✓	-	
(4)	Pro	Standard server blades with LPAR manager firmware 58-2X or earlier versions/High-performance server blades with LPAR manager firmware 78-2X or earlier versions			
		-	-	-	Display only
		Standard server blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions			
		-	✓	-	
(5)	Shr	-	✓	-	
(6)	Ded	-	✓	-	
(7)	Scd	✓	✓	-	
(8)	Grp	Δ (Can be changed only in shared mode.)	✓	-	
(9)	Srv	Δ	Δ	-	Can be changed only in shared mode.
(10)	Mem	-	✓	-	
(11)	VN	-	-	-	Display only
(12)	PN	-	-	-	Display only
(13)	MN	-	Δ	-	Only with NUMA enabled
(14)	ID	✓	✓	-	
(15)	AA	-	✓	-	
(16)	AC	-	✓	-	
(17)	PC	Δ	Δ	-	Can be changed only in shared mode.
(18)	VC	✓	✓	-	
(19)	PB	-	✓	-	
(20)	OSType	-	✓	-	

✓: can be changed -: cannot be changed Δ: can be changed with conditions

(1) How to rename an LPAR

Open the **Logical Partition Configuration** screen. Move the cursor over the name of the LPAR that you want to rename. The name is displayed at the beginning of the row under the **Name** column. Press **Enter** to display a subscreen for renaming the LPAR. After entering the new name, press **Enter**.

The LPAR name can be set at up to 31 characters. You cannot give a different LPAR the same name. The LPAR name can be changed only when the relevant LPAR is inactive.

If the LPAR name consists of nine or more characters, the eighth character is represented as ~ and the ninth and subsequent characters are omitted. You can use the characters "0~9", "a~z", "A~Z", "-", and "_" in the LPAR name, but the first character in a LPAR name must be a letter: "a~z", or "A~Z".

(2) How to activate (power-on) an LPAR

Open the **Logical Partition Configuration** screen. Move the cursor over the **Sta** column of the LPAR row that you want to activate, and press **Enter**. Move the cursor over **Activate** on the displayed subscreen and press **Enter**.

You can also activate a LPAR by pressing **F3** in the **Logical Partition Configuration** screen. Move the cursor over the LPAR that you want to activate on the displayed subscreen and press **Enter**.

This activation operation works only on LPARs that are deactivated.

(3) How to deactivate (power-off) an LPAR

Open the **Logical Partition Configuration** screen. Move the cursor over the **Sta** column of the LPAR row that you want to deactivate, and press **Enter**. Move the cursor over **Deactivate** on the displayed subscreen and press **Enter**.

You can also deactivate a LPAR by pressing **F4** in the **Logical Partition Configuration** screen. Move the cursor over the LPAR that you want to deactivate on the displayed subscreen and press **Enter**.

This deactivation operation works only on LPARs that are activated.

LPAR deactivation is equivalent to server power-off. Caution is necessary in performing this operation especially if performed during data access (such as starting a guest OS). Because a disk might be damaged, we recommend shutting down the guest OS instead of deactivation.



- When shutting down the guest OS in operation on an LPAR, the guest OS might hang up in the final process. If the guest OS hangs up, deactivate the LPAR. The disk will not be damaged because the LPAR has been disconnected from the disk.

(4) How to reactivate an LPAR

Open the **Logical Partition C**onfiguration screen. Move the cursor over the **Sta** column of the LPAR row that you want to reactivate, and press **Enter**. Move the cursor over **Reactivate** on the displayed subscreen and press **Enter**.

This reactivation operation works only on LPARs that are activated.

LPAR reactivation is equivalent to server restarting. Caution is necessary in performing this operation especially if performed during data access (such as starting a guest OS). Because a disk might be damaged, we recommended restarting the guest OS instead of reactivation.

Note

- When rebooting the guest OS in operation on an LPAR, the guest OS might hang up in the final process. If the guest OS hangs up, reactivate the LPAR. The disk will not be damaged because the LPAR has been disconnected from the disk.

(5) How to change the number of shared processors to allocate to an LPAR
Standard server blades with LPAR manager firmware 58-2X or earlier versions/High-performance server blades with LPAR manager firmware 78-2X or earlier versions

Open the **Logical Partition Configurat**ion screen. Move the cursor over the **Shr** column of the LPAR whose number of shared processors you want to change, and press **Enter**. This will open a subscreen where you can select the number of processors. Enter the desired number of processors, and press **Enter**. The number of shared processors can be changed only when the relevant LPAR is inactive

Note

You can assign the number of logical processors the same as or less than that of physical processors available in shared mode to an LPAR in shared mode. If you assign more logical processors than physical processors to an LPAR in shared mode, performance might extremely slow down.

It is recommended that the total number of logical processors assigned to an LPAR in shared mode should be four times or less than the number of physical processors available in shared mode.

(6) How to change the number of dedicated processors allocated to an LPAR
Standard server blades with LPAR manager firmware 58-2X or earlier versions/High-performance server blades with LPAR manager firmware 78-2X or earlier versions

Open the **Logical Partition Configuration** screen. Move the cursor over the **Ded** column of the LPAR whose number of dedicated processors you want to change, and press **Enter**. This will open a subscreen where you can select the number of processors. Enter the desired number of processors, and press **Enter**. The number of occupied processors can be changed only when the relevant LPAR is inactive.

(7) How to change scheduling modes of an LPAR

Standard server blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions

Display the **Logical Partition Configuration** screen. Place the cursor on the intersection between the LPAR line to change the scheduling mode and **Scd** column, and press **Enter** to display a subscreen. Type a scheduling mode to configure, and press **Enter** on the subscreen.

You can change scheduling modes between Dedicated and Shared dynamically without deactivating the LPAR. If one of the following conditions is met, however, an error message will appear to terminate the screen.

(a) Sufficient physical processors do not exist for assigning all logical processors in shared mode to the groups assigned to the LPAR, when the shared mode is dynamically changed to the dedicated mode.

(b) A physical processor, not belonging to the LPAR group, is included in the physical processor assignment on the Logical Processor Configuration screen, when the shared mode is dynamically changed to the dedicated mode.

(8) How to change the number of physical processors to assign to an LPAR

Standard server blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions

Display the **Logical Partition Configuration** screen. Place the cursor on the intersection between the LPAR line to change the logical processor number and **Pro** column, and press **Enter** to display a subscreen. Type the number of logical processors to configure, and press **Enter** on the subscreen.



You can assign the number of logical processors the same as or less than that of physical processors available in shared mode to an LPAR in shared mode. If you assign more logical processors than physical processors to an LPAR in shared mode, performance might extremely slow down.

It is recommended that the total number of logical processors assigned to an LPAR in shared mode should be four times or less than the number of physical processors available in shared mode.

(9) How to change a processor group number of an LPAR

Standard server blades with LPAR manager firmware 58-3X or later versions/ High-performance server blades with LPAR manager firmware 78-3X or later versions

Display the **Logical Partition Configuration** screen. Place the cursor on the intersection between the LPAR line to change the processor group number and **Grp** column, and press **Enter** to display a subscreen. Select a processor group number of the LPAR to configure, and press **Enter** on the subscreen.

You can change a processor group number, when the LPAR is deactivated or activated in shared mode. If one of the following conditions is met, however, an error message will appear to terminate the screen.

(a) The scheduling mode of an LPAR is Shared and the LPAR is activated.

(b) No physical processor in shared mode exists in the group whose number is to be changed.

See (3) How to add a processor group and (1) How to change the number of a processor group for how to add and set a processor group number.

(10) How to change the service ratio allocation of processor shared between LPARS

Open the **Logical Partition Configuration** screen. Move the cursor over the **Srv** column of the LPAR whose processor service ratio you want to change, and press **Enter**. This will open a subscreen where you can enter a Service ratio value. Enter the desired service ratio (between 1 and 999), and press **Enter**.

Shared processor mode must be configured to change this setting.

Note

Set “the number of processors assigned to an LPAR multiplied by 250 ms” or greater as a service ratio. If not, processing performance might slow down under heavy load.

(11) How to change the memory size allocated to an LPAR

Open the **Logical Partition Configuration** screen. Move the cursor over the **Mem** column of the LPAR whose memory size you want to change, and press **Enter**. This will open a subscreen where you can enter the memory size. Adjust the memory size with the arrow keys ([↑], [→], [↓] or [←]), and press **Enter**.

The number of memory capacity can be changed only when the relevant LPAR is inactive.

Tip

Memory area, isolated due to memory failure detected, cannot be assigned to an LPAR.

Note

With high-performance server blades with LPAR manager firmware version 78-3X, up to 1044480 MB memory can be assigned to LPARs.

(12) How to change the number of memory node to assign to an LPAR
LPAR manager firmware version 59-2X/79-2X or later

Place the cursor on the **MN** column of an LPAR line and press **Enter** to open a subscreen. Set A or a node number and press **Enter**.

Note

Assuming an LPAR with memory node assigned and that with memory node not assigned are included in an environment, the LPAR with memory node assigned might fail to be activated when activation is executed from the LPAR with memory node not assigned. Thus, make sure to assign memory node to all LPARs when assigning memory node to even one LPAR. If creating a mixed configuration, make sure to activate the LPAR with memory node assigned first, and to activate the LPAR with memory node not assigned last.

(13) How to find the node number of processor and memory assigned to an LPAR
LPAR manager firmware version 59-2X/79-2X or later

You can find the processor and memory assigned to an LPAR that belongs to the same node by checking **PN: Processor Node**, and **MN: Memory Node** on the screen. When the same number: node number is displayed as the value of PN and MN, the physical processor and physical memory assigned to the LPAR belong to the same node.

When M: Multiple node is displayed as a value of PN or MN, check the node number using the following steps.

- When a dedicated processor is assigned:

  1. Find a physical processor number assigned to the LPAR on Logical Partition Configuration screen, and write it down.

  2. Check the physical processor number, Node #, written down in step 1 on the Physical Processor Configuration screen.

- When a shared processor is assigned

  Check the physical processor number, Node #, which belongs to the LPAR processor group on the Physical Processor Configuration screen.

For memory node number, press the **F2** key on the **Logical Partition Configuration screen** to show Memory Allocation Display. You can find the assigned memory node number, Node # on the Display.

If one of the following three is displayed, you might not make the full use of memory performance.

- PN and MN have different numbers: the physical processor and physical memory assigned to the LPAR belong to different nodes.
- When a dedicated processor is assigned, M: Multiple nodes are shown in PN or MN.
- When a shared processor is assigned, a memory that does not belong to a node not included in the processor group.

(14) How to enable/disable the function that detects the idle status of an LPAR's logical processors (Idle Detection function)

Open the **Logical Partition Configuration** screen. Move the cursor over the ID column of the LPAR whose Idle Detection settings you want to change, and press **Enter**. This will open a subscreen. Use the arrow keys ([↑] or [↓]) to select Yes or No, and press **Enter**.

(15) How to activate an LPAR automatically

Open the **Logical Partition Configuration** screen. Move the cursor over the **AA** column of the LPAR which you want to set Auto Activate, and press **Enter**. This will open a subscreen. Enter a value between 1 and 99, and press **Enter**. If you do not want to enable the Auto Activation, enter **"*"**.

You can set Auto Activate on a deactivated LPAR.

When you start LPAR manager, it will automatically activate the LPARs in the order of the values set in the above subscreen, starting with the smallest numbers. If the same value has been set for two LPARs, LPAR manager will activate the LPAR with the lower LPAR number first.

If, for whatever reason (inability to secure assigned memory size, and so on), the Auto Activation of one of the LPARs fails, it will not execute on the other LPARs that have not yet been automatically activated.

Before starting the Auto Activate processing, LPAR manager accepts the cancellation requests for 15 seconds. If you want to cancel the Auto Activate processing, press and hold **Ctrl + c** at the time

It might not be possible to cancel the automatic activation of LPARs once it has already started.

If Pre-State Auto Activation is set, the Auto Activation Order might be ignored. See Options or more on Pre-State Auto Activation.

(16) How to enable the automatic clear function of an LPAR's logical SEL

Open the **Logical Partition Configuration** screen. Move the cursor over the **AC** column of the LPAR whose Auto Clear settings you want to change, and press **Enter**. This will open a subscreen. Use the arrow keys ([↑] or [↓]) to select **Yes**, and press **Enter**. The automatic logic SEL clear function can be changed only when the relevant LPAR is inactive.

(17) How to add an LPAR

Press **F6** in the **Logical Partition Configuration** screen. In the subscreen that opens, move your cursor over the LPAR that you want to add and press **Enter**.

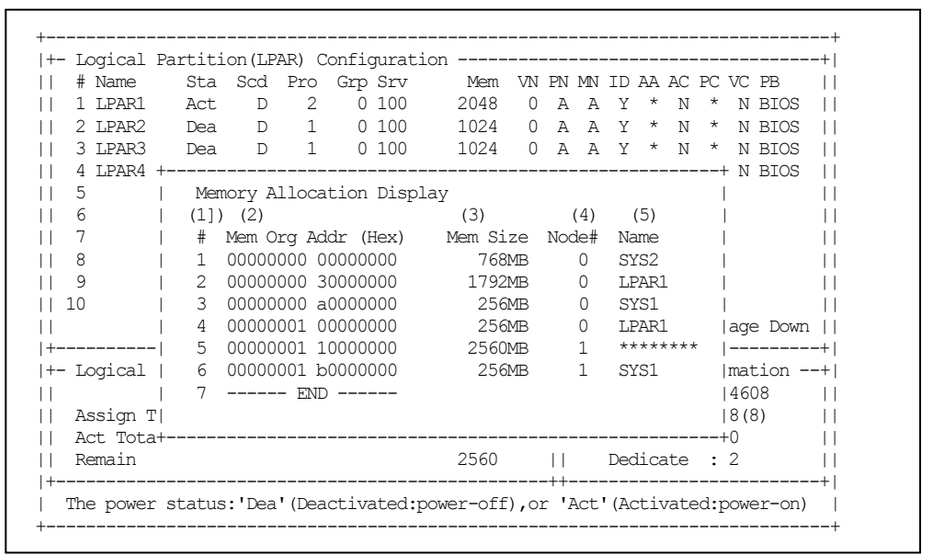
(18) How to delete an LPAR

Press **F7** in the **Logical Partition Configuration** screen. Move your cursor on the displayed subscreen over the LPAR that you want to remove and press **Enter**.

The LPAR can be deleted only when it is inactive. When you remove an LPAR, all the resources that had been assigned to the LPAR become unassigned.

(19) How to display memory allocation

Press **F2** in the **Logical Partition Configuration** screen to open the subscreen shown below. This subscreen displays the memory allocation status in the address ascending order.



The following table shows the descriptions of the items displayed in the Memory Allocation Display subscreen.

#	Title	Description
(1)	#	Serial numbers of memory blocks to be displayed
(2)	Mem Org Addr (Hex)	Displays the start address of the allocated memory in hexadecimals. The addresses are listed in ascending order. When the Memory Allocation Display has no more content, "-------- END ------- " will be displayed. This screen displays up to 15 memory blocks (the first row on the first page is taken up by descriptions). If there are more than 15 memory blocks, you will have to scroll using the Page Up, Page Down keys to view the display content. For more details, see the table below showing key operations.
(3)	Mem Size	This displays the memory size in decimal numbers in units of MB.
(4)	Node#	Displays the memory node number. When NUMA is disabled, “-“ is displayed.
(5)	Name	Displays what is using the memory area indicated by Mem Size from the address of Mem Org Addr. The meaning of the system names is shown below. SYS1: Indicates that the LPAR manager kernel is using the memory area. SYS2: Indicates that the LPAR manager's communications and service control components are using the memory area. LPARx: Indicates that the LPAR having number x is using the processor. (The LPAR name is not displayed.) ISOLATED: Indicates that the area is isolated from the system target due to memory error detection. Only the active LPARs are displayed. ********: Indicates an unallocated area

Note 1: The memory area D000 0000 to FFFF FFFF for the IPF version LPAR manager and the memory area D000 0000 to FFFF FFFF are used for hardware. So, they are not displayed on this screen

Note 2: A single guest memory area can be allocated up to four separated memory blocks. When this happens, the display is also split up into four blocks.

Note 3: For SYS1, NUMA features are not enabled.

The key operations in the Memory Allocation Display subscreen are shown in the table below.

#	Key	Operation/Role
1	Esc	Closes the subscreen that displays the memory allocation status. To refresh the contents of the Memory Allocation Display subscreen, close the screen with the Esc key and then re-open it by pressing the F2 (Mem) key. When you press the F2 key after temporarily closing the screen with the Esc key, the state of the display that existed before (by using the Page Up, Page Down keys) is not inherited.
2	PageDown	Displays the contents of the memory block after the currently displayed ones. If there is no next memory block to be displayed, this key operation is ignored.
3	PageUp	Displays the content of the memory block before the currently displayed ones. If there is no previous memory block to be displayed, this key operation is ignored.
4	Other keys	Not used. (Ignored)

(20) How to enable the processor capping function

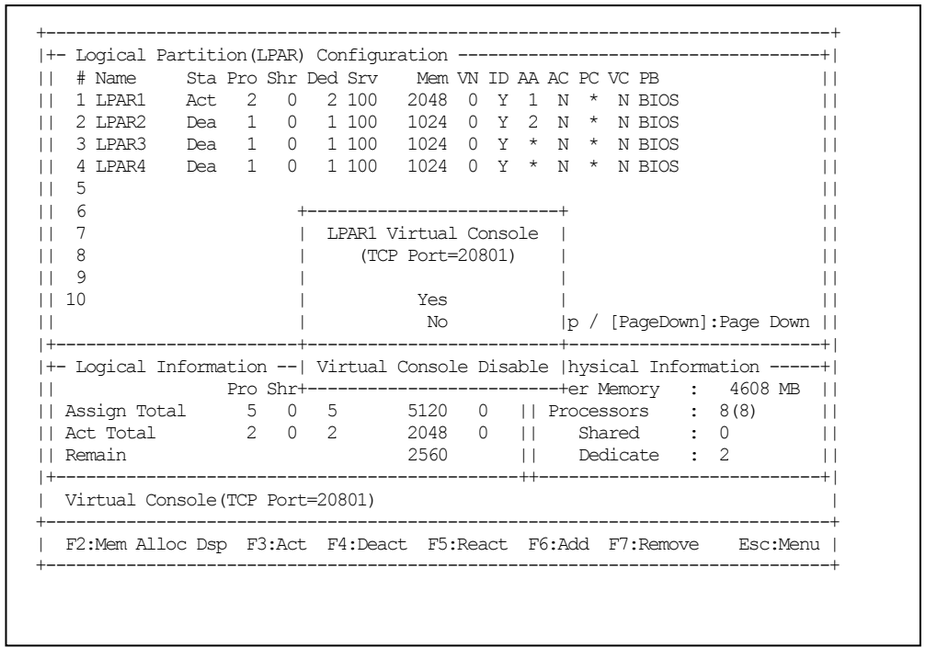
Open the **Logical Partition Configuration** screen. Move the cursor over the **PC** column of the LPAR whose Processor Capping you want to enable, and press **Enter**. This will open a subscreen. Use the arrow keys ([↑] or [↓]) to select **Yes**, and press **Enter**.

(21) How to enable the virtual COM console function

Display the **Logical Partition Configuration** screen.

Place the cursor on the **VC** column of the LPAR line whose virtual COM console function you want to enable, and then press **Enter** to display the subscreen. Select **Yes** by moving the cursor with the [↓] [↑] keys, and then press **Enter**. As a result, you can connect the LPAR guest screen via telnet. The TCP port to be used at the connection via telnet can be found in the comment that appears when pointing to the VC column of LPAR line or in the subscreen that appears when pointing to the VC column of LPAR line and pressing **Enter**.

When the virtual COM console function is enabled and connected to the LPAR guest console via telnet, LPAR guest screen connection by using the **F8** key in the LPAR manager screen is still available. In this case, the LPAR guest screen displayed on the LPAR manager screen is preceded.



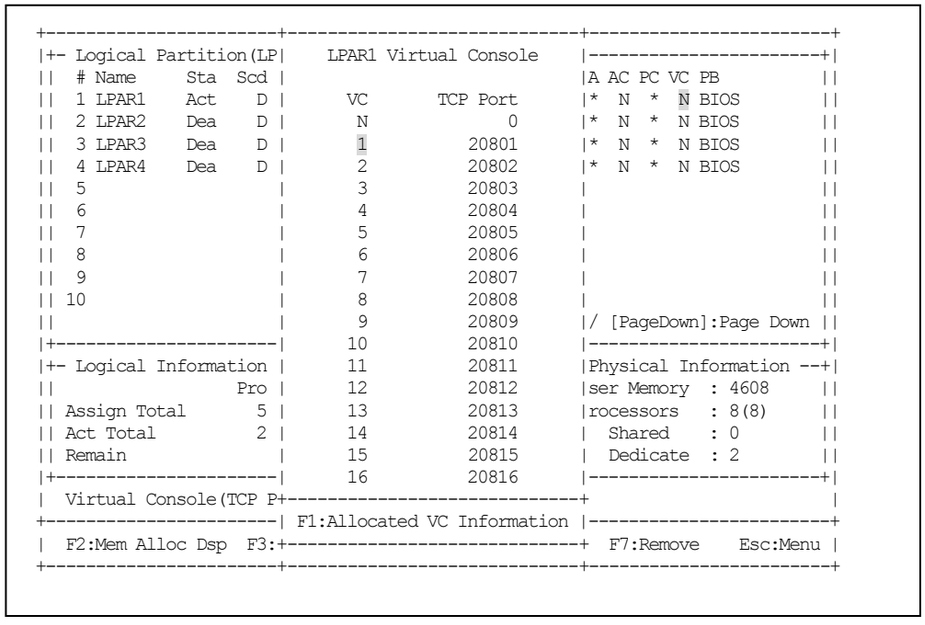
LPAR manager firmware 58-4X/78-4X or later versions

Display the **Logical Partition Configuration** screen.

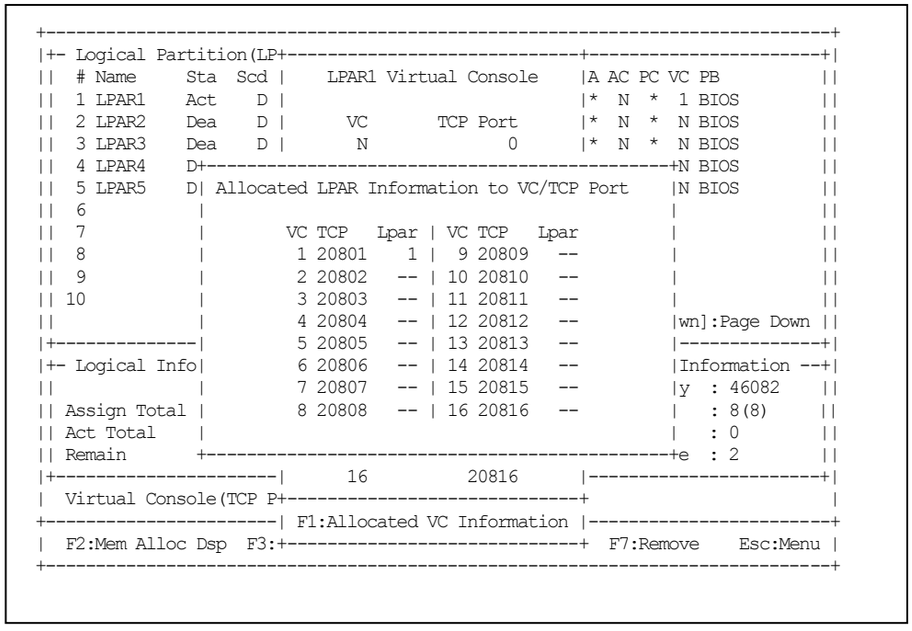
Place the cursor on the **VC** column of the LPAR line whose virtual COM console function you want to enable, and then press the **F1** key to display a subscreen. Select a VC number to connect by moving the cursor with the [↓] [↑] keys, and then press **Enter**. As a result, you can connect the LPAR guest screen via telnet. The TCP port to be used at the connection via telnet can be found in the comment that appears when pointing to the VC column of LPAR line.

When the virtual COM console function is enabled and connected to the LPAR guest console via telnet, LPAR guest screen connection by using the **F8** key in the LPAR manager screen is still available. In this case, the LPAR guest screen displayed on the

LPAR manager screen is preceded.



When you press the **F1** key on this subscreen, assignments of VC numbers and TCP ports are displayed.



(22) How to change OS types

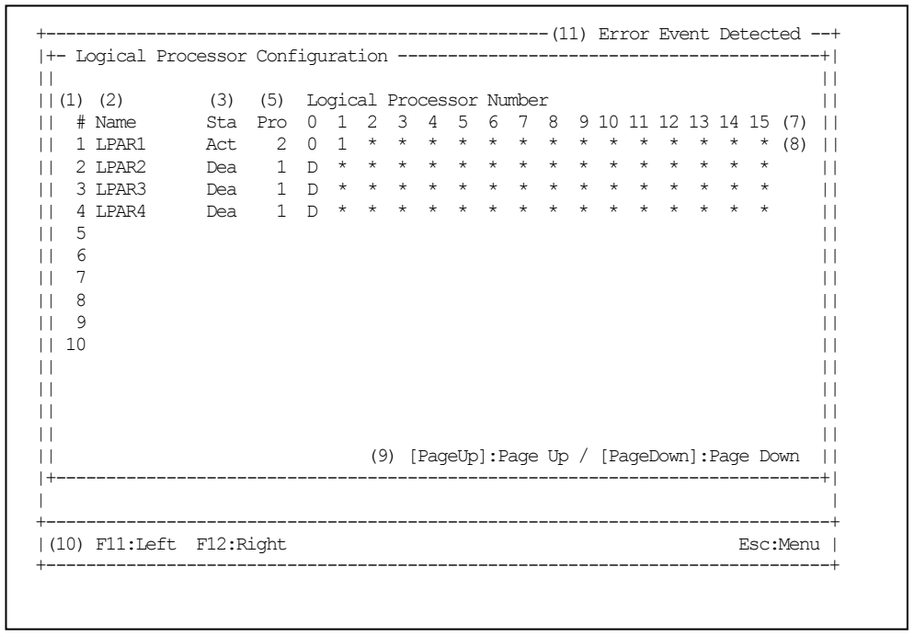
Display the **Logical Partition Configuration** screen. Scroll the screen to the right or left using the **F11** key or **F12** key. Place the cursor at the intersection of a row of the target LPAR and the **OS Type** column, and press **Enter** to display a subscreen. Move the cursor with arrow keys: [↑] or [↓] to select **Default** or **Solaris**, and press **Enter**. OS Type can be changed only when the LPAR is deactivated.

❑ Logical processor configuration

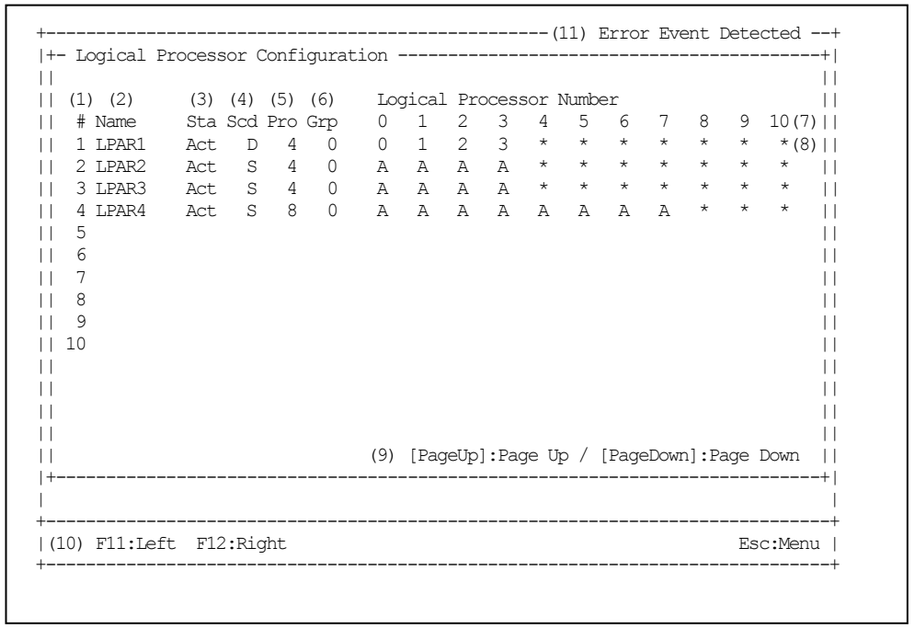
The following functions are available in the **Logical Processor Configuration** screen.

- Changing the physical processor assignment to each LPAR
- Display the names of the LPARs, their operating status, and their number of logical processors.

For: Standard server blades with LPAR manager firmware 58-2X or earlier versions;
High-performance server blades with LPAR manager firmware 78-2X or earlier versions



For: Standard server blades with LPAR manager firmware 58-3X or later versions; High-performance server blades with LPAR manager firmware 78-3X or later versions



The following table shows the descriptions of all the items displayed in the Logical Processor configurations screen.

#	Title	Full name	Description	Initial value (LPAR added)
(1)	#	LPAR Number	Displays LPAR numbers 1-16.	-
(2)	Name	LPAR Name	Displays LPAR names	NO_NAME
(3)	Sta	Status	Displays LPAR status. Act (Activated): the power is on. Dea (Deactivated): the power is off. Fai (Failure): Not available due to unrecoverable failure. Reboot LPAR manager when this happens.	Dea
(4)	Scd	Scheduling Mode	Sets a scheduling mode. S: Shared mode D: Dedicated mode	D
(5)	Pro	Logical Processors	Displays the number of logical processors assigned to the LPAR.	1
(6)	Grp	Processor Group	Displays a processor group number.	0
(7)	Logical Processor Number	Logical Processor Number	Displays the logical processor number.	-
(8)	Logical Processor Assignment	Logical Processor Assignment	Standard server blades with LPAR manager firmware 58-2X or earlier versions/High-performance server blades with LPAR manager firmware 78-2X or earlier versions Assigns a logical processor to each LPAR. *: No yet assigned. S: Assigned in the shared mode. D: Assigned in the dedicated mode. (only when the LPAR id deactivated) Number: displays the physical processor shown by the number is assigned. (only when the physical processor number is assigned if the dedicated LPAR is activated or deactivated.)	-
			Standard server blades with LPAR manager firmware 58-3X or later versions/High-performance server blades with LPAR manager firmware 78-3X or later versions Assigns a logical processor to each LPAR. *: Not assigned right now. A: Automatically selects a physical processor to assign to an LPAR when the LPAR is activated in shared or dedicated mode. Numeric: A physical processor shown as a number is assigned to an LPAR when the LPAR is active in dedicated mode. If the display is other than that, a physical processor will be assigned to an LPAR the next time the LPAR is activated in shared mode.	
(9)	Page Up / Page Down keys	Page Up / Page Down	Page Up: Scrolls a page of the screen upwards. Page Down: Scrolls a page of the screen downwards.	-
(10)	Function Key	Function Key	Displays function keys available on this screen. F11 key: Scrolls the screen to the left. F12 key: Scrolls the screen to the right.	-

#	Title	Full name	Description	Initial value (LPAR added)
(11)	Error event detected	Error event detection	Displays that LP system logs of the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the ESC key with this screen or open the system logs screen.	

#	Title	Guest status			Remarks
		Activate	Deactivate	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	-	-	Display only
(3)	Sta	-	-	-	Display only
(4)	Scd	-	-	-	Display only
(5)	Pro	-	-	-	Display only
(6)	Grp	-	-	-	Display only
(7)	Logical Processor Number	-	-	-	Display only -
(8)	Logical Processor Number	Standard server blades with LPAR manager firmware 58-2X or earlier versions/ High-performance server blades with LPAR manager firmware 78-2X or earlier versions			
		-	Δ	-	Changeable in the dedicated mode
		Standard server blades with LPAR manager firmware 58-3X or later versions/ High-performance server blades with LPAR manager firmware 78-3X or later versions			
		Δ Changeable in shared mode	✓	-	

✓: can be changed -: cannot be changed Δ: can be changed with conditions

(1) How to a physical processor to a logical processor in the dedicated mode

Any physical processor can be assigned to the logical processor in the shared mode.

Open the **Logical Processor Configuration** screen.

Place the cursor on the intersection between the LPAR column and the logical processor number row, and press **Enter** to display the subscreen. Enter the physical processor number, and press **Enter**.

Standard server blades with LPAR manager firmware 58-2X or earlier versions/ High-performance server blades with LPAR manager firmware 78-2X or earlier versions

Deactivate the LPAR and set it in the dedicated mode before executing this setting.

Standard server blades with LPAR manager firmware 58-3X or later versions/ High-performance server blades with LPAR manager firmware 78-3X or later versions

Deactivate the LPAR, or activate it in the shared mode, before executing this setting.

If not setting the physical processor number using this function, LPAR manager will assign a physical processor when the LPAR is activated.



When you have changed configurations by adding or removing physical processors, such as enabling/disabling SMT or cancelling an SMP configuration, you need to reset the configuration information for use.

The following table provides detailed information for resetting.

Standard server blade

<table>
<tr><th colspan="2">LPAR manager firmware</th><th>Physical processor</th><th>Description</th></tr>
<tr><td colspan="2">(1) Version currently used
57-0X to 58-22</td><td>Added or reduced</td><td>Because the setting is taken over as it is, the incorrect setting information remains set.
On the Logical Partition Configuration screen, reset the number of LPAR logical processors using the function. Then If the physical processor number needs to be set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, an error occurs when you create LPAR configuration or update it from SC/BSM.</td></tr>
<tr><td colspan="2">58-40 or later</td><td>Added or reduced</td><td>The setting is initialized.
If the physical processor number needs to be set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, LPAR manager will automatically assign a physical processor.</td></tr>
<tr><td colspan="2">(2) Update to a specific version</td><td rowspan="3">Added or reduced</td><td rowspan="3">The setting is initialized, but the information remains internally.
On the Logical Partition Configuration screen, reset the number of LPAR logical processors using the function. Then If the physical processor number needs to set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, an error occurs when you create the LPAR configuration or update it from SC/BSM.</td></tr>
<tr><td>Before update</td><td>After update</td></tr>
<tr><td>57-0X to 58-22</td><td>58-40 to 78-7X</td></tr>
</table>

High-performance server blade

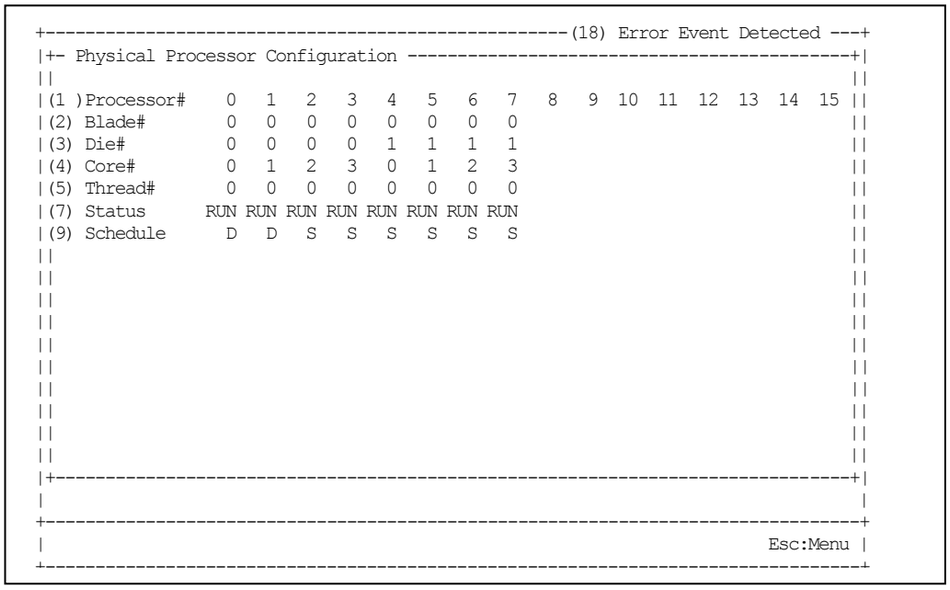
<table>
<tr><th colspan="2">LPAR manager firmware</th><th>Reduction in physical processors</th><th>Description</th></tr>
<tr><td colspan="2">Version currently used (1)</td><td rowspan="2">Added or reduced</td><td rowspan="2">Since the setting is taken over as it is, the incorrect setting information remains set.
On the Logical Partition Configuration screen, reset the number of LPAR logical processors using the function. Then if the physical processor number needs to be set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, an error occurs when you create LPAR configuration or update it from SC/BSM.</td></tr>
<tr><td colspan="2">78-12 to 78-22</td></tr>
<tr><td colspan="2">78-40 or later</td><td>Added or reduced</td><td>The setting is initialized.
If the physical processor number needs to be set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, LPAR manager will automatically assign a physical processor.</td></tr>
<tr><td colspan="2">Update to a specific version (2)</td><td rowspan="3">Not added/ reduced</td><td rowspan="3">The setting is initialized, but the information remains internally.
On the Logical Partition Configuration screen, reset the number of LPAR logical processors using the function. Then if the physical processor number needs to set to the logical processor, reset it on the Logical Processor Configuration screen and save the LPAR manager configuration. Without resetting, an error occurs when you create LPAR configuration or update it from SC/BSM.</td></tr>
<tr><td>Before update</td><td>After update</td></tr>
<tr><td>78-12 to 78-22</td><td>78-40 to 78-7X</td></tr>
</table>

❑ Physical processor configuration

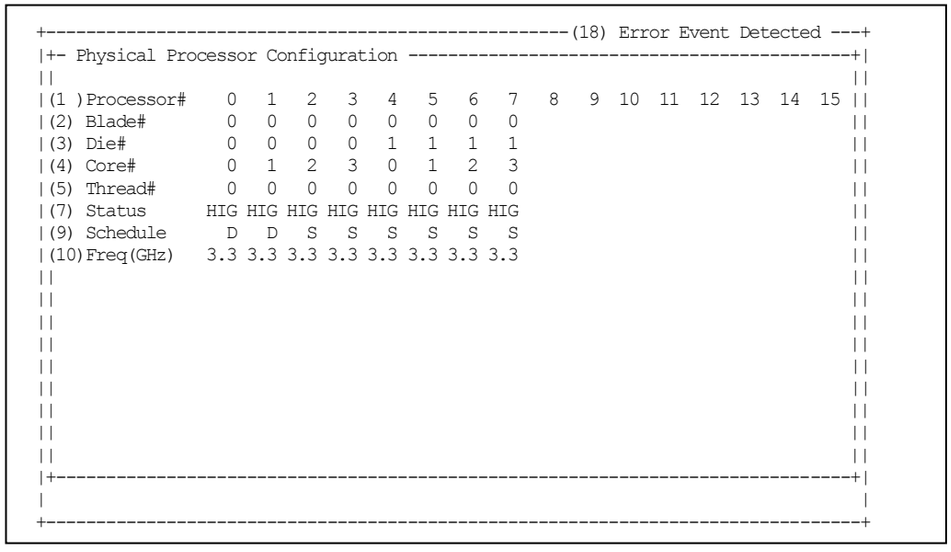
The following functions are possible in the Physical Processor Configuration screen.

- Display the physical processor status
- Display the physical processor configuration
- Add, delete, and change processor groups

LPAR manager firmware version 57-0X



Standard server blades with LPAR manager firmware 58-2X or earlier versions/ High-performance server blades with LPAR manager firmware 78-2X or earlier versions



Standard server blades with LPAR manager firmware 58-3X or later versions/ High-performance server blades with LPAR manager firmware 78-3X or later versions

```
+-------------------------------------------------(18) Error Event Detected --+
|+- Physical Processor Configuration ----------------------------------------+|
|(1) Processor#    0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15||
|(2) Blade#        0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0||
|(3) Socket#       0   0   0   0   0   0   0   0   1   1   1   1   1   1   1   1||
|(4) Core#         0   0   1   1   2   2   3   3   0   0   1   1   2   2   3   3||
|(5) Thread#       0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1||
|(6) State       ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT ACT||
|(7) Status      HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG HIG||
|(8) Group#        0   0   0   0   0   0   0   0   1   1   1   1   1   1   1   1||
|(9) Schedule      D   D   D   D   S   S   S   S   S   S   S   S   S   S   S   S||
|(10)Freq(GHz)   1.7 1.7 1.7 1.8 1.7 1.6 1.7 1.7 1.7 1.7 1.7 1.8 1.7 1.6 1.7 1.7||
|(11)Node#         0   0   0   0   0   0   0   0   1   1   1   1   1   1   1   1||
||                                                                              ||
|+------------------------------------------------------------------------------+|
|+- Processor Group Configuration -------------------------------------------+|
|(12)Group#            0       1                                             ||
|(13)Name          NO_NAME NO_NAME                                           ||
|(14)Total Core        4       4                                             ||
|(15)Shr Core          2       4                                             ||
|(16)Ded Core          2       0                                             ||
||                                                                            ||
|+------------------------------------------------------------------------------+|
+--------------------------------------------------------------------------------+
|(17)F1:Add  F2:Remove  F11:Left  F12:Right                          Esc:Menu |
+--------------------------------------------------------------------------------+
```

The following table describes each item on this screen.

#	Title	Description
(1)	Processor#	Displays the physical processor numbers.
(2)	Blade#	Displays the server blade number on which the physical processor is installed.
(3)	Die# Socket#	Displays the die number in the server blade.
(4)	Core#	Displays the core number in the die.
(5)	Thread#	Displays the thread number.
(6)	State	Display status of a core. Act (Activate): Normal state Wrn (Warning): Beyond the threshold of the number of unrecoverable failures Deg (Degenerate): Degenerated due to preventively replaced or preventively degenerated High-performance server blades with LPAR manager firmware 78-3X or later versions: Cores are deactivated and degenerated.

#	Title	Description
(7)	Status	Displays the status of the physical processor. LPAR manager firmware version 57-0X RUN: The physical processor is running normally. FAI: The physical processor is in failure state. ERR: The physical processor is in error state. OFF: The physical processor is in off-line. LPAR manager firmware 57-10 or later versions HIG: The physical processor can work at the highest rate. But it might not work at the highest rate if the processor turbo mode or power capping is enabled, or if the processor is at idle. MXX: The physical processor is running at a moderate rate. * M01 is the fastest; as the number of a processor increases, its rate decreases. LOW: The physical processor can work at the lowest rate. FAI: The physical processor is in failure state. ERR: The physical processor is in error state. OFF: The physical processor is in off-line.
(8)	Group#	Sets the number of a processor group.
(9)	Schedule	Displays the scheduling mode of a physical processor. D: Dedicated mode S: Shared mode
(10)	Freq (GHz)	Displays the current frequency of the physical processor. The processor might not work at the highest rate, if the processor turbo mode or power capping is enabled, or if the processor is at idle..
(11)	Node#	Displays the physical processor node number. When NUMA is disabled, “-“ is displayed.
(12)	Group#	Displays the number of a processor group.
(13)	Name	Sets a processor group name.
(14)	Total Core	Displays the total number of cores.
(15)	Shr Core	Displays the total number of cores in shared mode.
(16)	Ded Core	Displays the total number of cores in dedicated mode.
(17)	Function Key	Displays function keys available in this screen. F1: Adds a processor group. F2: Deletes a processor group. F11: Scrolls the screen to the left. F12: Scrolls the screen to the right.
(18)	Error event detected	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.

(1) How to change the number of a processor group

Display the **Physical Processor Configuration** screen. Place the cursor on the intersection between the **Processor** column whose number to change and Group line, and press **Enter** to display a subscreen that displays the numbers of defined processor groups. Select a processor group number to change, and press **Enter**.

Changing the number of a processor group can be performed to cores in Activate or Warning at any time. If one of the following conditions is met, an error message will appear to terminate the screen.

(a) An LPAR in dedicated mode is activated on the target core.

(b) When an LPAR in shared mode is activated in the target core: a shared mode LPAR is activated on the group whose number is to be changed; change in the group number of the target core removes the physical processor in shared mode in the source group.

(2) How to change a processor group name

Display the **Physical Processor Configuration** screen. Place the cursor on the **Name** line which you need to change, and press **Enter** to display a subscreen. Type a processor group name to change, and press **Enter**. You cannot configure the same name to different processor groups.

A processor group name can include up to 31 characters: [0] to [9], [a] to [z], [A] to [Z], [-], and [_]. The first character available, however, is [a] to [z] and [A] to [Z]. If a group name contains more than seven characters, the 7th character is shown as a tilde “~” and the following characters are omitted

(3) How to add a processor group

Press **F1**: **Add** on this screen to display a subscreen, place the cursor on a processor group number to add on the subscreen, and press **Enter**.

(4) How to delete a processor group

Press **F2**: **Remove** on this screen to display a subscreen, place the cursor a processor group number to remove on the subscreen, and press **Enter**.

Processor group 0, the default processor group, cannot be deleted.

(5) How to deactivate a processor core

High-performance server blades with LPAR manager firmware version 78-3X or later

Display the **Physical Processor Configuration** screen. Place the cursor on the **State** line of a processor column which you need to deactivate, and press **Enter** to display a subscreen to confirm for the deactivation. Select **Yes** and press **Enter**.

You can deactivate only a core activated when the number of core licenses has been found short. If one of the following conditions is met, an error message will appear to close the screen.

(a) An LPAR in dedicated mode is activated on the target core.

(b) When an LPAR in shared mode is activated in the target core: a shared mode LPAR is activated on the group that is assigned to the core, deactivating the target core removes the physical processor in shared mode in the group.

(6) How to degenerate a processor core

High-performance server blades with LPAR manager firmware 78-3X or later versions

Display the **Physical Processor Configuration** screen. Place the cursor on the **State** line of a processor line which you need to degenerate, and press **Enter** to display a subscreen to confirm for the degeneration. Select **Yes** and press **Enter**.

You can degenerate only a core in Warning. If one of the following conditions is met, an error message will appear to terminate the screen.

(a) An LPAR in dedicated mode is activated on the target core.

(b) When an LPAR in shared mode is activated in the target core: a shared mode LPAR is activated on the group that is assigned to the core, degenerating the target core removes the physical processor in shared mode in the group.

(c) The target core is the last one in the system.



If unrecoverable failure occurs in the physical processor, the following symptom might occur.

- NIC function is temporarily unavailable and communication with the management module and external networks break down.

  LPARs also have the following symptoms depending on the scheduling mode of the physical processor.

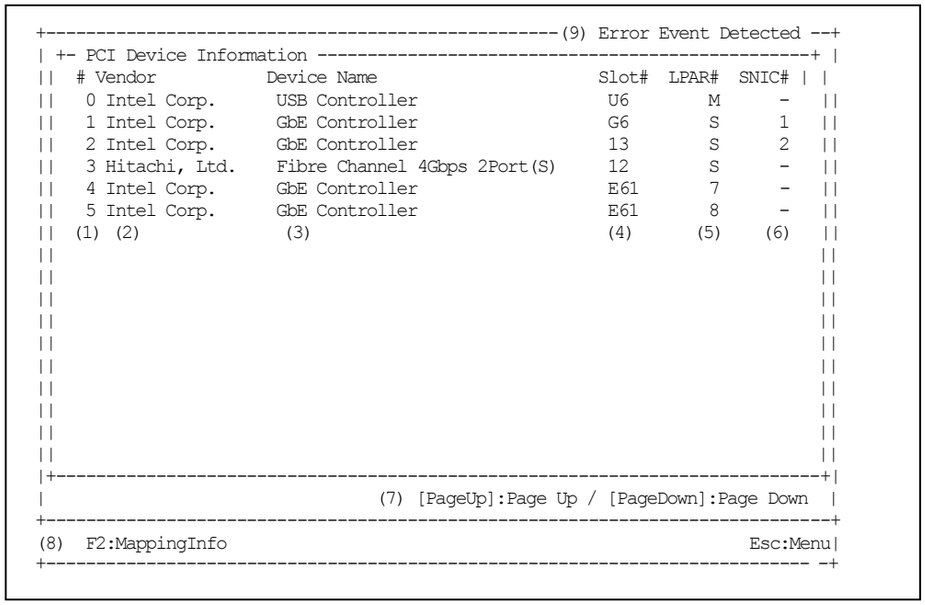
- Dedicated mode: A failure occurs in the LPAR using the failed physical processor in the dedicated mode. Other LPARs are not affected.
- Shared mode: LPARs using the processor in the shared mode will have failure when a fault occurs in the processor.
  Other LPARs performance in the shared mode might slow down. When this happens, deactivate the slow-down LPAR and then reactivate it to restore it.

❑ PCI device information

The following functions are available in the PCI Device Information screen.

- Displays the vendor name, device name, slot number, LPAR number, and shared NIC number corresponding to each PCI device number.

  PCI device refers to a PCI card that has been inserted into a PCI slot or a PCI device that has been integrated in the server blade.



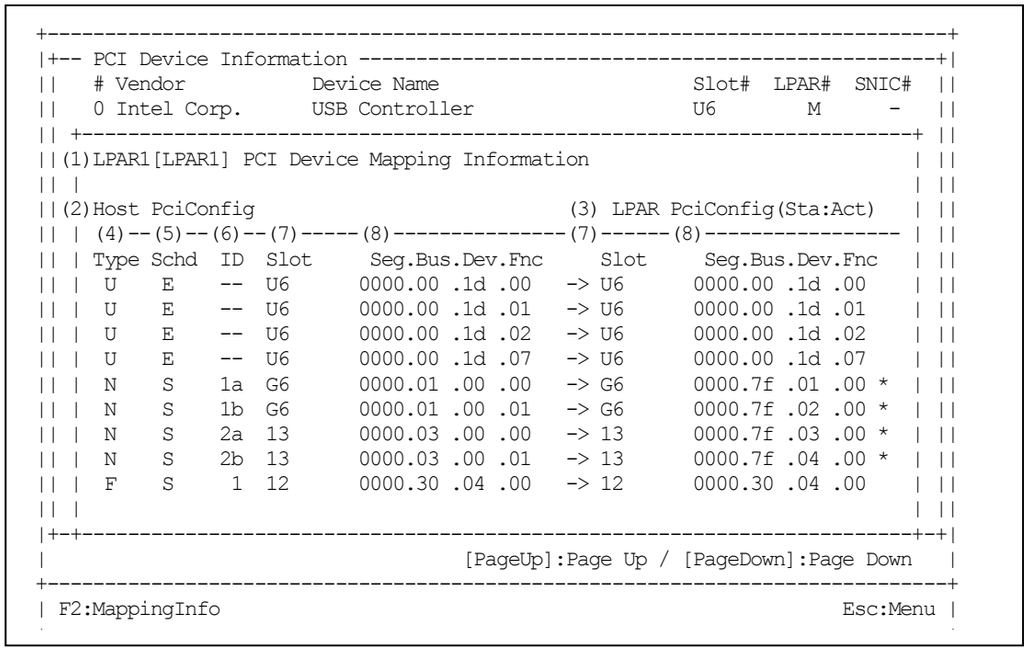
The following table describes each item on this screen.

#	Title	Official Name	Description
(1)	#	PCI Device Number	Displays the number that LPAR manager gives each PCI device for identification purposes.
(2)	Vendor	Vendor Name	Displays the name of the vendor of the PCI device. (displays up to 15 characters)
(3)	Device Name	Device Name	Displays the name of the PCI device. (displays up to 31 characters)
(4)	Slot#	Slot Number	Displays the slot number to which the PCI device is inserted. **Device type** / **Slot #** Onboard USB (Front USB, Remote console) / Ux Onboard SAS / Sx Onboard NIC (Kawela) / Gx PCI card slot 0-15 / 0-15 Mezzanine card slot0 / Ex0 Mezzanine card slot1 / Ex1 I/O board slot 0-15 / Iy0-Iy15 x: Server blade number; y: I/O slot expansion unit number
(5)	LPAR#	LPAR Number	Displays the LPAR number to which the PCI device is assigned. Number: When the PCI device has been assigned to a single LPAR, the LPAR number that the PCI Device has been assigned to. M: The PCI device has been assigned to multiple LPARs. S: The PCI device is being shared. - : The PCI device is not assigned.
(6)	SNIC#	Shared NIC Number	Displays the shared NIC number of a PCI device if it is a shared NIC. Number: Indicates that the PCI device is a shared NIC number - : Indicates that the PCI device is not a shared NIC.
(7)	PageUp / PageDown Keys	Page Up / Page Down	Page Up: scrolls a page upwards. Page Down: scrolls a page downwards.
(8)	Function Key	Function Key	LPAR manager firmware version 58-7X/78-7X or later Displays the function key available on this screen. F2: Use this key to display the PCI device mapping information.
(9)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.

(1) Viewing PCI Device Mapping Information

LPAR manager firmware version 58-7X/78-7X or larger

With the following screen, press **F2**: **MappingInfo** to display a subscreen. On the subscreen place the cursor on an LPAR number to display, and press **Enter**.



The following table describes the items for memory allocation in the above screen.

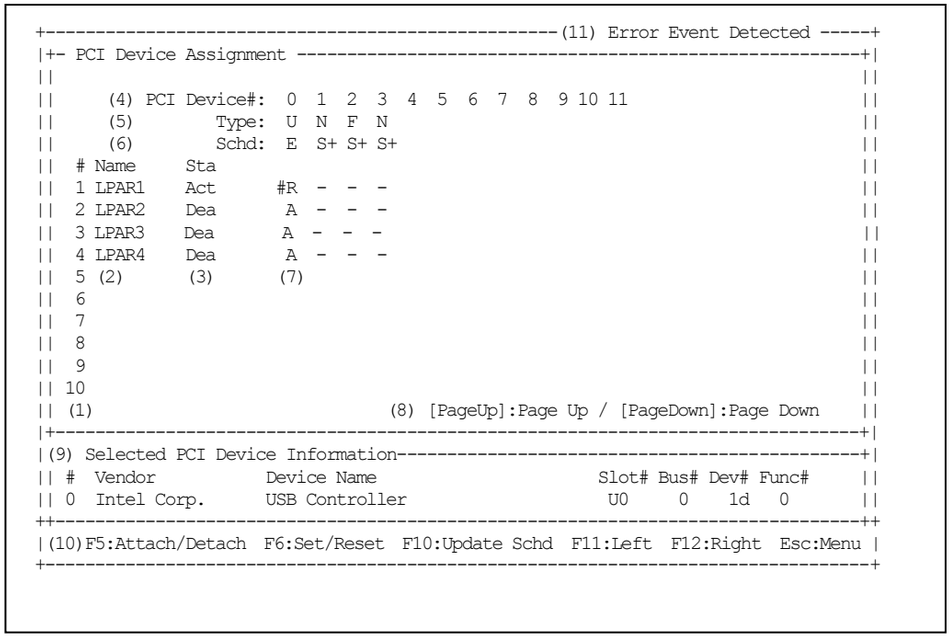
No.	Title	Description
(1)	LPARxxx [yyy]	Displays an LPAR number and name. xxx: LPAR number yyy: LPAR name
(2)	Host PciConfig	Displays information on physical PCI devices assigned to the activated LPAR.
(3)	LPAR PciConfig	Displays the PCI configuration address of the physical PCI device assigned to a LPAR viewed on the LPAR.
(4)	Type	Displays the type of a physical PCI device. S: SCSI controller, RAID controller N: Network Interface Card (NIC) When SR-IOV is enabled, “v” is added to the end. F: Fibre-channel U: USB controller
(5)	Schd	Displays the scheduling mode of a physical PCI device. D: Dedicated mode S: Shared mode E: Exclusive-shared mode -: Virtual NIC

No.	Title	Description
(6)	ID	Displays the ID used by the LPAR when the physical PCI device is in shared mode. Numeric: vfcID 1a-8h: Network segment identifier for a shared NIC When SR-IOV is enabled, “v” is added to the end. Va-Vd: network segment identifier for a virtual NIC
(7)	Slot	Host PciConfig Displays a physical location of a physical PCI device. With a virtual NIC, the location is shown as “-“. “err” following the slot display indicates that the physical PCI device is blocked. LPAR PciConfig Displays a location of a logical PCI device. With a virtual NIC, the location is shown as “-“.
(8)	Seg.Bus.Dev.Fnc	Host PciConfig Displays PCI configuration addresses of a physical PCI device and virtual NIC. LPAR PciConfig Displays the PCI configuration address of a logical PCI device viewed on the LPAR. “*” at the end of a PCI configuration address indicates the difference between the physical PCI information and logical PCI information.

❑ PCI device assignment

The following functions are available in the PCI Device Assignment screen.

- Display the PCI device type
- Specify the PCI device's scheduling mode (IPF version LPAR manager only)
- Allocate the PCI devices to LPARs
- Display the information of PCI devices selected by the cursor
- Switch USB devices assignment



The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(1)	#	LPAR Number	Displays LPAR numbers.	-
(2)	Name	LPAR Name	Displays the LPAR name.	NO_NAME
(3)	Sta	Status	Displays the LPAR status. Act (Activate): The LPAR is powered on. Dea (Deactivate): The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot LPAR manager when this happens.	Dea
(4)	PCI Device#	PCI Device Number	Displays the number that LPAR manager gives each PCI device for identification purposes.	-
(5)	Type	Device Type	Displays the PCI device type. S: SCSI controller N: Network interface Card (NIC) When SR-IOV is enabled, “v” is added to the end. F: Fibre-channel U: USB controller	-
(6)	Schd	Scheduling Mode	Sets the PCI device's scheduling mode. D: Assigns to a LPAR in the dedicated mode. (IPF version LPAR manager only) E: Assigns to a LPAR in the exclusively shared mode. S: Assigns to a LPAR in the shared mode. A PCI device available for changing its scheduling mode has [+] on the right of Schd. A PCI device, Schd without [+], is not available for changing its mode.	-
(7)	Device Assignment	Device Assignment	Sets the assignment of the PCI device to LPARs. *: unassigned A: assigned but not activated R: activated and attached -: cannot be assigned LPAR manager firmware version 59-0X/79-0X or later A USB device with the automatic Attach setting has # next on the left to the assignment status, A or R.	- (Device type except USB) A (Device type: USB)
(8)	PageUp / PageDown keys	Page Up / Page Down	Page Up: scrolls a page upwards. Page Down: scrolls a page downwards.	-

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(9)	Selected PCI Device Information	PCI Device Information	Displays the information for the PCI device selected with the cursor. #: Displays the number that LPAR manager gives each PCI device for identification purposes. Vendor: Displays the vendor name (up to15 characters) Device Name: The device name (up to 31 characters) Slot#: Displays the slot number. Bus#: Displays the bus number of the PCI configuration space Dev#: Displays the device number of the PCI configuration space Func#: Displays the function number of the PCI configuration space.	-
(10)	Function Key	Function Key	Displays the function keys that can be used in this screen. F5: Switches USB device assignment. F10: Updates the content of any changes to the Scheduling Mode of a PCI device to LPAR manager. (IPF version LPAR manager only) F11: Scrolls the page to the left within the screen. F12: Scrolls the page to the right within the screen. LPAR manager firmware version 59-0X/79-0X or later F6: Changes the USB Auto Attach settings. Shown when USB Auto Allocation to LPAR is set to Disable on the LP Options screen.	-
(11)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	

The following table describes each item on this screen.

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	-	-	Display only
(3)	Sta	-	-	-	Display only
(4)	PCI Device#	-	-	-	Display only
(5)	Type	-	-	-	Display only
(6)	Schd	-	✓	-	
(7)	Device Assignment	Δ	✓	-	Cannot be changed when the LPAR has been activated.

✓: can be changed -: cannot be changed Δ can be changed with conditions

(1) How to change Scheduling Mode (Schd)

You can change the Scheduling Mode (Schd) of a NIC or FC that support shared allocation. In the Xeon-version LPAR manager firmware 56-XX or later versions, "+" is added to the scheduling mode (Schd) of the PCI device that can be configured.
Before modifying the Schd setting of a NIC or FC, you must deactivate all LPARs.

Open the **PCI Device Assignment** screen. Move the cursor to the intersection between the **Schd** row and the PCI device number column, and press **Enter**. This opens a subscreen where you can select assignments. Move the cursor over the item that you want to change, and press **Enter**.

To apply the changes of Schd to the LPAR manager system, press **F10** and select **Yes** in the confirmation subscreen that opens. After you select **Yes**, you will not be able to perform any operations on LPAR manager for one to three minutes until the setting changes completes.

To abort the change of **Schd**, press **F10** and select **No** in the confirmation screen that opens. All changed settings are restored to their original values.

It takes time to apply the change in Schd to the LPAR manager system. You cannot change settings except the Schd or move to another screen until the process is complete. To change except the Schd or move to another screen, press F10: Update PCI Dev Schd, select either "Yes" or "No" to complete the change process, or cancel the change.

(2) How to assign a PCI device to an LPAR

Open the **PCI Device Assignment** screen. Move the cursor over the intersection between the **LPAR**, to which you want to assign the PCI device, and the PCI device column, and press **Enter**. In the subscreen that appears, move the cursor over **A** and press Enter. To undo an assignment, select "*".

(3) How to change LPARs to connect a PCI device

Open the **PCI Device Assignment** screen. Press **F5 Attach/Detach** to display a subscreen. Select an LPAR to change on the subscreen and press **Enter**.

(4) How to change settings for USB Auto Allocation

LPAR manager firmware version 59-0X/79-0X or later

- Disable **USB Auto Allocation to LPAR** on the **LP Options screen before using this function.**
- When an LPAR with USB status #A is activated, the state will be changed to #R. If the USB is attached to another LPAR, it will not be automatically attached to the LPAR activated later.
- When USB status is changed to Not assigned, the USB Auto Allocation setting will be cancelled.

You can change USB Auto Allocation settings for activated and deactivated LPARs.

Point the cursor on **A** or **R** for status, and press **F6**: **Set/Reset** to toggle between Set and Reset. This setting is exclusive. Then, if the USB has been **Set** to another LPAR, the setting will be shifted.

When **Set** is selected, **A** or **R** will change to **#A** or **#R** respectively. USB Attach/Detach is not performed.

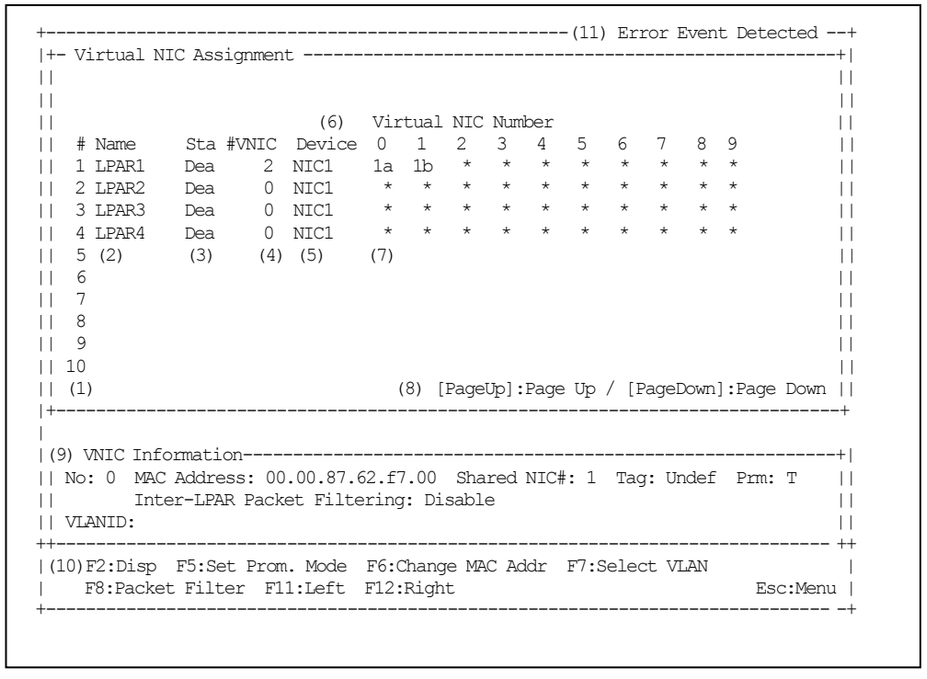
When **Reset** is selected, **#A** or **#R** will change to **A** or **R** respectively. USB Attach/Detach is not performed.

A USB is automatically attached only to an LPAR with the USB status #A when the LPAR is activated. If the USB status to the LPAR is not #A, the USB is not automatically attached. If no LPAR has the status #A, the USB is not automatically attached to any LPAR.

❑ Virtual NIC (VNIC) assignment

The following are executed on the VNIC Assignment screen.

- Assigns a VNIC to each LPAR.
- Sets a VNIC device type to each LPAR.
- Displays information on the VNIC selected by the cursor.
- Sets the promiscuous mode to the VNIC selected by the cursor.
- Changes the MAC address of the VNIC selected by the cursor.
- Sets VLAN to the VNIC selected by the cursor.
- Sets Inter-LPAR Packet Filtering to the VNIC selected by the cursor.
- Displays the list of the promiscuous mode and VLAN settings to the VNIC selected by the cursor.



The following table describes each item on the screen.

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(1)	#	LPAR Number	Displays LPAR numbers.	-
(2)	Name	LPAR Name	Displays the LPAR name.	NO_NAME
(3)	Sta	Status	Displays the LPAR status. Act (Activate): The LPAR is powered on. Dea (Deactivate): The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot LPAR manager when this happens.	Dea
(4)	#VNIC	Total number of VNIC	Displays the number of VNICs assigned to LPARs.	0

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(5)	Device	VNIC Device Type	LPAR manager firmware version 59-0X/79-0X or later Sets VNIC Device Type. NIC1: PRO/1000 NIC2: 82576 For X55R4 model, assign only NIC2 to LPARs. If NIC1 is assigned, it might not work.	X55R4 model: NIC2 Other than X55R4: NIC1
(6)	Virtual NIC Number	VNIC Number	Displays the VNIC number.	-
(7)	VNIC Assignment	Virtual NIC Assignment	Assigns VNIC to each LPAR. *: Not assigned Va - Vd: Sets the identifier for the network segment of the VNIC. 1a – 8h: Sets the identifier for the network segment of the shared NIC. When SR-IOV is enabled, “v” is added to the end. Content on the screen depends on the LPAR manager firmware version and onboard NIC.	-
(8)	PageUp / PageDown keys	Page Up / Page Down	Page Up: scrolls a page upwards. Page Down: scrolls a page downwards.	-

<table>
<tr><th>#</th><th>Title</th><th>Official Name</th><th>Description</th><th>Initial Value
(When LPAR is added)</th></tr>
<tr><td>(9)</td><td>VNIC Information</td><td>Virtual NIC Information</td><td>Displays the information on the virtual NIC selected by the cursor.
No: Displays the virtual NIC number.
MAC Address: Displays the MAC address of the virtual NIC.
Shared NIC#: Displays the shared NIC number.
Tag: Displays the VLAN mode of the virtual NIC.
Undef: VLAN mode not defined.
Tag: Defined to the UnTagged port.
Prm: Displays the promiscuous mode of the virtual NIC.
R: Receives the same MAC address as the virtual NIC.
T: Received all packets.
VLANID: Displays the defined VLAN ID.
<table><tr><th>VLAN mode</th><th>VLAN ID</th></tr><tr><td>Tagged</td><td>Up to 16 IDs from 1 to 4094, or All (IDs)
For VF NIC, only [All] (all IDs) can be specified.</td></tr><tr><td>Untagged</td><td>One ID from 1 to 4094.</td></tr></table>
For LPAR manager firmware 57-30 or later versions:
Inter-LPAR Packet filtering: Displays the inter-LPAR packet filter of the VNIC.
・ Disable: Inter-LPAR packets are transferred inside LPAR manager, but not transferred outside LPAR manager.
・ Enable: Inter LPAR packets are transferred outside LPAR manager, but not inside LPAR manager.
・ Disable (ALL): Inter-LPAR packets are transferred both inside and outside LPAR manager (LPAR manager 57-31 or later versions).
For LPAR manager firmware 59-7X/79-7X or later versions
TXRATE: Displays transmission bandwidth limitation for VF NIC.</td><td>Tag: Undef
(Shared NIC/Virtual NIC/VF NIC *1)

Tag: Tag
(VF NIC *2)

Prm:T
(Shared NIC/Virtual NIC)

Prm: R (VF NIC)

Inter-LPAR Packet Filtering: Disable

TXRATE: 10000 Mbps

Others: -

*1: When Emulex NIC firmware version is 4.6.x.x

*2: When Emulex NIC firmware version is 10.2.x.x-</td></tr>
</table>

#	Title	Official Name	Description	Initial Value (When LPAR is added)
(10)	Function Key	Function Key	Displays the function keys that can be used in this screen. F2: Displays the list of assigned VLAN ID. F5: Used to set the promiscuous mode. F6: Used to change MAC addresses. F7: Used to set the VLAN mode. **For LPAR manager firmware 57-30 or later versions:** F8 is used for setting Inter-LPAR Packet Filtering. **For LPAR manager firmware 59-7X/79-7X or** later **versions** F9: Used to set transmission bandwidth limitation for VF NIC. Sets from 100 Mbps to 10000 Mbps by the 100 Mbps. **For LPAR manager firmware 58-71/78-71 or later in LPAR manager expansion mode:** F11: Scrolls the screen to the left. F12: Scrolls the screen to the right .	-
(11)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	-	-	Display only
(3)	Sta	-	-	-	Display only
(4)	#VNIC	-	-	-	Display only
(5)	Device	-	✓	-	LPAR manager firmware version 59-0X/79-0X or later
(6)	VNIC Number	-	-	-	Display only
(7)	VNIC Assignment	-	✓	-	
(8)	PageUP/ PageDown keys	-	-	-	Display only
(9)	VNIC Information for Shared NIC/Virtual NIC				
	MAC Address	-	✓	-	
	Tag	✓	✓	-	
	Prm	✓	✓	-	
	VLANID	✓	✓	-	
	Inter-LPAR Packet Filtering	✓	✓	-	LPAR manager firmware 57-30 or later versions.

(9)	VNIC Information for VF NIC				
	MAC Address	-	✓	-	LPAR manager firmware version 59-7X/79-7X or later
	Tag	-	✓	-	
	Prm	-	-	-	
	VLANID	-	✓	-	
	Inter-LPAR Packet Filtering	-	-	-	
	TXRATE	✓	✓	-	

✓: can be changed. -: cannot be changed.

(1) How to change VNIC device types for Shared NIC/Virtual NIC

LPAR manager firmware version 59-0X/79-0X or later

Deactivate the LPAR before changing the VNIC device types.

Display the **Virtual NIC Assignment** screen.

Place the cursor on the value in the LPAR line and the Device column, and press **Enter** to display the subscreen. Select a Device Type and press **Enter**.

The following table shows support for VNIC types per guest OS.

Guest OS	VNIC Device type	Standard server blade				High-performance server blade	
		X55A1	X55A2	X55R3/ X55S3	X55R4	X57A1	X57A2
Red hat Enterprise Linux 5.3	NIC1	✓	-	-	-	-	-
	NIC2	-	-	-	-	-	-
Red hat Enterprise Linux 5.4	NIC1	✓	✓	-	-	✓	-
	NIC2	-	-	-	-	-	-
Red hat Enterprise Linux 5.6	NIC1	✓	✓	-	-	✓	✓
	NIC2	-	-	-	-	-	-
Red hat Enterprise Linux 5.7	NIC1	✓	✓	✓	-	✓	✓
	NIC2	✓	✓	✓	-	✓	✓
Red hat Enterprise Linux 5.9[*5]	NIC1	✓	✓	✓	-	✓	✓
	NIC2	✓	✓	✓	-	✓	✓
Red hat Enterprise Linux 6.1[*1]	NIC1	✓	✓	-	-	✓	✓
	NIC2	-	-	-	-	-	-
Red hat Enterprise Linux 6.2	NIC1	-	-	-	-	-	-
	NIC2	✓	✓	✓	-	✓	✓
Red Hat Enterprise Linux 6.4[*4]	NIC1	-	-	-	-	-	-
	NIC2	✓	✓	✓	✓	✓	✓
Red Hat Enterprise Linux 6.5[*7]	NIC1	-	-	-	-	-	-
	NIC2	✓	✓	✓	✓	✓	✓
Red Hat Enterprise Linux 6.6[*8]	NIC1	-	-	-	-	-	-
	NIC2	✓	✓	✓	✓	✓	✓
Windows Server 2003 R2 SP2	NIC1	✓	✓	-	-	✓	-
	NIC2	-	-	-	-	-	-
Windows Server	NIC1	✓	-	-	-	-	-

Guest OS	VNIC Device type	Standard server blade				High-performance server blade	
		X55A1	X55A2	X55R3/ X55S3	X55R4	X57A1	X57A2
2008	NIC2	-	-	-	-	-	-
Windows Server 2008 SP2	NIC1	✓	✓	✓	-	✓	✓
	NIC2	✓	✓	✓	-	✓	✓
Windows Server 2008 R2	NIC1	✓	✓	-	-	✓	✓
	NIC2	✓	✓	-	-	✓	✓
Windows Server 2008 R2 SP1	NIC1	✓	✓	✓	-	✓	✓
	NIC2	✓	✓	✓	✓	✓	✓
Windows Server 2012	NIC1	-	-	-	-	-	-
	NIC2	-	✓*3	✓*2	✓	✓*3	✓*2
Windows Server 2012 R2	NIC1	-	-	-	-	-	-
	NIC2	-	-	-	✓	-	✓

✓: Supported and available; -: Not supported

*1: "Yes" might be shown for Link detected when you perform the ethtool eth(x) command after performing the ifconfig eth(x) down command. But this will not affect the actual operation.

*2: Supported by LPAR manager firmware version 59-2X/79-2X or later.

*3 Supported by LPAR manager firmware version 59-3X/79-3X or later.

*4 Supported by LPAR manager firmware version 59-4X/79-4X or later.

*5 Supported by LPAR manager firmware version 59-51/79-51 or later.

*6 Supported by LPAR manager firmware version 59-52/79-52 or later.

*7 Supported by LPAR manager firmware version 59-5X/79-5X or later.

*8 Supported by LPAR manager firmware version 59-72/79-72 or later.

(2) How to Change VNIC assignment

Display the **Virtual NIC Assignm**ent screen.

Deactivate the LPAR to change the virtual NIC assignment. Place the cursor on the crossing item of the LPAR in line and the virtual NIC number in the column, and press **Enter** to display the subscreen for selecting the assignment. Place the network segment of the virtual NIC you want to change, and then press **Enter**.



- When LPAR manager operating mode is changed from the expansion mode to standard mode, virtual NIC numbers 8 to 15 assigned to each LPAR and VF NIC definition are released.
- When you have assigned a segment duplicately in LPAR manager expansion mode, the duplicate segment assignment remains even if LPAR manager is changed to the standard mode. To disable the segment duplicate assignment, cancel the setting and then set the shared NIC again.
- When you have defined a setting by the port, the setting per port remains even if LPAR manager is changed to the standard mode. To disable the setting per port, cancel the setting and then set the shared NIC again.

- With LPAR manager in expansion mode, LPARs to which one of virtual NIC numbers 8 to 15 is assigned have restrictions on LPAR migration to LPAR manager in standard mode or without supporting LPAR manager expansion mode.
- More than 16 VF NICs can be assigned to an LPAR on screen. However, you can use up to 16 VF NICs per physical port when activating the LPAR.
- When the total of VF NICs for an LPAR to activate exceeds 16 per physical port, a message “The VF is already assigned the maximum assignable times to LPARs.” appears when you activate the LPAR, and the activation fails.

(3) How to Change MAC address

Display the **Virtual NIC Assignment** screen.

Place the cursor on the crossing item of the LPAR in line and the virtual NIC number in the column, and press **F6**: Change MAC Add to display the subscreen. Enter the new value and press **Enter**. Values to set range from 00:00:00:00:00:00 to FF: FF: FF: FF: FF: FF. The value reserved by LPAR manager, however, cannot be set. Do not set a multicast address and broad cast address. See “(1) MAC address for Virtual NIC” for details of the MAC address.



It is not recommended to change the MAC address .

In case of changing MAC addresses, make sure that there is not the same MAC address port on the network With more than one of the same MAC address on a network, the fatal failure might occur on the network.

(4) How to change VLAN mode

Displays the Virtual NIC Assignment screen.

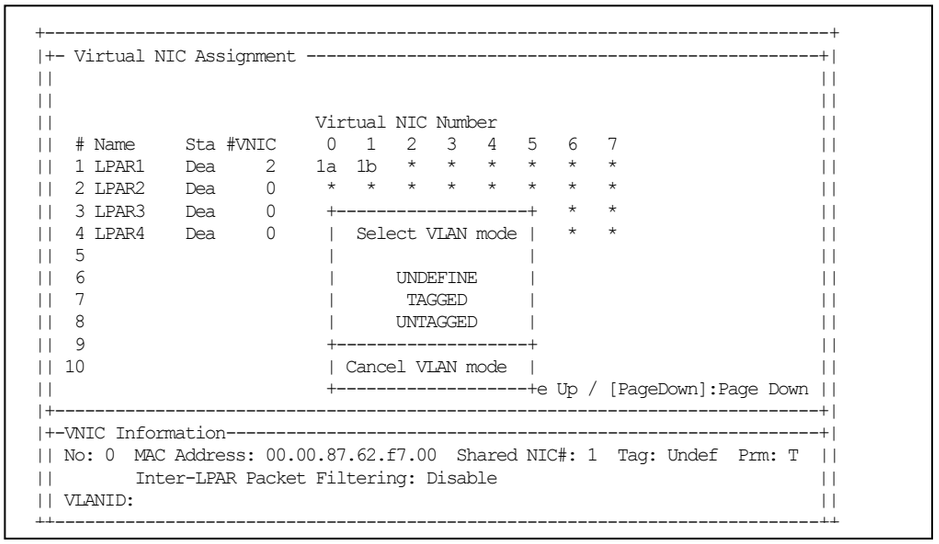


- When VF NIC is assigned, you can specify only [All] to Tagged VLAN ID.
- Do not change VLAN settings for VF NIC assigned to an activated LPAR.

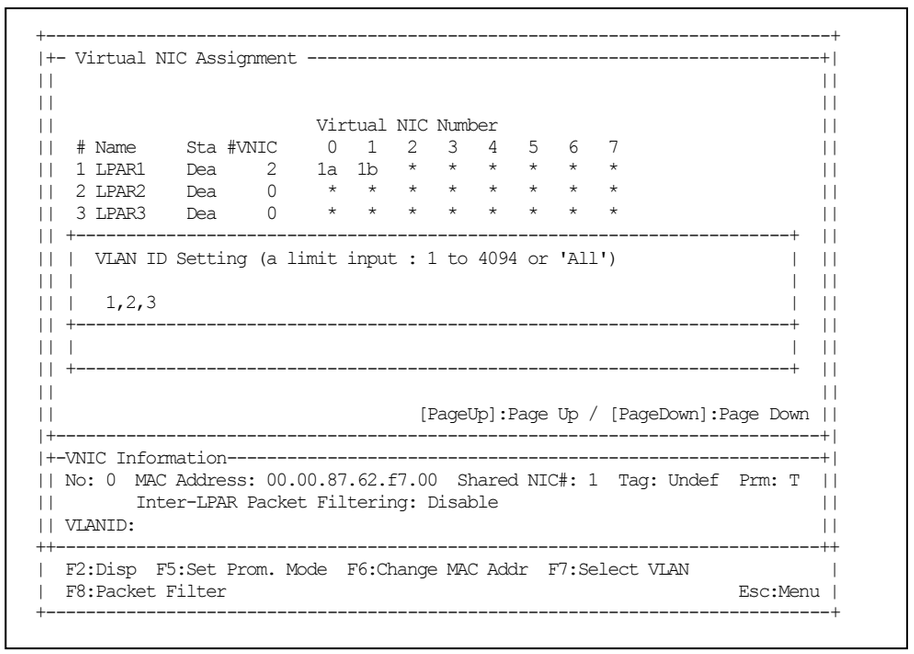
Displays the Virtual NIC Assignment screen.

See “(2) How to use VLAN” for further details.

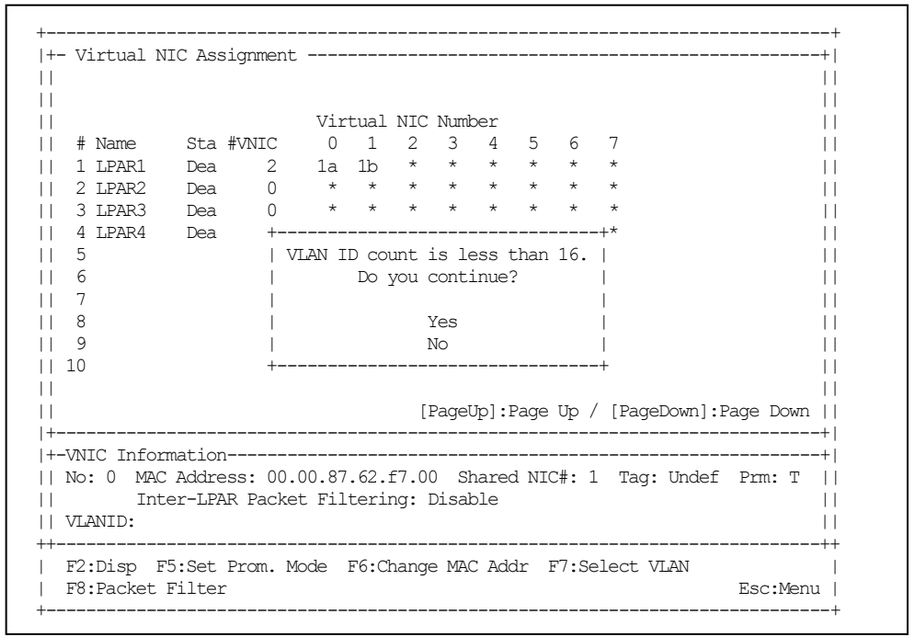
Place the cursor on the intersection between the LPAR in line and the virtual NIC number in column, and press **F7: Select VLAN** to display the subscreen. Select the VLAN mode and press **Enter**.



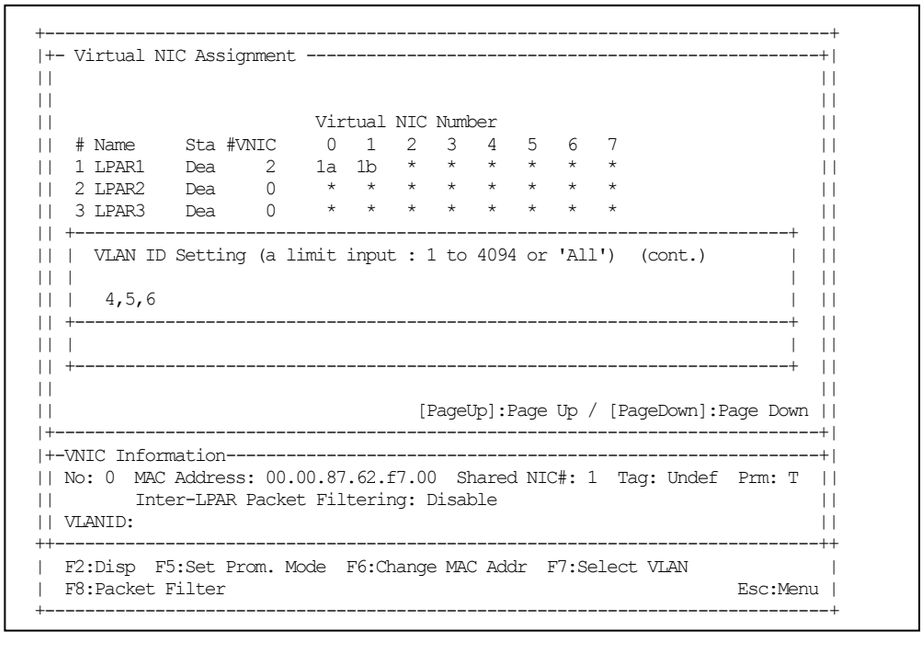
- When selecting **Tagged** or **Untagged** as the VLAN mode, a subscreen is displayed. Enter the VLAN ID to change, and press **Enter**. If a wrong VLAN ID is entered, an error message is displayed. Enter the correct VLAN ID.



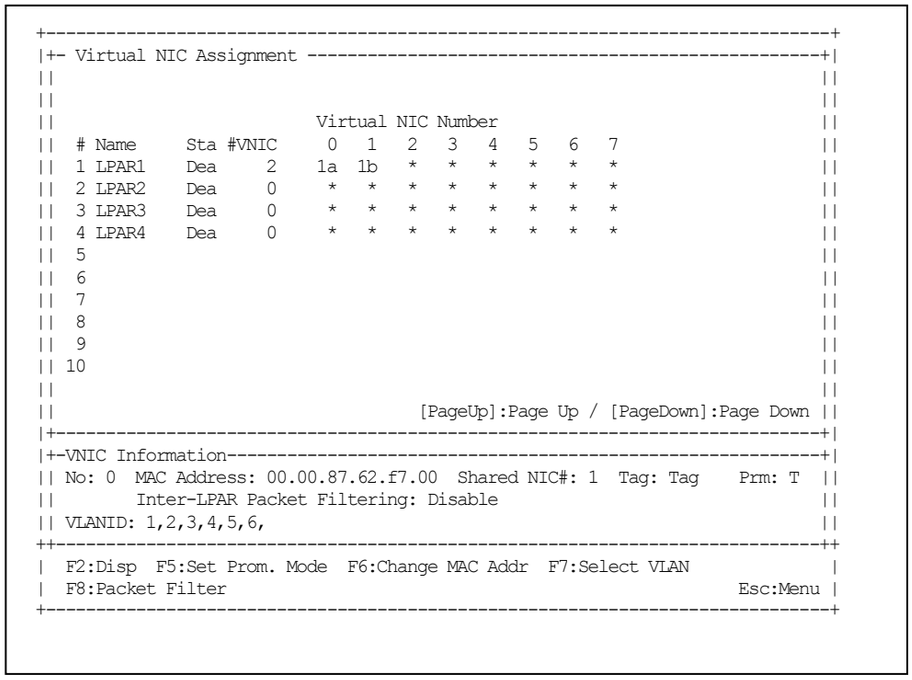
- When selecting **Tagged** as the VLAN mode and the number of VLAN ID settings is less than 16, another subscreen is displayed. Select **Yes** if continuing to set VLAN IDs, or select **No** and press **Enter** if finishing the VLAN ID setting.



When selecting **Yes**, one more subscreen is displayed. Enter the VLAN ID and press **Enter**. If entering the wrong VLAN ID, the subscreen with the error message is displayed. Enter the correct VLAN ID.



- Example: Defining VLAN mode=Tab; VLANID=1, 2, 3, 4, 5, 6 to LPAR1; Virtual NIC 1a with virtual NIC Number0



(5) How to change Promiscuous Mode

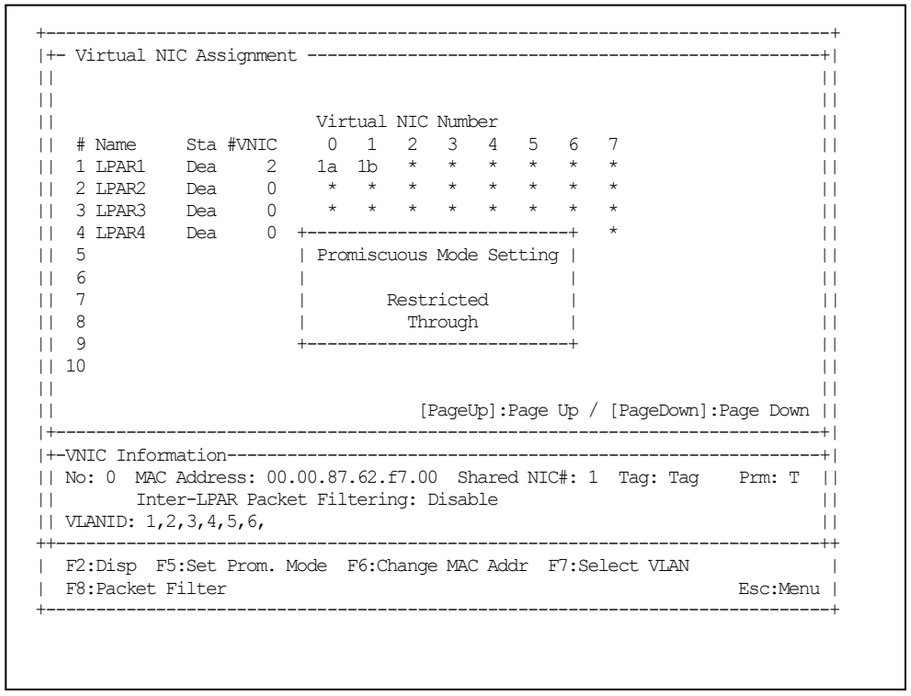
Note

When VF NIC is assigned, you can select only **Restricted**.

Display the **Virtual NIC Assignment** screen.

Place the cursor on the crossing item of the LPAR in line and the virtual NIC number in column, and press **F5: Set Prom. Mode** to show a subscreen. Select a promiscuous mode and press **Enter**.

Promiscuous setting		**Receiving packets**
Guest OS	**LPAR manager screen**	
Disable	Restricted/ Through	Receives only packets addressed to the LPAR (MAC).
Enable	Restricted	Receives only packets addressed to the LPAR (MAC)..
	Through	Receives all packets on the same network segment.



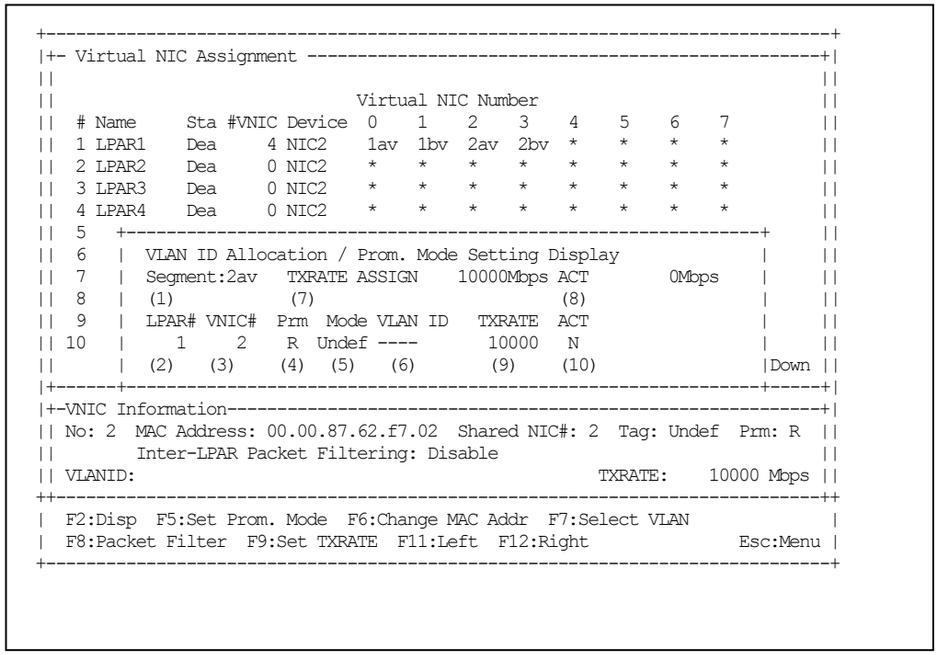
(6) How to show the list of VLAN ID assignment and Promiscuous Mode settings

Press **F2: Disp** to show the list of VLAN ID assignment and Promiscuous Mode settings defined in the network segment identifier where the cursor is placed on this screen.

If placing on the area without the network segment identifier defined, nothing is displayed by pressing **F2: Disp**.

To close the list, press the **Esc** key. To display the list of VLAN ID assignment and Promiscuous Mode settings defined in the different network segment identifier from the list displayed with **F2: Disp.,** press the **Esc** key to close the current display, move the cursor, and press **F2: Disp** again.

The following figure is an example for the list of VLAN ID assignment and Promiscuous Mode settings.



The following table describes the list of VLAN ID assignment and Promiscuous Mode settings.

#	Title	Description
(1)	Segment:	Displays the network segment identifier to show the list.
(2)	LPAR#	Displays the LPAR number to set the network identifier shown in (1) from smaller to larger numbers.
(3)	VNIC#	Displays the virtual NIC number corresponding to the LPAR shown in (2) from smaller to larger numbers.
(4)	Prm	Displays the promiscuous mode defined in the virtual NIC shown in (3).
(5)	Mode	Displays the VLAN mode defined in the virtual NIC shown in (3).
(6)	VLAN ID	Displays VLAN IDs defined in the virtual NIC shown in (3) from smaller to larger numbers.
(7)	TXRATE ASSIGN	LPAR manager firmware version 59-7X/79-7X or later For VF NIC: Displays the total of transmission bandwidth limitation assigned to the LPAR.
(8)	ACT	LPAR manager firmware version 59-7X/79-7X or later For VF NIC: Displays the total of transmission bandwidth limitation used by the activated LPAR.
(9)	TXRATE	LPAR manager firmware version 59-7X/79-7X or later For VF NIC: Displays transmission bandwidth limitation for the LPAR.
(10)	ACT	LPAR manager firmware version 59-7X/79-7X or later For VF NIC: Displays the LPAR status. Y (Activate): Powered on N (Deactivate): Powered off

Note: If the VLAN ID is not defined in the network segment identifier specified by the cursor and F2:Disp VLAN ID Map is pressed, a message ‘VLAN ID is not set.’ is displayed.

The following table describes key operations on the screen for the list of VLAN ID assignment and Promiscuous Mode setting.

#	Key	Description
(1)	Esc	Closes the screen for the list of VLAN ID assignment and promiscuous mode settings.
(2)	PageUp	Displays the previous entry. If no previous entry, nothing happens by pressing this button.
(3)	PageDown	Displays the next entry. If no previous entry, nothing happens by pressing this button.
(4)	Other than keys above	Nothing happens: ignored.

(7) How to change the inter-LPAR packet filtering (for LPAR manager firmware 57-30 or later versions)



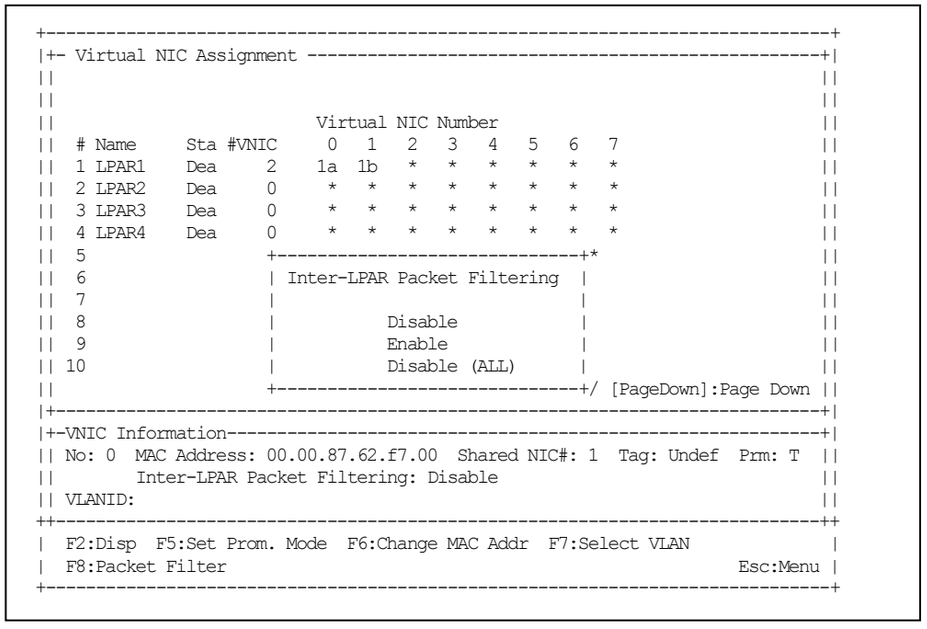
When VF NIC is assigned, you can select only **Disable**.

Display the **Virtual NIC Assignment** screen.

Place the cursor at an item where an LPAR line crosses a VNIC number column, and press **F8: Packet Filter** to display the subscreen. Select an inter-LPAR packet filtering to change, and press **Enter**.

Inter-LPAR packet filtering	Inter-LPAR packets		Packets to outside LPAR manager	Use
	Inside LPAR manager	Outside LPAR manager		
Disable	Transferred	Not transferred	Transferred	Enables inter-LPAR communication in the same segment. Used for inter-LPAR communication only inside LPAR manager.
Enable	Not transferred	Transferred	Transferred	Disables inter-LPAR communication in the same segment. Used for improving independence and security of LPARs when each LPAR has a respective owner.

Inter-LPAR packet filtering	Inter-LPAR packets		Packets to outside LPAR manager	Use
	Inside LPAR manager	Outside LPAR manager		
Disable (ALL)	Transferred	Transferred	Transferred	LPAR manager firmware: 57-31 or later versions Enables inter-LPAR communication in the same segment. Used for inter-LPAR communication using network redundancy configuration.



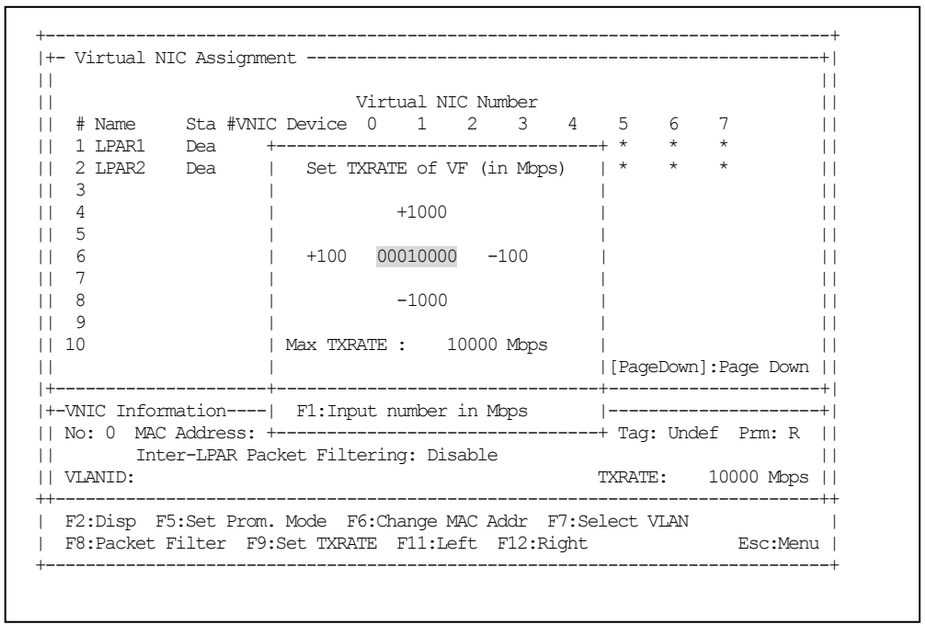
Note:If you press **F8: Packet Filter** when the shared NIC, specified with the cursor, is not defined in the network segment identifier, the subscreen will not be displayed.

(8) How to change the transmission bandwidth limitation for VF NIC (for LPAR manager firmware 59-7X/79-7X or later versions)

Display the Virtual NIC Assignment screen.

Place the cursor at an item where an LPAR line crosses a VNIC number column, and press [F9]: Set TXRATE to display the subscreen. Select a numeric value to change, and press the [Enter] key.

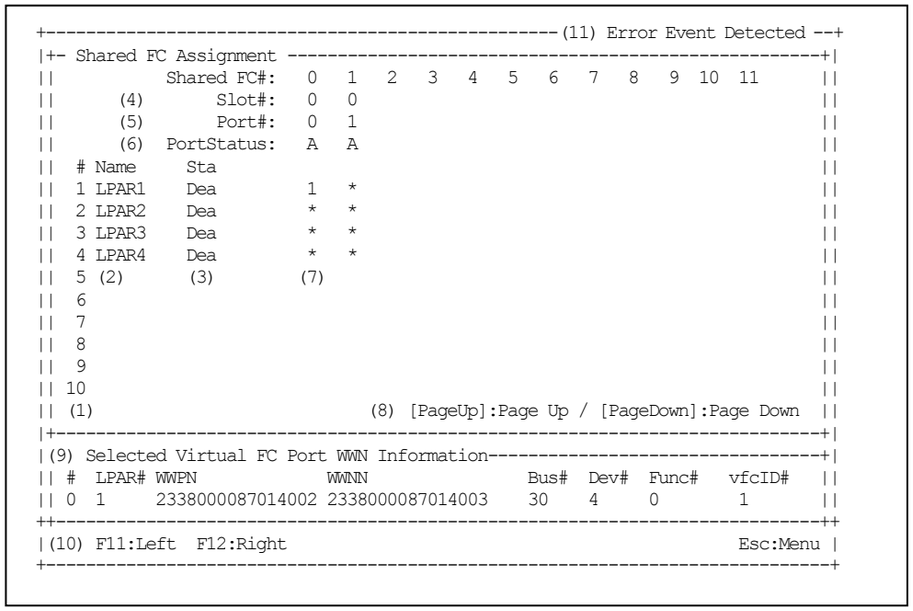
When pressing F1 on the subscreen, you can enter a numeric value by the 100 Mbps.



❑ Shared FC assignment

Following tasks can be done on the Shared FC Assignment screen.

- Assigns a shared FC to each LPAR
- Displays information on the FC selected by the cursor.
- Changes vfcID of the FC selected by the cursor.



The following table describes each item on this screen.

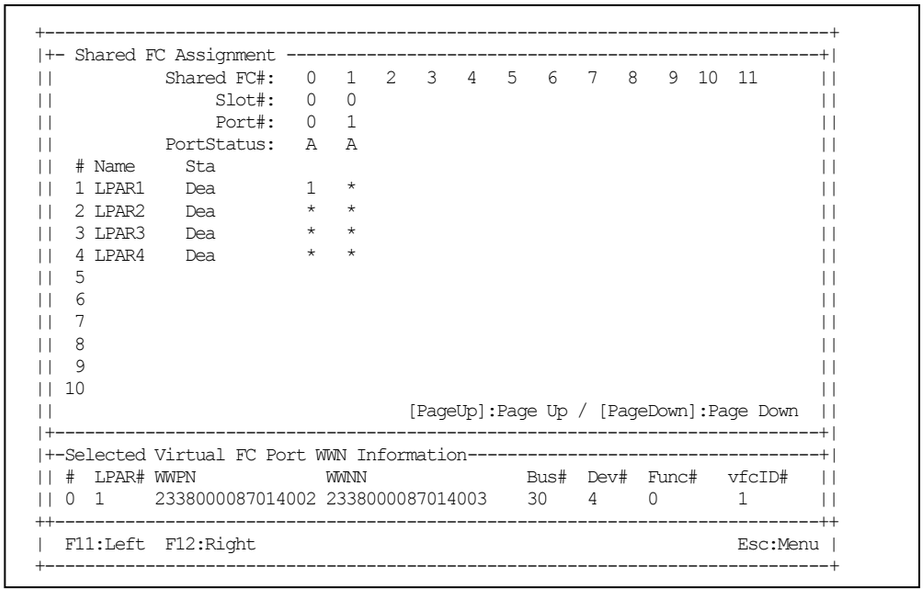
#	Title	Official Name	Description	Initial Value (When LPAR is added)
(1)	#	LPAR Number	Displays LPAR numbers.	-
(2)	Name	LPAR Name	Displays the LPAR name.	NO_NAME
(3)	Sta	Status	Displays the LPAR status. Act (Activate): The LPAR is powered on. Dea (Deactivate): The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot LPAR manager when this happens.	Dea
(4)	Slot#	Slot Number	Displays the number of the PCI slot into which the FC is inserted.	-
(5)	Port#	Port#: Number	Displays the shared FC port number.	-
(6)	PortStatus	PortStatus	Displays the shared FC port status: A: Available. Normal status D: LinkDown. Unavailable because the cable is not connected. C: ConfigCheck. Unavailable due to configuration problem. E: Error Check. Unavailable due to unrecoverable failure. -: (Unknown) Unavailable due to the unknown status. See “(3) PortStatus” for further details.	-
(7)	Shared FC Assignment	Shared FC Assignment	Sets the shared FC port to each LPAR. To assign the shared FC port, select the shared FC port by eh cursor to display a subscreen and set vfcID.	*
(8)	PageUp / PageDown keys	Page Up / Page Down	Page Up: scrolls a page upwards. Page Down: scrolls a page downwards.	-
(9)	Selected Virtual FC Port WWN Information	Virtual FC Port WWN Information	Displays the information on the shared FC port selected by the cursor. LPAR#: Displays the LPAR# to which the shared FC is assigned. WWPN: Displays WWPN of the shared FC. WWNN: Displays WWNN of the shared FC. Bus#/Dev#/Func#: Displays Bus#/Dev#/Fuc# of the PCI device with the shared FC implemented/ vfdOD#: Displays vfcWWN-ID set in the shared FC.	-
(10)	Function Key	Function Key	Displays the function keys that can be used in this screen. F11: Scrolls the page leftward to show the screen. F12: Scrolls the page rightward to show the screen.	-
(11)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	-	-	Display only
(3)	Sta	-	-	-	Display only
(4)	Slot#	-	-	-	Display only
(5)	Port#	-	-	-	Display only
(6)	PortStatus	-	-	-	Display only
(7)	Shared FC Assignment	-	✓	-	
(8)	Selected Virtual FC Port WWN Information	-	-	-	Display only

✓: can be changed. -: cannot be changed.

(1) How to change the shared FC assignment Display the Shared FC Assignment screen.

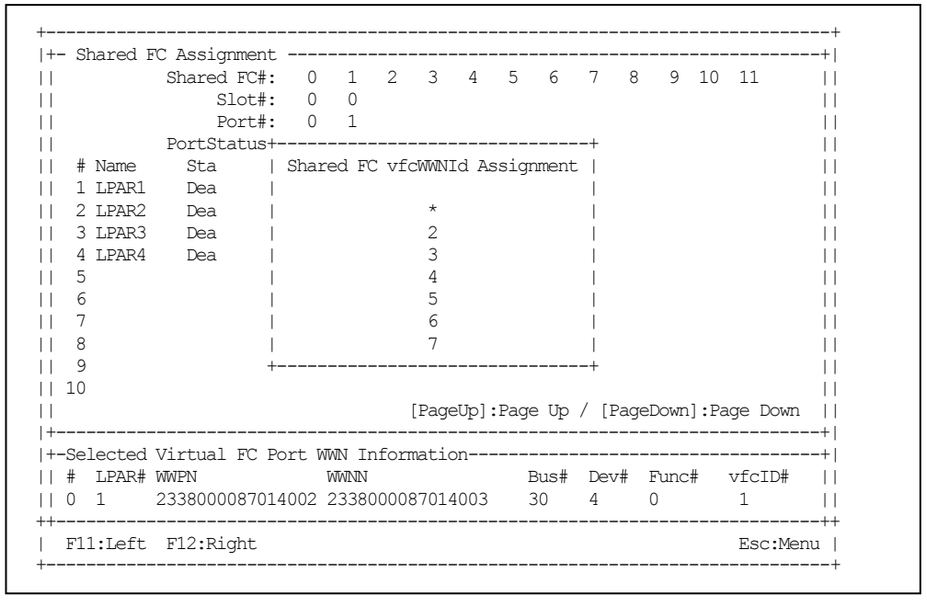
Deactivate the LPAR to change the shared FC assignment.



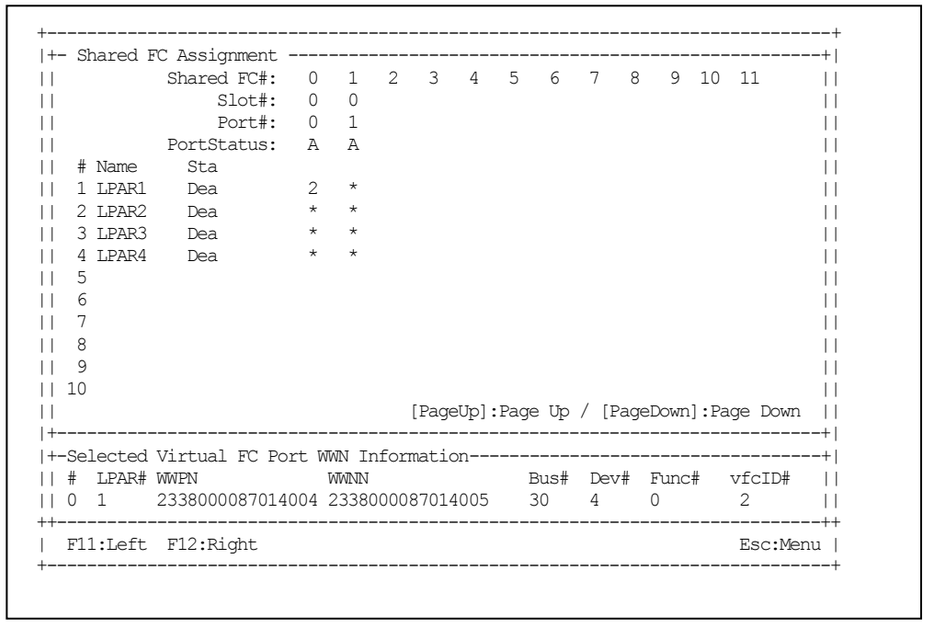
Place the cursor on the intersection between the LPAR in line and the Shared FC number in column, and press **Enter** to display the subscreen for assigning vfcID.

Select the **vfcID#** shown on the subscreen, place the cursor on it, and press **Enter**. You can select from a range of vfcIDs shown in the subscreen per shared FC port. The same vfcID, however, cannot be defined to multiple LPARs.

A screen displayed might be different depending on FC adapters installed.



◆ Example for assigning Shared FC#=0 with vfcID#=2 to LPAR1



(2) WWN for Shared FC

WWN used for the shared FC is called vfcWWN, which is created automatically by the vfcID value assigned on the Shared FC Assignment screen. Select **FC Assign** on the **Shared FC Assignment** screen, the created vfcWWN is displayed in **Selected Virtual FC Port WWN Information**.

The **Allocated FC Information** screen displays WWN information on dedicated and shared FCs implemented in LPAR manager.

(3) PortStatus

If PortStatus is none but "'A': Available", execute the following.

- When PortStatus is "'D': LinkDown, unavailable because the cable is not connected", check the following:
  - Is the FC cable properly plugged into the FC adapter?
  - Are FC switches connected to the FC adapter powered on and performing properly?
  - Does the same symptom occur using a new FC cable? (Execute this if possible.)

  If the problem is not fixed the problem by checking and dealing with the above, contact our maintenance personnel.
- When PortStatus is "C": Config Check, unavailable due to configuration problem", check the following:
  - When 4 Gbps fiber channel adapter is used, does the FC switch support N_Port ID Virtualization (NPIV)? Does the FC switch port have NPIV enabled?
  - When 4 Gbps fiber channel adapter is used, is the FC switch connected Auto?
  - When 8 Gbps Fibre-channel adapter is directly connected to storage, is it a loop connection?

  If the problem is not fixed the problem by checking and dealing with the above, contact our maintenance personnel.
- When PortStatus is "'E': Error Check, unrecoverable failure, contact the reseller from which you purchased this equipment or consult maintenance personnel.

❑ Allocated FC information

The following functions are available on the Allocated FC Information screen.

- Displaying configuration information on the FibreChannel adapter assigned to each LPAR (WWN) as a list

  Standard server blade with LPAR manager firmware version 59-0X or earlier
  High-performance server blade with LPAR manager firmware version 79-0X or earlier]

```
+-------------------------------------------------(12) Error Event Detected --+
|+- Allocated FC Information ------------------------------------------------+|
||   (2)   (3)   (4)   (5)   (6)         (10) Vfc Seed Info. 1 (11) << 1/  1>>||
||   Lpar# Slot# Port# SchMd vfcID WWPN             WWNN                     ||
||      1     0     0     S     1  2338000087014002 2338000087014003          ||
||      2     0     0     S     2  2338000087014004 2338000087014005          ||
||      3     0     0     S     3  2338000087014006 2338000087014007          ||
||      4     0     0     S     4  2338000087014008 2338000087014009          ||
||                                 (7)              (8)                       ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                              (9) [PageUp]:Page Up / [PageDown]:Page Down   ||
|+----------------------------------------------------------------------------+|
+------------------------------------------------------------------------------+
|                                                                     Esc:Menu |
+------------------------------------------------------------------------------+
```

  Standard server blade with LPAR manager firmware version 59-1X or later
  High-performance server blade with LPAR manager firmware version 79-1X or later

```
+-------------------------------------------------(12) Error Event Detected --+
|+- Allocated FC Information ----------------------------(1) WWN (Migration) -+|
||   (2)   (3)   (4)   (5)   (6)          (10) Vfc Seed Info. 1 (11)<< 1/  1>>||
||   Lpar# Slot# Port# SchMd vfcID WWPN             WWPN (Migration)          ||
||      1     0     0     S     1  2338000087014002 2338000087014003          ||
||      2     0     0     S     2  2338000087014004 2338000087014005          ||
||      3     0     0     S     3  2338000087014006 2338000087014007          ||
||      4     0     0     S     4  2338000087014008 2338000087014009          ||
||                                 (7)              (8)                       ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                                                                            ||
||                              (9) [PageUp]:Page Up / [PageDown]:Page Down   ||
|+----------------------------------------------------------------------------+|
+------------------------------------------------------------------------------+
|                                                                     Esc:Menu |
+------------------------------------------------------------------------------+
```

The following table describes items on this screen.

#	Title	Official Name	Description
(1)	Select Display	Select Display	LPAR manager firmware version 59-1X/79-1X or later Selects one of World Wide Names to display: WWN: World Wide Name for FC WWN (Migration): World Wide Name for FC temporarily used in migration
(2)	Lpar#	LPAR Number	Displays the LPAR numbers to which a Fibre-channel (FC) has been allocated, in ascending order. "-" is displayed if the FC has not been allocated to any LPAR.
(3)	Slot#	Slot Number	Displays the physical slot number to which the FC is inserted.
(4)	Port#	Port Number	Displays the port number of the FC.
(5)	SchMd	Scheduling Mode	Displays the FC's scheduling mode. D: Allocated to a LPAR in the dedicated mode. S: Allocated to a LPAR in the shared mode.
(6)	vfcID	VfcWWNID	Displays the configured vfcWWNID if the allocated FC is in the shared mode. Displays "-" for anything other than the shared FC.
(7)	WWPN	World Wide Port Name	Displays the FC's World Wide Port Name. Displays "?" for anything other than the Hitachi FC adapter.
(8)	WWNN	World Wide Node Name	Displays the FC's World Wide Node Name. Displays "?" for anything other than the Hitachi FC adapter.
	WWPN (Migration)	World Wide Port Name (Migration)	LPAR manager firmware version: 59-1X/79-1X or later and LP model: Enterprise Displays World Wide Name for FC temporarily used in migration. For details, see *HVM Navigator User's Guide Migration Functions*. This item is displayed when WWN (Migration) is selected in item (1).
(9)	PageUp/ PageDown keys	Page Up/ Page Down	Page Up: scrolls a page of the screen upwards. Page Down: scrolls a page of the screen downwards.
(10)	Vfc Seed Info.	Vfc seed Information	Displays the Vfc seed information used in creating WWN.
(11)	Pages	Pages	Numerator: Displays the current page. Denominator: Displays the total number of pages.
(12)	Error Event Detected	Error event detection	Displays that LP system logs of the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this screen, press Esc on the LPAR manager Menu screen or open the LP System Logs screen.

(1) How to change WWNs to display

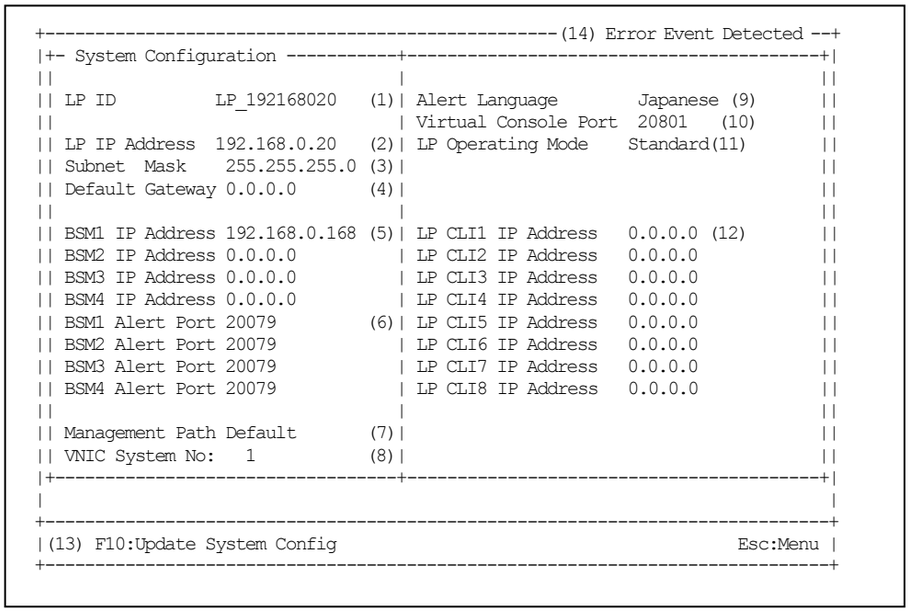
LPAR manager firmware version 59-1X/79-1X or later

Place the cursor on **Select Display** on the upper right and press **Enter** to display a subscreen. On the subscreen, select a WWN to display and press **Enter**.

❑ System configuration

The following functions are available in the System Configuration screen.

- Changes the LP ID, virtual NIC system number or administrative path.
- Changes the IP address of LPAR manager or ServerConductor/Blade Server Manager (BSM).
- Configure the TCP port of the virtual COM console.
- Change LPAR manager operating modes.



The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	LP ID	LPAR manager identifier	Sets the ID that identifies LPAR manager Numbers, in which periods are omitted from the LPAR manager IP address, are reflected as the initial value following "LP_".	LP_0000
(2)	LP IP Address	LPAR manager IP address	Make sure to set the new LPAR manager IP address from the default. Otherwise, you cannot go to another screen.	0.0.0.0
(3)	Subnet Mask	Subnet mask	Make sure to set the new Subnet Mask from the default. Otherwise, you cannot go to another screen.	255.255.255.255
(4)	Default Gateway	Default gateway	Sets the IP address of the Default Gateway.	0.0.0.0
(5)	BSM1~4 IP Address	BSM1~4 IP addresses	Sets the BSM IP addresses. Sets IP address for a server blade on which ServerConductor/Blade Server Manager (BSM), HvmSh command, and HvmGetPerf command operate. When LPAR manager is started, the System Manager 1~4 IP Addresses, which are set to the management module, are applied as the initial values.	-

#	Title	Official Name	Description	Initial Value
(6)	BSM1~4 Alert Port	BSM1~4 Alert ports	Sets the BSM alert port When LPAR manager is started, the System Manager 1~4 Alert Ports, which are set to the management module, are applied as initial values. (Recommended setting)	-
(7)	Management Path	Management path	Displays NIC used for the management path. default: uses onboard NIC for the management path.	default:
(8)	VNIC System No	Virtual NIC system number	Sets a unique value to each LPAR manager system including Compute Blade 1000, Compute Blade 2000, and Compute Blade 320. This value is used as part of the Virtual NIC's MAC address. Without setting this number, you cannot go to another screen.	0
(9)	Alert Language	Alert Language Mode	Sets the language used in the alert messages. When LPAR manager is started, the Language Mode that is set to the management module will be applied as the initial value. (Recommended setting) Japanese: Displays the alert message in Japanese. English: Displays the alert message in English.	-
(10)	Virtual Console Port	Virtual COM console TCP port	Set the TCP port to connect the LPAR guest console via telnet. Can set only a TCP port that is connect to VC1. One is added to the TCP number of VC2 and consecutive TCPs as one is added to the number of VC. When LPAR manager is booted, the TCP ports (serial numbers starting from 20801) that LPAR manager obtains are reflected by default: this setting is recommended.	20801
(11)	LPAR manager Operating Mode	LPAR manager Operating Mode	LPAR manager firmware version 58-71/78-71 or later Set LPAR manager operating modes. Standard: LPAR manager standard mode Expansion: LPAR manager expansion mode When the configuration of the previous version exists, the mode is Standard. - Standard server blade X55R4 model supports only Expansion	Expansion
(12)	LP CLI1-8 IP Address	LP CLI1-8 IP Address	LPAR manager firmware version 58-6X/78-6X or later: Sets LP CLI IP Address. Sets the IP address of a server blade where commands such as PFM, ITRM, and HvmSh operate.	0.0.0.0
(13)	Function Key	Function key	Displays the function keys that can be used in this screen. F10: Used when changes are reflected in the LPAR manager system.	-

#	Title	Official Name	Description	Initial Value
(14)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key on this screen or open the system logs screen.	

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	LP ID	- (*1)	✓	-	
(2)	LP IP Address	- (*1)	✓	✓	
(3)	Subnet Mask	- (*1)	✓	✓	
(4)	Default Gateway	- (*1)	✓	✓	
(5)	BSM 1 - 4 IP Address (*1)	Standard server blades with LPAR manager firmware 58-3X or earlier versions/ High-performance with LPAR manager firmware 78-3X or earlier versions			
		- (*1)	✓	✓	
		Standard server blades with LPAR manager firmware 58-4X or later versions/ High-performance with LPAR manager firmware 78-4X or later versions			
		✓	✓	✓	
(6)	BSM 1 - 4 Alert Port (*1)	Standard server blades with LPAR manager firmware 58-3X or earlier versions/ High-performance with LPAR manager firmware 78-3X or earlier versions			
		- (*1)	✓	✓	
		Standard server blades with LPAR manager firmware 58-4X or later versions/ High-performance with LPAR manager firmware 78-4X or later versions			
		✓	✓	✓	
(7)	Management Path	- (*1)	-	-	Display only
(8)	VNIC System No	- (*1)	✓	-	
(9)	Alert Language	- (*1)	✓	✓	
(10)	Virtual Console Port	- (*1)	✓	-	
(11)	LPAR manager Operating Mode	Standard server blade: LPAR manager firmware 58-71 or later versions High-performance server blade: LPAR manager firmware 78-71 or later versions			
		-	✓	-	
(12)	LP CLI1-8 IP Address	Standard server blade: LPAR manager firmware 58-6X or later versions] High-performance server blade: LPAR manager firmware 78-6X or later versions			
		✓	✓	✓	

✓: can be changed. -: cannot be changed.

(*1) Operation with F10 (Update System Config) should be done with no activated LPAR. If it is performed with an activated LPAR, network communication

between LPARs is lost for several minutes.
SC/BSM shows that LPAR manager is deactivated and no error notification is performed.

(1) How to set the LP ID

Display the **System Configuration** screen.

Place the cursor on the LP ID and press **Enter** to display a subscreen. Enter the new ID on the subscreen. You can use up to 16 characters for the ID.

You can enter the following characters.

Alphanumeric, "~", "@", "#", "$", "%", "^", "-" (hyphen), "+", "=", "_" (underscore), "." (period), "[", "]"

LP ID is used to identify of each when the multiple LPAR manager systems exist. For example, when you control the LPAR manager system from ServerConductor/Blade Server Manager (BSM), LP ID is used to identify each. Therefore, when setting the LP ID, set a value that is unique among all systems including Compute Blade 1000, 2000, and 320.

LPAR manager does not check if the entered value is used for another LPAR manager system.

You can change the LP ID only when all LPARs are deactivated.

(2) How to set the LP IP Address

Display the **System Configuration** screen.

Place the cursor on the LP IP Address and press **Enter** to display a subscreen. Enter the new address on the subscreen and press **Enter**.

The LP IP Address is set as 0.0.0.0 by default. Without setting another address except 0.0.0.0 at the first boot, however, the LPAR manager system will not boot. Do not set a multicast address and broad cast address.

(3) How to set the Subnet Mask

Display the **System Configuration** screen. Place the cursor on the Subnet Mask and press **Enter** to display a subscreen. Enter the new Subnet Mask on the subscreen and press **Enter**.

(4) How to set the Default Gateway

Display the **System Configuration** screen. Place the cursor on the Default Gateway and press **Enter** to open a subscreen. Enter the new Default Gateway on the subscreen and press **Enter**.

(5) How to set the ServerConductor/Blade Server Manager (BSM) IP Address

Display the **System Configuration** screen. Place the cursor on the BSM IP Address and press **Enter** to display a subscreen. Enter the new System Manager IP Address on the subscreen and press **Enter**.



With Standard server blades with LPAR manager firmware 58-4X or later versions/ High-performance with LPAR manager firmware 78-4X or later versions, operation with F10: Update system Config is not required for update. It might take about ten seconds for update.

(6) How to set the ServerConductor/Blade Server Manager (BSM) Alert Port

Display the **System Configuration** screen. Place the cursor on the BSM Alert Port and press **Enter** to display a subscreen. Enter the new SVP Alert Port Number in the subscreen and press **Enter**.

You can set an alert port to a number ranging from 0 to 65535.



With Standard server blades with LPAR manager firmware 58-4X or later versions/ High-performance with LPAR manager firmware 78-4X or later versions, operation with **F10**: Update system Config is not required for update. It might take about ten seconds for update.

(7) How to set the virtual NIC System Number

Display the **System Configuration** screen. Place the cursor on the VNIC System No. and press **Enter** to display a subscreen. Enter the new virtual NIC Setting Number on the subscreen and press **Enter**.

The initial setting of the virtual NIC System Number is 0. Set the new value except 0 at the first LPAR manager boot. Otherwise, the LPAR manager system will not boot.

The following table shows available VNIC System Numbers.

Item	LPAR manager firmware version	
	57-1X or later/78-1X or later	59-21 or later/79-21 or later
Range of numbers available for VNIC System number	1 to 128	1 to 1024

The value set for the virtual NIC System Number will be used as the fourth and fifth bytes of the MAC address of the virtual NIC inside in the LPAR manager system

You can change the virtual NIC System Number only when all LPARs are deactivated.

LPAR manager does not check if the entered value is used for another LPAR manager system.



- VNIC System No is used to create the MAC address to avoid creating the duplicate virtual NIC MAC address. Specify a unique value to every LPAR manager system including BladeSymphony 1000, Compute Blade 2000, and Compute Blade 320.
- Do not change LPAR manager VNIC System No when the system is in operation. If you do, the following problems might occur:
  - MAC address of shared NIC or virtual NIC assigned to a guest OS on the LPAR manager is changed to a different one.
  - When a VNIC System No used by another LPAR manager is re-used, the same MAC address of shared NIC or virtual NIC might be created.

(8) How to set the Alert Language

Display the **System Configuration** screen. Place the cursor on the Alert Language and press **Enter** to display a subscreen. Select a language to use on the subscreen and press **Enter**.

(9) How to set the Virtual Console Port

Display the **System Configuration** screen.

Place the cursor on Virtual Console Port and press **Enter** to display a subscreen. Input a virtual console port that you want to change, and then press **Enter**.

TCP ports from 1024 to 65520 are available for setting..

When changing the virtual console port value, the TCP port is changed. Therefore, reconnecting the LPAR guest screen is necessary.

If the changed value of the virtual console port is the same as the TCP port used in another application, you might not be able to access the LPAR guest console.

(10) How to change the LPAR manager Operating Mode

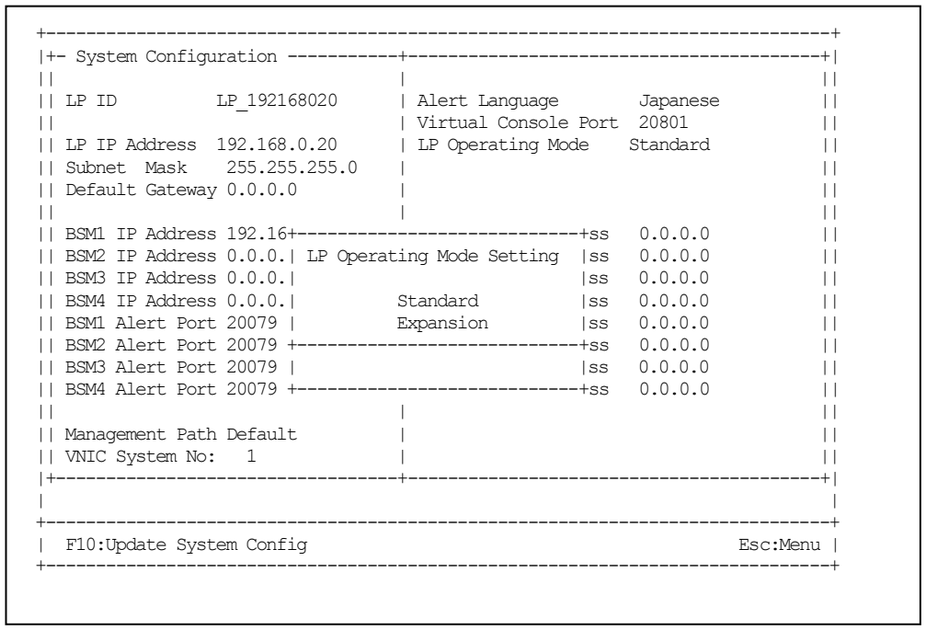
Standard server blades with LPAR manager firmware version 58-71 or later /High-performance server blades with LPAR manager firmware version 78-71 or later



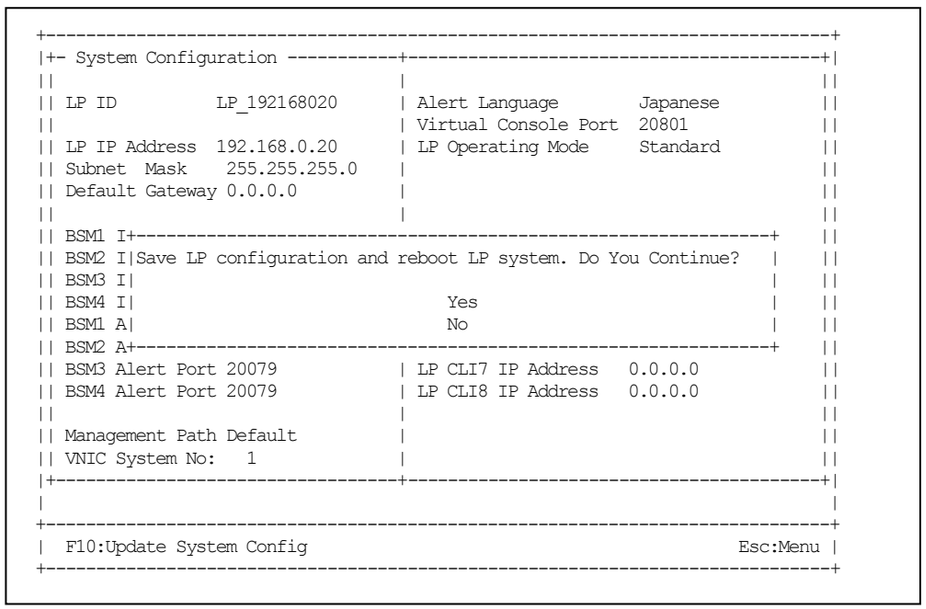
- When LPAR manager Operating Mode is changed from standard mode to expansion mode, LPAR manager starts with memory to which 256 MB is added. The memory for the guest OS is reduced by 256 MB. This might cause some LPARs not to activate due to a memory shortage if the maximum memory has been used in LPAR manager standard mode
- For LPAR manager operating mode, see LPAR manager operating mode, LPAR manager Functions.
- Place the cursor on **LPAR manager Operating Mode** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- System Configuration -----------+-----------------------------------------+|
||                                  |                                         ||
|| LP ID          LP_192168020      | Alert Language        Japanese          ||
||                                  | Virtual Console Port  20801             ||
|| LP IP Address  192.168.0.20      | LP Operating Mode     Standard          ||
|| Subnet  Mask    255.255.255.0    |                                         ||
|| Default Gateway 0.0.0.0          |                                         ||
||                                  |                                         ||
|| BSM1 IP Address 192.168.0.168    | LP CLI1 IP Address   0.0.0.0            ||
|| BSM2 IP Address 0.0.0.0          | LP CLI2 IP Address   0.0.0.0            ||
|| BSM3 IP Address 0.0.0.0          | LP CLI3 IP Address   0.0.0.0            ||
|| BSM4 IP Address 0.0.0.0          | LP CLI4 IP Address   0.0.0.0            ||
|| BSM1 Alert Port 20079            | LP CLI5 IP Address   0.0.0.0            ||
|| BSM2 Alert Port 20079            | LP CLI6 IP Address   0.0.0.0            ||
|| BSM3 Alert Port 20079            | LP CLI7 IP Address   0.0.0.0            ||
|| BSM4 Alert Port 20079            | LP CLI8 IP Address   0.0.0.0            ||
||                                  |                                         ||
|| Management Path Default          |                                         ||
|| VNIC System No:   1              |                                         ||
|+----------------------------------+-----------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F10:Update System Config                                        Esc:Menu |
```

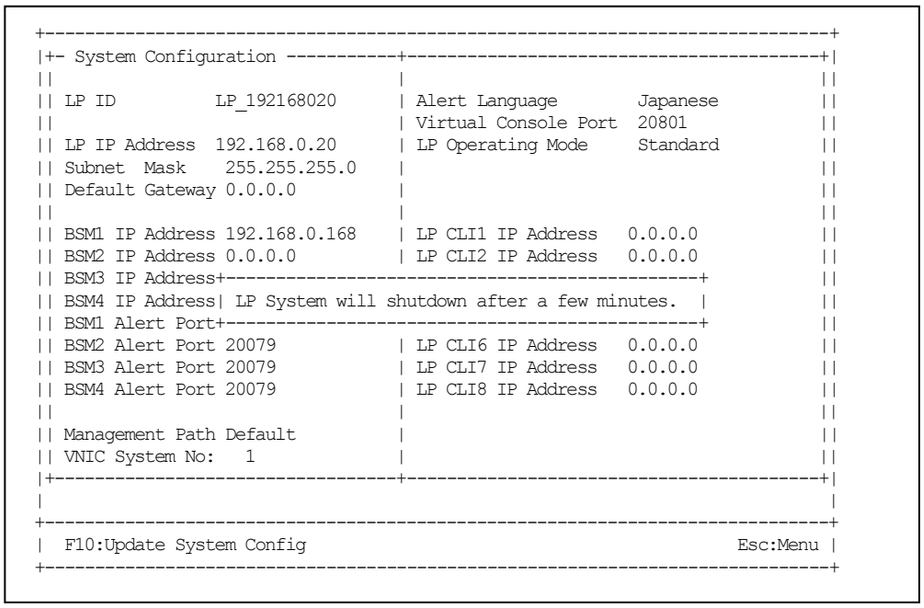
- When the subscreen appears, select **Standard** or **Expansion**.



- When **Standard** or **Expansion** is selected, another subscreen appears. Select **Yes** or **No**. When **Yes** is selected, the configuration is saved, When **No** is selected, the configuration is not saved.

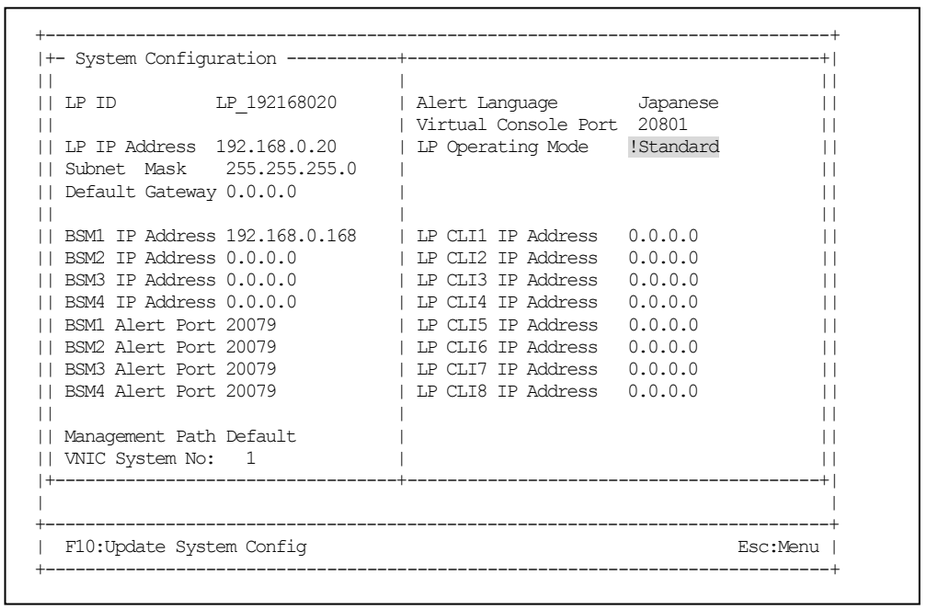


- When the configuration has been saved, LPAR manager will be rebooted.

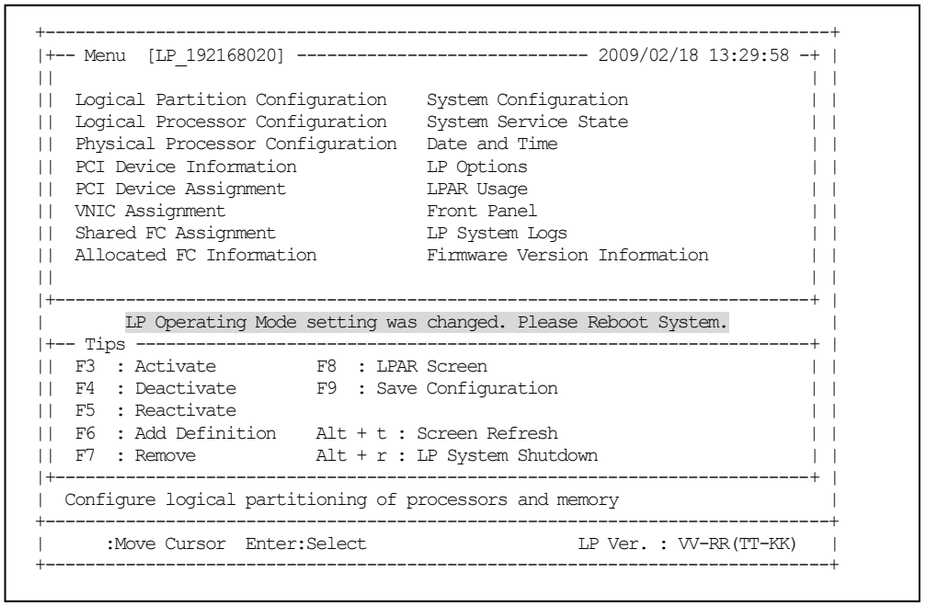




- Change in LPAR manager operating mode is applied at the reboot. If the reboot fails or you have changed the LPAR manager operating mode with HvmSh command, “!” is shown at the head of the LPAR manager operating mode, Standard or Expansion due to the discrepancy between the active LPAR manager operating mode and the one stored in the configuration.



If you keep using LPAR manager without reboot, Menu screen shows a message to let you know that the reboot is not performed.



(11) How to set LP CLI IP Address

Standard server blades with LPAR manager firmware version 58-6X or later /High-performance server blades with LPAR manager firmware version 78-6X or later

Display the **System Configuration** screen. Place the cursor on LP CLI IP Address and press **Enter** to display a subscreen. On the subscreen, type an LP CLI IP Address to change and press **Enter**.

Do not set any multicast address or broadcast address.



The new setting can be applied without **F10: Update System Config.** It might take about 10 seconds to update the setting.

(12) How to apply the changes to the LPAR manager system

To apply all the changes made in the System Configuration screen to the LPAR manager system, press **F10**: **Update System Config** and select **Yes** in the confirmation subscreen that opens.

After selecting "Yes", you will not be able to perform any operations on LPAR manager for one to three minutes.

To cancel the changes, press **F10: Update System Config** and select **No** in the confirmation screen that opens. All changed settings will be restored to their original values.

You cannot move to other screens while changes are being made. To move to another screen, press **F10**, select either **Yes** or **No**, and conclude the change process.

Because it takes time for the changed settings to be reflected in the LPAR manager system, the movement to another screen is not allowed before the reflection has finished completely. If you go to another screen, press **F10: Update System Config** and select **Yes** to complete the reflection, or select **No** to cancel the changes.



- Operation with F10: Update System Config should be done with no activated LPAR. If it is operated with an activated LPAR, network communication between LPARs is lost for several minutes. SC/BSM displays Deactivate as the LPAR manager state and no error notification is performed.
- The operation with F10: Update system Config provides a temporary change in the screen when LPAR manager is running. Thus, the setting, which is not saved, will disappear when LPAR manager is rebooted. Execute **F9: Save configuration** in the **LPAR manager Menu** screen to save the new setting.
- If you change a BSM IP address, BSM alert port, or alert language in this screen, the setting values are effective only during LPAR manager running and not saved with F9: Save Configuration. When you reboot LPAR manager, the value set in the management module will become the initial value.



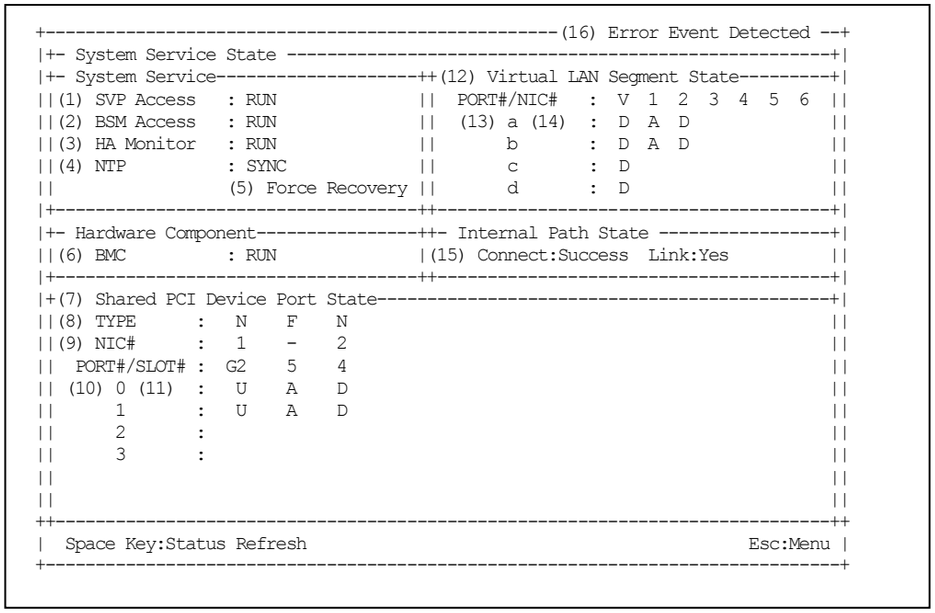
Operation with F10: Update System Config is not required to reflect a setting change. It might take about 10 seconds to reflect a setting change.

❑ System service state

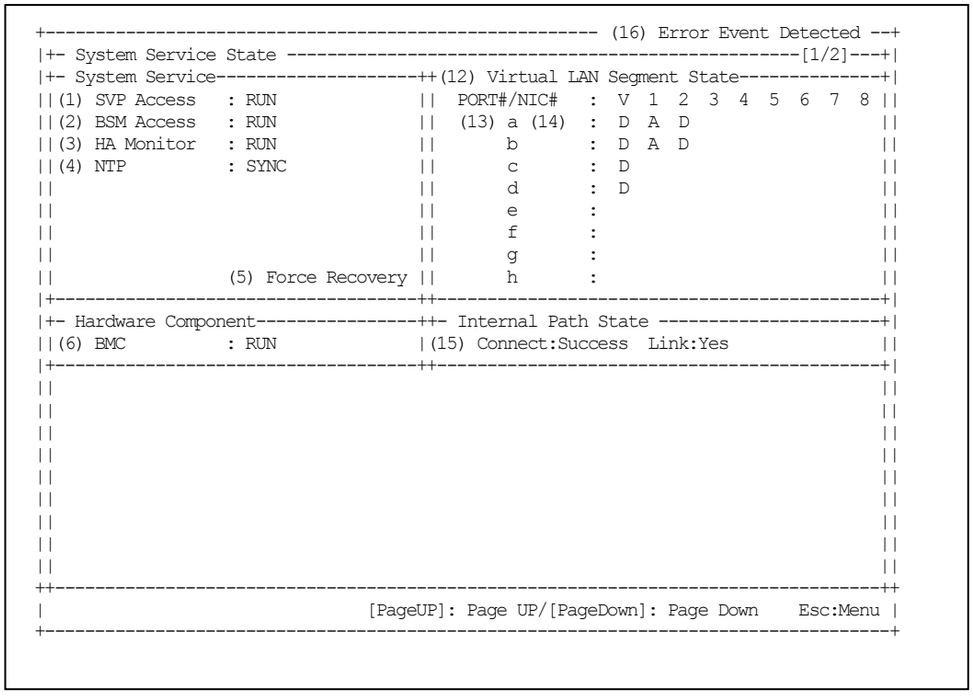
The following functions are available in the System Service State screen.

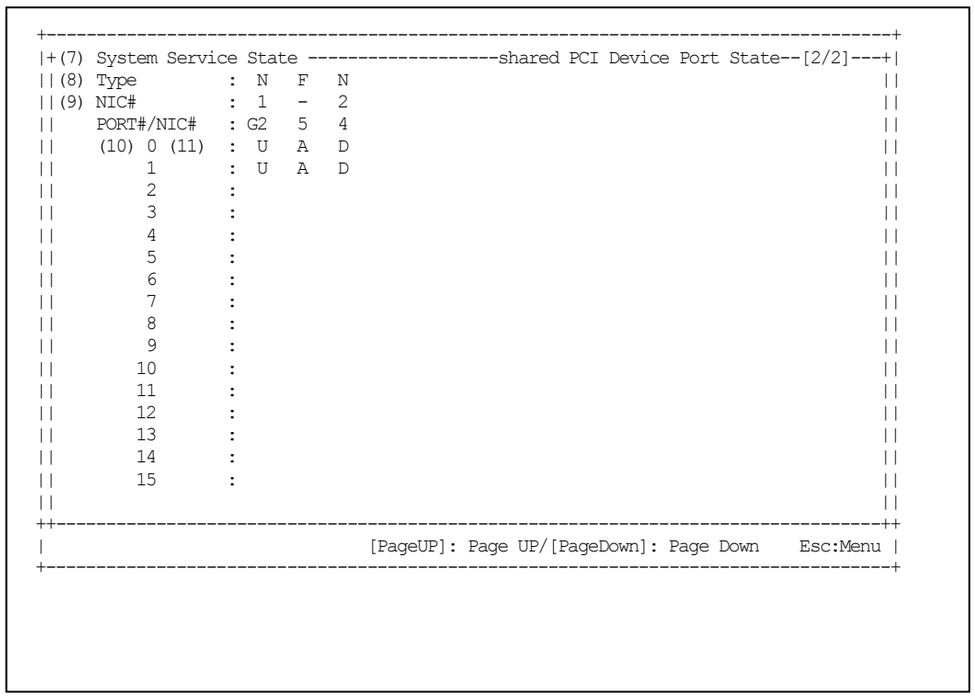
- Displays the System Service status.
- Provides recovery processes if System Service status is abnormal.
- Displays the Hardware Component status.
- Displays the virtual LAN segment status.

Standard server blade with LPAR manager firmware version 58-8X or earlier
High-performance server blade with LPAR manager firmware version 78-8X or earlier



Standard server blade with LPAR manager firmware version 59-0X or later
High-performance server blade with LPAR manager firmware version 79-0X or later





The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	SVP Access	SVP access	Displays the SerVice Processor (SVP) access status. RUN: The service is operating normally. STOP: The service is stopping. ERROR: The service is in the error state. UNKNOWN: No updates from the service patrol.	STOP
(2)	BSM Access	BSM access	Displays the ServerConductor/Blade Server Manager (BSM) access status. RUN: The service is operating normally. STOP: The service is stopping. ERROR: The service is in the error state. UNKNOWN: No updates from the service patrol.	STOP
(3)	HA Monitor	HA monitor	Displays the HA Monitor status. RUN: The service is operating normally. STOP: The service is stopping. ERROR: The service is in the error state. UNKNOWN: No updates from the service patrol.	STOP
(4)	NTP	NTP	LPAR manager firmware version 58-7X/78-7X or later Displays NTP status. SYNC: Synchronization with NTP is successful. NO SYNC: Synchronization with NTP is not executed. ERROR: Synchronization with NTP failed. INACTIVE: Synchronization with NTP is cancelled. With multiple NTP servers configured, having synchronized with any NTP server shows SYNC; not with any NTP server shows ERROR.	No SYNC
(5)	Force Recovery	Forced recovery	Recovers the System Service when it is not operating normally. Note: Operation with Force Recovery should be done with no activated LPAR. If it is operated with an activated LPAR, network communication between LPARs is lost for several minutes. SC/BSM shows that LPAR manager is deactivated and no error notification is performed.	-
(6)	BMC	BMC	Displays the physical Baseboard Management Controller (BMC) status. RUN: BMC is operating normally. ERROR: BMC is in the error state.	RUN

#	Title	Official Name	Description	Initial Value
(7)	Shared PCI Device Port State	Shared PCI device status	Displays the status of the PCI device in the shared scheduling mode on the PCI Device Assignment screen. The following status values are displayed in the position where a port number column indicated in (10) and the slot number line indicated in (11) are intercrossed: When Device Type is N shown in (8): U: Link Up status D: Link Down status E: The device cannot be used due to an unrecoverable error. -: Not available because the status is unknown. Blank: Shared NIC is not defined. When Device Type is F shown in (8): A: Available. The device is in the normal status and usable. D: LinkDown. The device cannot be used because no cable is connected to it. C: ConfigCheck. The device cannot be used because of a configuration problem. E: Error Check. The device cannot be used because of an unrecoverable error. -: Not available because the status is unknown.	D
(8)	TYPE	Device Type	Shows the type of the PCI device in the shared scheduling mode on the PCI Device Assignment screen. N: Network interface Card (NIC) When SR-IOV is enabled, “v” is added to the end. F: Fibre-channel	-
(9)	NIC#	Shared NIC number	Displays the shared NIC numbers when the device type is N shown in (8). Displays “-“ when the device type is F in (8).	-
(10)	PORT#	Port number	Displays the port number.	-
(11)	SLOT#	Slot number	Displays the slot number	
(12)	VLAN Segment	Virtual LAN segment	Displays the status of the virtual LAN segment Displays the following status values at the intersection between the port number column shown in (13) and the shared NIC number line shown in (14). A: Active S: Standby D: Down F: Fault Blank: Not a shared NIC Not supported b VF NIC	
(13)	PORT#	Port number	Displays the port number.	-
(14)	NIC#	NIC number	Displays the NIC number.	-
(15)	Internal Path State	Internal path status	Displays the internal path status. Connect: shows the internal path connection is in ‘Success’ or ‘Fail’. Link: shows ‘Yes’ if the internal paths are linked; ’No’ if not linked.	-

#	Title	Official Name	Description	Initial Value
(16)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

(1) How to recover System Service to a normal state

Display the **System Service State** screen. Since the cursor is already placed on Force Recovery, press **Enter** to display a subscreen. Select **Yes**, and press **Enter**.

Force Recovery processing takes one to three minutes to complete. During the period, you will not be able to perform any operations on LPAR manager.



Operation with Force Recovery should be done with no activated LPAR. If it is operated with an activated LPAR, network communication between LPARs is lost for several minutes. SC/BSM shows that LPAR manager is deactivated and no error notification is performed.

❑ Date and time

The following actions are possible in the Date and Time screen.

- Displays the RTC time of the current LPAR.
- Displays the RTC time when the LPAR is activated or deactivated last.
- Displays the RTC time of the LPAR updated last by the guest.
- Specifies LPAR's SEL (System Event Log) date and time mode.
- Sets LPAR's SEL date and time.
- Sets LPAR's SEL time zone.
- Sets LPAR manager display time.
- Sets LPAR manager system time zone.
- Synchronizes RTC time and SEL time to the LPAR manager system time or UTC time.
- Synchronizes LPAR manager system time with NTP servers.

NOTICE

- It is recommended that you use NTP for operating LPAR manager with LPAR manager firmware version 58-7X/78-7X or later.
- Use the same time zone for management modules, BMC, and LPAR manager. If not, the exact time when a failure occurs cannot be found because each clock shows a different time.
- It is recommended that BMC and LPAR manager clocks be synchronized using the management module.



- See Management Module Settings in Chapter 6 > System Web Console > Time Setting for setting the time of a management module.
- See Server Blade Setup in Chapter 5 > Standard Server Blade Setup Menu (X55A1/X55A2 Models) or High-performance Server Blade Settings (X57A1\X57A2 Models) > BMC Time Settings for setting the BMC time.

Set the logical SEL (System Event Log) time to each LPAR by which the physical SEL detected by LPAR manager is reported to each LPAR.

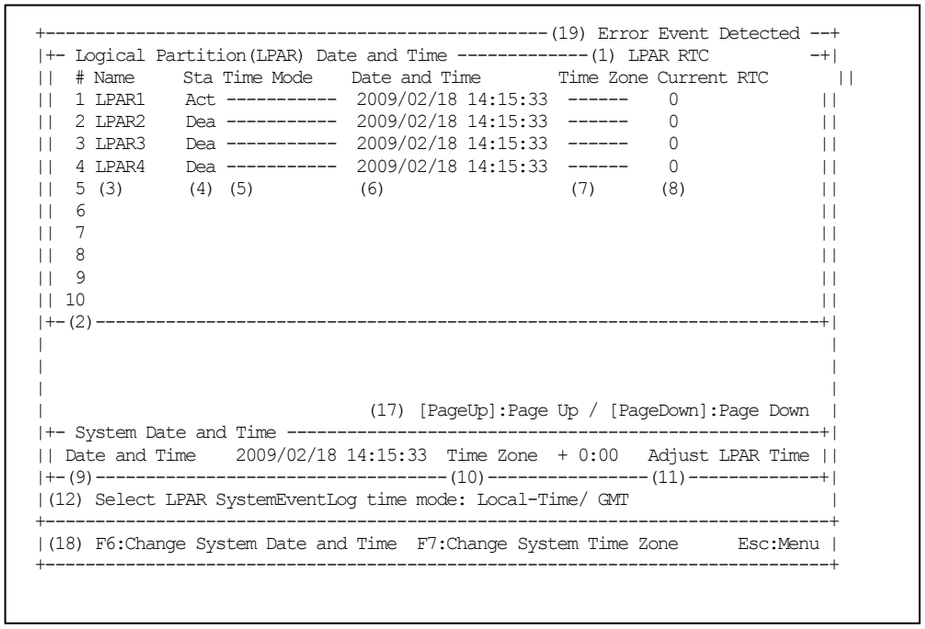
Any values modified on this screen will not be saved automatically in the LPAR manager System and lost at the LPAR manager boot. Press **F9: Save Configuration** on the **LPAR manager Menu** screen explicitly to save the newly set value. To change the LPAR manager system time, change the system equipment time, or synchronize the LPAR manager system time with an NTP server.



Make sure to save the configuration after enabling NTP. If you reboot the LPAR manager without saving it, the LPAR RTC might be out of sync by the time adjusted with NTP.

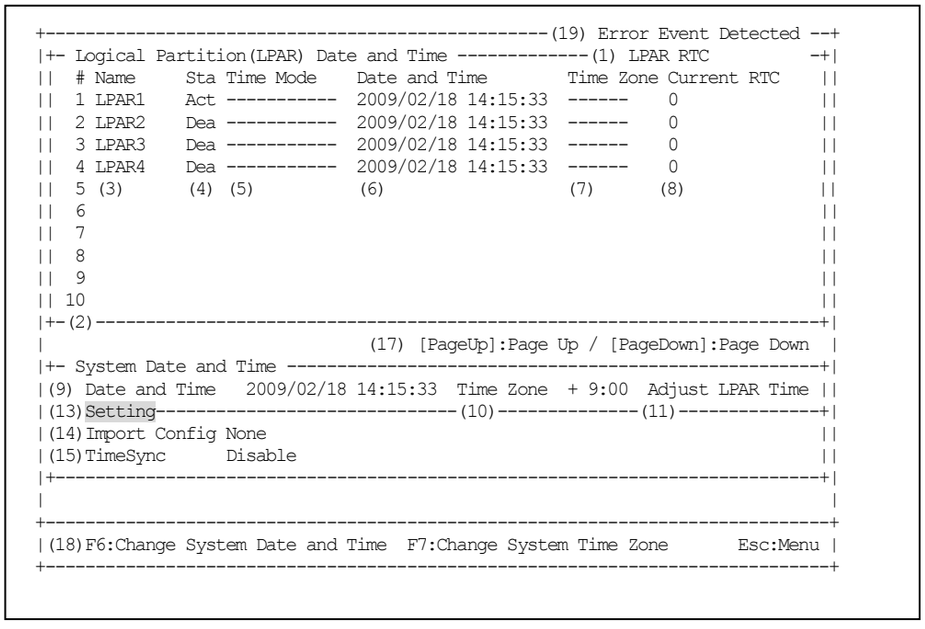
This Date and Time screen refreshes every second, so the cursor display might not be stable. Moreover, the time might be displayed during updating.

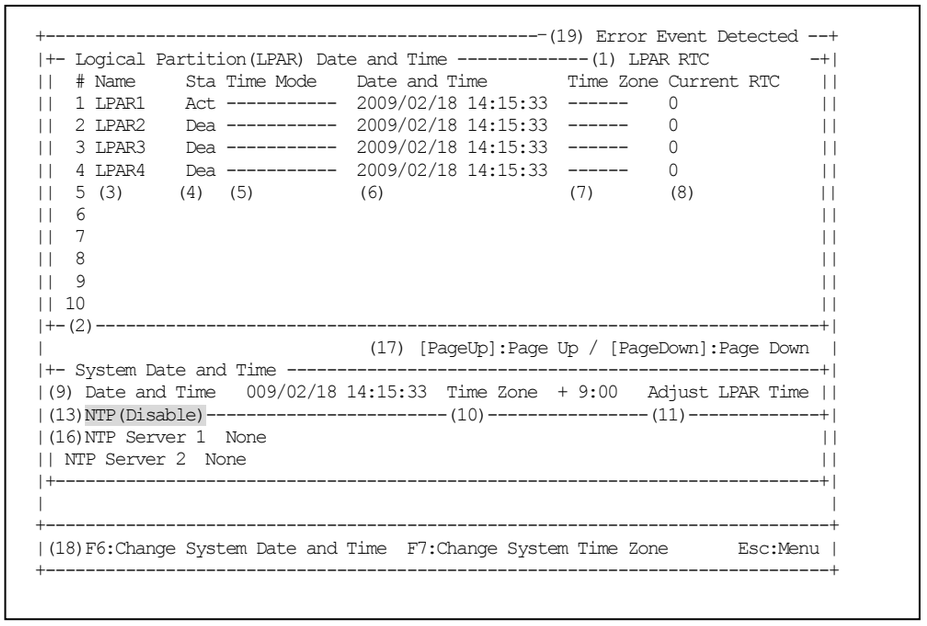
Standard server blades with LPAR manager firmware version 58-6X or earlier/
High-performance server blades with LPAR manager firmware version 78-6X or earlier



Standard server blades with LPAR manager firmware version 58-7X or later/
High-performance server blades with LPAR manager firmware version 78-7X or later

When setting NPT, place the cursor on the shaded area to switch the screen. Setting NTP on the screen allows the LPAR manager system time to be synchronized with the NTP server.





The following table describes each item on this screen.

#	Title	Official Name	Function	Initial Value (When LPAR is added)
(1)	Select Display	Display time selection	Specifies the time information to be displayed. The initial value is set to display the current RTC time (LPAR RTC). LPAR RTC: Displays the current RTC time of the LPAR. LPAR SEL Time: Displays the logical SEL time of the LPAR. Last Activated: Displays the RTC time when the LPAR is activated last. Last Deactivated: Displays the RTC time when the LPAR is deactivated last. RTC Last Modified: Displays the RTC time of the LPAR updated last by the guest.	LPAR RTC
(2)	#	LPAR number	Displays LPAR numbers.	-
(3)	Name	LPAR name	Displays the LPAR name.	NO_NAME
(4)	Sta	Status	Displays the LPAR status. Act (Activated): The LPAR is powered on. Dea (Deactivated): The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot LPAR manager when this happens.	Dea
(5)	Time Mode	SEL date and time mode	Sets the SEL date and time mode. GMT: GMT (Greenwich Mean Time) mode Local-Time: Local time mode The SEL time mode can be set when LPAR SEL Time has been displayed in the display time selection.	Local-Time

#	Title	Official Name	Function	Initial Value (When LPAR is added)
(6)	Date and Time	RTC Time SEL Time	Displays the time selected in the display time selection. The format is “YYYY/MM/DD hh:mm:ss.” YYYY: Calendar year MM: Month DD: Day hh: Hour (24-hour representation) mm: Minute ss: Second The minimum value is 2000/01/01 00:00:00 and the maximum value is 2099/12/31 23:59:59. The SEL time can be set when LPAR SEL Time has been displayed in the display time selection. When the SEL time mode is local mode, the time that has added the SEL time zone is displayed. When the SEL time mode is GMT, the SEL time zone is not added. The time stamp of the logical SEL to be reported to the LPAR becomes this SEL time.	-
(7)	Time Zone	SEL time zone	Displays or sets which time zone the SEL date and time belongs to. When the SEL date and time mode is Local-Time, the changes to this will automatically adjust the SEL date and time. You can specify it on 1-hour basis, and the minimum value is -12 hours and the maximum value is +14 hours. You cannot set when the SEL date and time mode is GMT. The SEL time zone is set only when LPAR SEL Time is displayed in the display time selection.	LPAR manager System time zone
(8)	Current RTC Init RTC	Differential RTC Initial RTC	Displays, in decimal, the difference value between the LPAR RTC time saved in the configuration information and the system time. This value is determined immediately after the LPAR manager system startup and is not changed during LPAR manager system operation. The initial RTC value is displayed when RTC Last Modified has been displayed in the display time selection.	0
(9)	Date and Time	LPAR manager display time	With no LPAR manager system time synchronization with NTP server: Shows the same time as the LPAR manager system time unless F6: Change System Date and Time is performed, With time synchronization with NTP server: Shows the LPAR manager system time. The system equipment time is applied as the default at LPAR manager boot.	-

#	Title	Official Name	Function	Initial Value (When LPAR is added)
(10)	Time Zone	LPAR manager System time zone	Displays or set which time zone the LPAR manager System date and time belongs to. This item only shows the difference between LPAR manager system time and GMT and the values can be changed by pressing F7: Change System Time Zone. You can specify it on 1-hour basis, and the minimum value is -12 hours and the maximum value is +14 hours. Changing the LPAR manager system time zone will not affect the LPAR manager system time. LPAR manager system time zone will be set in the SEL time zone when an LPAR is created.	+ 0:00
(11)	Adjust LPAR Time	LPAR time adjustment	Adjusts the RTC and SEL time for the LPAR to the LPAR manager system time or UTC time. The last RTC time for activation and deactivation of the LPAR and the last update RTC time are cleared at that time. LPAR manager firmware version 59-41/79-41 or later LP System Time: Synchronizes RTC time and SEL time of an LPAR with LPAR manager system time. Specified Zone: In a specified time zone, synchronizes RTC time and SEL time of an LPAR with LPAR manager system time. UTC: Synchronizes RTC time and SEL time of an LPAR with UTC time. All LPAR manager firmware versions All LPAR: Synchronizes time of all LPARs. LPAR name: Synchronizes time of the specified LPARs.	-
(12)	Comment	Comments	Displays a brief description of the selected item.	-
(13)	Select Setting Display	Select Setting Display	LPAR manager firmware version 58-7X/78-7X or later Selects which NTP setting to display. Setting: Displays Import Config and Time Sync. NTP: Displays NTP server settings.	Setting
(14)	Import Config	Import Configuration	LPAR manager firmware version 58-7X/78-7X or later Selects an import source for time synchronization. None: Not import time configuration. SVP: Imports SVP NTP setting and the time zone. BMC: Imports BMC NTP setting and the time zone.	None

#	Title	Official Name	Function	Initial Value (When LPAR is added)
(15)	TimeSync	Time Synchronization	LPAR manager firmware version 58-7X/78-7X or later Selects one of NTP time synchronization settings. Disable: Not synchronize the time with an NTP server. NTP: Synchronizes the time with the NTP server specified to NTP server 1 or NTP server 2. SVP: Synchronizes the time with the NTP server on SVP. LPAR manager system time synchronization with the NTP server is performed immediately after LPAR manager bootup and then every 15 minutes.	Disable
(16)	NTP Server 1 – 2	NTP server setting	LPAR manager firmware version 58-7X/78-7X or later Configures an IP address for NPT servers. - This item is effective only when TimeSynch is set to NTP. - Configure an NTP server with NTP version 3 or 4.	None
(17)	PageUp / PageDown keys	Page Up / Page Down	Page Up: scrolls the SEL Date and Time frame upwards. Page Down: scrolls the SEL Date and Time frame downwards.	-
(18)	Function Key	Function key	Displays function keys available on this screen. F6: Changes the LPAR manager display time. F7: Changes the LPAR manager system time zone. Those keys are available only when TimeSync is set to Disable.	
(19)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	

Conditions to change items in the Date and Time screen

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	Select Display	✓	✓	✓	
(2)	#	-	-	-	Display only
(3)	Name	-	-	-	Display only
(4)	Sta	-	-	-	Display only
(5)	Time Mode	-	Δ	-	Changeable only when LPAR SEL Time has been displayed.
(6)	Date and Time	-	Δ	-	Changeable only when LPAR SEL Time has been displayed.
(7)	Time Zone	-	Δ	-	Changeable when LPAR SEL Time has been displayed. Changeable only when the time mode is only Local-Time.
(8)	Current RTC Init RTC	-	-	-	Display only
(9)	Date and Time	LPAR manager firmware version 58-6X/78-6X or earlier			
		✓	✓	✓	
		LPAR manager firmware version 58-7X/78-7X or later			
		Δ	Δ	Δ	only with TimeSync Disable
(10)	Time Zone	LPAR manager firmware version 58-6X/78-6X or earlier			
		✓	✓	✓	
		LPAR manager firmware version 58-7X/78-7X or later			
		Δ	Δ	Δ	only with TimeSync Disable
(11)	Adjust LPAR Time	-	✓	-	
(12)	Comment	-	-	-	Display only
(13)	Select Setting Display	LPAR manager firmware version 58-7X/78-7X or later			
		✓	✓	✓	
(14)	Import Config	LPAR manager firmware version 58-7X/78-7X or later			
		✓	✓	✓	
(15)	TimeSync	LPAR manager firmware version 58-7X/78-7X or later			
		✓	✓	✓	
(16)	NTP Server 1-2	LPAR manager firmware version 58-7X/78-7X or later			
		✓	✓	✓	
(17)	PageUp / PageDown	-	-	-	Display only

✓: can be changed. -: cannot be changed. Δ: can be changed with some condition

(1) Adjust LPAR Time

You can synchronize LPAR time with LPAR system time or UTC time using Adjust LPAR Time. Adjust LPAR Time is available only for deactivated LPARs.

LPAR manager firmware version 59-40/79-40 or earlier

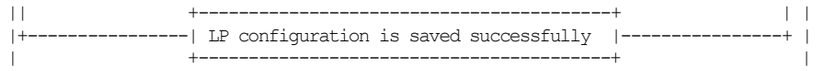
- On the **Date and Time** screen, place the cursor on **Adjust LPAR Time** and press **Enter** to show a subscreen.

```
|+- System Date and Time ------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00  Adjust LPAR Time ||
|+-Setting---------------------------------------------------------------+|
|| Import Config None                                                     ||
|| TimeSync      SVP                                                      ||
|+-----------------------------------------------------------------------+|
```

- Select a target LPAR on the subscreen and press **Enter**.

```
||  6                       +------------------+                          ||
||  7                       | Time Adjust LPAR |                          ||
||  8                       |                  |                          ||
||  9                       |  0 All LPAR      |                          ||
|| 10                       |  1 LPAR1         |                          ||
|+-------------------------|  2 LPAR2         |-------------------------+|
|                          |  3 LPAR3         |e Up / [PageDown]:Page Down  |
|+- System Date and Time -----|  4 LPAR4         |-------------------------+|
|| Date and Time    yyyy/mm/dd+------------------+  + 9:00   Adjust LPAR Time ||
```

- On the **Menu** screen, press **F9: Save Configuration** to save the configuration.



LPAR manager firmware version 59-41/79-41 or later

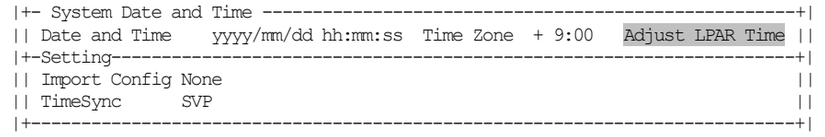
Examples for Adjust LPAR manager System Time, Specified Zone, and UTC are shown below.

Guest OS timer mode	Guest OS timezone	Adjust LPAR Time		
		LPAR manager System Time	Specified Zone	UTC
LocalTime	Same as LPAR manager	✓	-	-
	Different form LPAR manager	-	✓	-
	Unknown	-	-	-
UTC	Same as LPAR manager	-	-	✓
	Different form LPAR manager	-	-	✓
	Unknown	-	-	✓
Unknown	Same as LPAR manager	-	-	-
	Different form LPAR manager	-	-	-
	Unknown	-	-	-

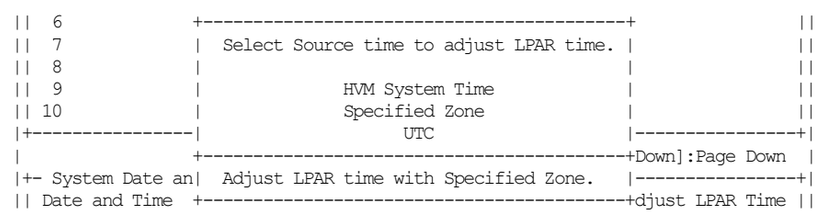
✓: Adjusts LPAR manager system time using Adjust LPAR Time.

- : Adjusts LPAR manager system time using the guest EFI or guest OS Not using Adjust LPAR Time.

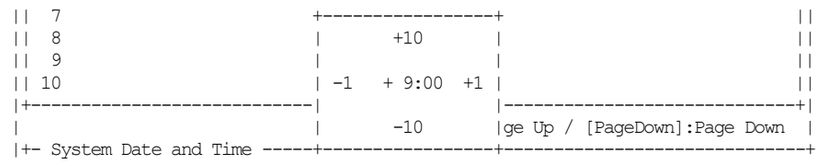
- On the **Date and Time** screen, place the cursor on **Adjust LPAR** Time and press **Enter** to show a subscreen.



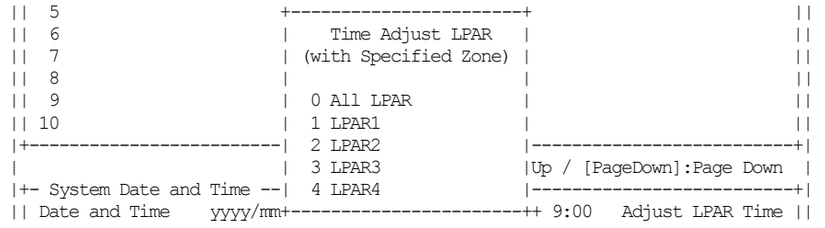
- Select a time source on the subscreen and press **Enter**.



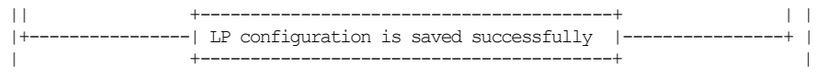
- Select **Specified Zone** in the figure above to show a subscreen. Specify a time zone on the following subscreen and press **Enter**.



- Select the target LPAR and press **Enter**.



- On the **Menu** screen, press **F9**: Save Configuration to save the configuration.



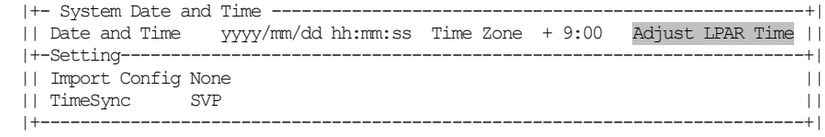
(2) How to adjust the LPAR RTC time

Adjusting the LPAR RTC can be executed only for activated LPARs.

(a) Using NTP (recommended)

Set NTP referring to (9) How to operate LPAR manager using NTP. If you have set NTP, perform the following steps.

- On the Date and Time screen, synchronize the LPAR time using Adjust LPAR Time.



- On the **Menu** screen, press **F9: Save Configuration** to save the configuration.

```
||              +---------------------------------------+              | |
|+--------------| LP configuration is saved successfully |--------------+ |
|               +---------------------------------------+                |
```

(b) Not using NTP

- Shut down all OSs.
- Shut down the LPAR manager.
- Press the **F2** key during the server blade startup, adjust the system equipment time in the EFI setup menu.
- Start LPAR manager and enter the LPAR manager screen.
- On the **Date and Time** screen, place the cursor on **LPAR RTC** and press **Enter** to show a subscreen. Select **LPAR SEL Time** and press **Enter**.

```
 +-------------------------------------------------------------------------------+
 |+- Logical Partition(LPAR) Date and Time ---------------- LPAR RTC          -+|
 ||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
 ||  1 LPAR1    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
 ||  2 LPAR2    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
 ||  3                                                                          ||
 ||  4                                                                          ||
 ||  5                 +---------------------------------+                      ||
 ||  6                 |       Select Display Time       |                      ||
 ||  7                 |                                 |                      ||
 ||  8                 |  LPAR RTC                       |                      ||
 ||  9                 |  LPAR SEL Time                  |                      ||
 || 10                 |  Last Activated                 |                      ||
 |+--------------------|  Last Deactivated               |----------------------+|
 |                      |  RTC Last Modified              |[PageDown]:Page Down  |
 |+- System Date and Tim+---------------------------------+----------------------+|
 || Date and Time    yyy|  Display LPAR SEL Time         |0   Adjust LPAR Time ||
 |+-Setting-------------+---------------------------------+----------------------+|
 || Import Config None                                                          ||
 || TimeSync      Disable                                                       ||
 |+-------------------------------------------------------------------------------+|
 |                                                                               |
 +-------------------------------------------------------------------------------+
 |  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
 +-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor on **Time Zone**, and press **Enter** to show a subscreen. Select your time zone and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
```

- On the **Date and Time** screen, place the cursor on **LPAR SEL Time** and press **Enter** to show a subscreen. Select **LPAR RTC** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  3                                                                          ||
||  4                                                                          ||
||  5                 +--------------------------------+                       ||
||  6                 |       Select Display Time      |                       ||
||  7                 |                                |                       ||
||  8                 |  LPAR RTC                      |                       ||
||  9                 |  LPAR SEL Time                 |                       ||
|| 10                 |  Last Activated                |                       ||
|+--------------------|  Last Deactivated              |---------------------+|
|                     |  RTC Last Modified             |[PageDown]:Page Down  |
|+- System Date and Tim+--------------------------------+---------------------+|
|| Date and Time    yyy|  Display LPAR RTC              |0   Adjust LPAR Time ||
|+-Setting-------------+--------------------------------+---------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, press **F7: Change system Time Zone** to show a subscreen. Set your time zone and press **Enter**.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-----------------------------------------------------------------+|
|| Import Config None                                                       ||
|| TimeSync      Disable                                                    ||
|+-------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, synchronize the LPAR time using **Adjust LPAR Time**.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-----------------------------------------------------------------+|
|| Import Config None                                                       ||
|| TimeSync      Disable                                                    ||
|+-------------------------------------------------------------------------+|
```

- On the **Menu** screen, press **F9: Save Configuration** to save the configuration.

```
||                +----------------------------------------+               | |
|+----------------| LP configuration is saved successfully |---------------+ |
|                 +----------------------------------------+                 |
```

(3) How to switch the time display

Display the **Date and Time** screen.

Place the cursor on **Select Display** at the upper right side and press **Enter** to display a subscreen for selecting the displayed time. Place the cursor on the time to display and press **Enter**.

The time display switches to the selected time information.

(4) How to change the SEL time mode of the LPAR

Display the **Date and Time** screen.

Place the cursor on **Select Display** at the upper right side and press **Enter** to display a subscreen for selecting the time to display. Place the cursor on **LPAR SEL Time** and press **Enter**.

The SEL time of the LPAR appears.

Place the cursor on the **Time Mode** column of the LPAR line to change the SEL time mode and press **Enter**. The subscreen for selecting the SEL time mode appears. Place the cursor on the desired SEL time mode and press **Enter**.

The SEL time mode can be changed only when the relevant LPAR is deactivated.

Specifying “GMT” does not add the SEL time zone to the SEL time. Specifying “Local-Time” adds the SEL time zone to the SEL time.

(5) How to change the SEL time of the LPAR

Display the **Date and Time** screen.

Place the cursor on **Select Display** on the upper right side and press **Enter** to display a subscreen for selecting the time to display. Place the cursor on **LPAR SEL Time** and press **Enter**.

The SEL time of the LPAR appears.

Place the cursor on any column of year/month/day/hour/minute/second of System Event Log Time in the LPAR line to change the SEL time and press **Enter**. The subscreen appears according to the item to be changed. Select the desired time with arrow keys ([↑], [↓], [←], [→]), PageUp, and PageDown and press **Enter**.

The SEL time can be changed only when the relevant LPAR is deactivated.

(6) How to change the SEL time zone of the LPAR

Display the **Date and Time** screen.

Place the cursor on **Select Display** at the upper right side and press **Enter** to display a subscreen for selecting the time to display. Place the cursor on **LPAR SEL Time** and press **Enter**.

The SEL time of the LPAR appears.

Place the cursor on the **Time Zone** column of the LPAR line to change the SEL time zone and press **Enter**. The subscreen for selecting the SEL time zone appears. Change the desired SEL time zone with arrow keys ([↑], [↓], [←], [→]), PageUp, and PageDown and press **Enter**.

The SEL time zone can be set only when the relevant LPAR is deactivated.

(7) How to switch NTP view settings

LPAR manager firmware version 58-7X/78-7X or later

Display the **Date and Time** screen. Place the cursor on **Setting** or **NTP** on the lower left and press **Enter** to display a subscreen. On the subscreen, place the cursor on an item to display and press **Enter**.

(8) How to import NTP settings

LPAR manager firmware version 58-7X/78-7X or later

Display the **Date and Time** screen. Place the cursor on **ImportConfig** and press **Enter** to display a subscreen. On the subscreen, place the cursor on an item to import and press **Enter**.

The following table shows what is displayed on the Date and Time screen when the NTP settings of SVP are imported using Import Config.

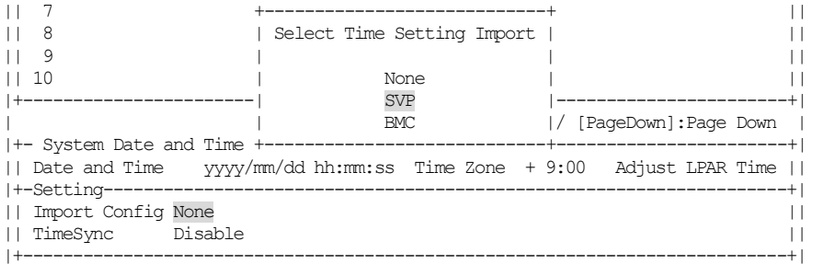
SVP time settings		Date and Time screen			
		Import Config	**TimeSync**	**NTP Server 1**	**NTP Server 2**
Automatic time Synchronization	Disable	SVP	Disable	NTP server0 *1	NTP server1 *1
	Enable	SVP	NTP	NTP server0 *1	NTP server1 *1

*1 When a domain name is specified, “None” is displayed.

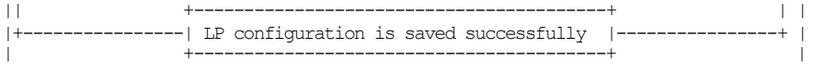
The following table shows what is displayed on the Date and Time screen when the NTP settings of BMC are imported using Import Config.

BMC time settings		Date and Time screen			
		Import Config	**TimeSync**	**NTP Server 1**	**NTP Server 2**
Time synchronization method	Do not use NTP	BMC	Disable	None	None
	Use NTP	BMC	NTP	NTP server1 *1	NTP server2
	Use the Management Module	BMC	SVP	None	None

- Place the cursor on **Import Config** and press **Enter** to show a subscreen. Place the cursor on an item to import and press Enter



- On the **Menu** screen, press **F9: Save Configuration** to save the configuration.





- Make sure that time synchronization settings for import sources have no problem when importing the time synchronization settings from SVP or BMC.
- When you select SVP as the import source, use the management module version A0182 or later. If not, the import fails.
- When you select SVP as the import source, NTP server settings of NTP server 2 and NTP server 3 for SVP time are not be imported.
- If the imported NTP server setting is a domain name, it is ignored by LPAR manager. Only an IP address is available as the NTP server setting.
- Only “hours” is effective as the imported item in LPAR manager, “minutes” is not.
- Daylight saving time is not supported.

(9) How to operate LPAR manager using NTP

LPAR manager firmware version 58-7X/78-7x or later

(a) Time synchronization with a management module. (recommended)

- Shut down all OSs.
- On the **Date and Time** screen, place the cursor on **LPAR RTC** and press **Enter** to open the subscreen. Select **LPAR SEL Time** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR RTC          -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
||  1 LPAR1    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                    ||
||  2 LPAR2    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                    ||
||  3                                                                          ||
||  4                                                                          ||
||  5                +---------------------------------+                     ||
||  6                |       Select Display Time       |                     ||
||  7                |                                 |                     ||
||  8                |  LPAR RTC                       |                     ||
||  9                |  LPAR SEL Time                  |                     ||
|| 10                |  Last Activated                 |                     ||
|+--------------------|  Last Deactivated               |---------------------+|
|                     |  RTC Last Modified              |[PageDown]:Page Down  |
|+- System Date and Tim+---------------------------------+---------------------+|
|| Date and Time    yyy|  Display LPAR SEL Time         |0   Adjust LPAR Time ||
|+-Setting------------+---------------------------------+---------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor **Time Zone** and press **Enter** to open the subscreen. Set your **Time Zone** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
```

- On the **Date and Time** screen, place the cursor on **LPAR SEL Time** press **Enter** to open the subscreen. Select **LPAR RTC** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  3                                                                          ||
||  4                                                                          ||
||  5                 +---------------------------------+                      ||
||  6                 |       Select Display Time       |                      ||
||  7                 |                                 |                      ||
||  8                 |  LPAR RTC                       |                      ||
||  9                 |  LPAR SEL Time                  |                      ||
|| 10                 |  Last Activated                 |                      ||
|+--------------------|  Last Deactivated               |----------------------+|
|                     |  RTC Last Modified              |[PageDown]:Page Down  |
|+- System Date and Tim+---------------------------------+----------------------+|
|| Date and Time    yyy|  Display LPAR RTC               |0   Adjust LPAR Time ||
|+-Setting-------------+---------------------------------+----------------------+|
|| Import Config None                                                          ||
|| TimeSync      Disable                                                       ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor on **TymeSync** and press **Enter** to open the subscreen. Select **Disable** and press **Enter**.

  You need to select “Disable” since time zones cannot be changed with “NTP” selected.

```
||  7                      +--------------------+                           ||
||  8                      | Select NTP Server  |                           ||
||  9                      |                    |                           ||
|| 10                      |      Disable       |                           ||
|+-------------------------|      NTP           |---------------------------+|
|                         |      SVP           |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+-------------------+---------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-------------------------------------------------------------------+|
|| Import Config None                                                        ||
|| TimeSync      Disable                                                     ||
|+-------------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, press **F7: Change System Time Zone** to open the subscreen. Set your time zone and press **Enter**.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-------------------------------------------------------------------+|
|| Import Config None                                                        ||
|| TimeSync      Disable                                                     ||
|+-------------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, place the cursor on **Setting** and press **Enter** to open the subscreen. Select **Setting** and press **Enter**.

```
||  7                     +------------------------+                       ||
||  8                     | Select Setting Display |                       ||
||  9                     |                        |                       ||
|| 10                     |         Setting        |                       ||
|+------------------------|         NTP            |-----------------------+|
|                         +------------------------+p / [PageDown]:Page Down  |
|+- System Date and Time ------------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting--------------------------------------------------------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+---------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, place the cursor on **Timesync** and press **Enter** to open the subscreen. Select **SVP** and press **Enter**.

```
||  7                      +-------------------+                       ||
||  8                      | Select NTP Server |                       ||
||  9                      |                   |                       ||
|| 10                      |      Disable      |                       ||
|+-------------------------|      NTP          |-----------------------+|
|                         |      SVP          |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+------------------+-------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting--------------------------------------------------------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+---------------------------------------------------------------------------+|-
```

- On the **System Service State** screen, confirm that the NTP state is **SYNC**.

```
|+- System Service--------------++-- Virtual LAN Segment State----------------+|
||  SVP Access   : RUN          ||   PORT#/NIC# :  V  1  2  3  4  5  6  7  8  ||
||  BSM Access   : RUN          ||       a      :  D  A  D                    ||
||  HA Monitor   : RUN          ||       b      :  D  A  D                    ||
||  NTP          : SYNC         ||       c      :  D                          ||
||                              ||       d      :  D                          ||
```

- On the **Date and Time** screen, synchronize the LPAR time using **Adjust LPAR Time**.

```
|+- System Date and Time ------------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting--------------------------------------------------------------------+|
|| Import Config None                                                         ||
|| TimeSync      SVP                                                          ||
|+---------------------------------------------------------------------------+|
```

- On the **Menu** screen, press **F9:Save Configuration** to save the configuration.

```
||               +----------------------------------------+               | |
|+---------------| LP configuration is saved successfully |---------------+ |
|                +----------------------------------------+                 |
```

(b) Time synchronization with NTP servers set to NTP Server 1 and 2

- Shut down all OSs.
- On the **Date and Time** screen, place the cursor on **LPAR RTC** and press **Enter** to open the subscreen. Select **LPAR SEL Time** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR RTC          -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
||  1 LPAR1    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
||  2 LPAR2    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
||  3                                                                          ||
||  4                                                                          ||
||  5                +--------------------------------+                      ||
||  6                |       Select Display Time      |                      ||
||  7                |                                |                      ||
||  8                |  LPAR RTC                      |                      ||
||  9                |  LPAR SEL Time                 |                      ||
|| 10                |  Last Activated                |                      ||
|+-------------------|  Last Deactivated              |----------------------+|
|                    |  RTC Last Modified             |[PageDown]:Page Down  |
|+- System Date and Tim+--------------------------------+----------------------+|
|| Date and Time    yyy|  Display LPAR SEL Time        |0   Adjust LPAR Time ||
|+-Setting-------------+--------------------------------+----------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor on **Time Zone** and press **Enter** to open the subscreen. Set your time zone and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time      -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
```

- On the **Date and Time** screen, place the cursor on **LPAR SEL Time** and press **Enter** to open the subscreen. Select LPA**R RTC** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time      -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                     ||
||  3                                                                          ||
||  4                                                                          ||
||  5                +--------------------------------+                      ||
||  6                |       Select Display Time      |                      ||
||  7                |                                |                      ||
||  8                |  LPAR RTC                      |                      ||
||  9                |  LPAR SEL Time                 |                      ||
|| 10                |  Last Activated                |                      ||
|+-------------------|  Last Deactivated              |----------------------+|
|                    |  RTC Last Modified             |[PageDown]:Page Down  |
|+- System Date and Tim+--------------------------------+----------------------+|
|| Date and Time    yyy|  Display LPAR RTC             |0   Adjust LPAR Time ||
|+-Setting-------------+--------------------------------+----------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor on **TymeSync** and press **Enter** to open the subscreen. Select **Disable** and press **Enter**.

  You need to select “Disable” since time zones cannot be changed with “NTP” selected.

```
||  7                      +-------------------+                          ||
||  8                      | Select NTP Server |                          ||
||  9                      |                   |                          ||
|| 10                      |      Disable      |                          ||
|+-------------------------|      NTP          |--------------------------+|
|                         |      SVP          |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+-------------------+--------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-------------------------------------------------------------------+|
|| Import Config None                                                        ||
|| TimeSync      Disable                                                     ||
|+--------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, press **F7: Change System Time Zone** to open the subscreen. Set your time zone and press **Enter**.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-------------------------------------------------------------------+|
|| Import Config None                                                        ||
|| TimeSync      Disable                                                     ||
|+--------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, place the cursor on **Setting** and press **Enter** to open the subscreen. Select **NTP** and press **Enter**.

```
||  7                    +------------------------+                       ||
||  8                    | Select Setting Display |                       ||
||  9                    |                        |                       ||
|| 10                    |         Setting        |                       ||
|+-----------------------|         NTP            |-----------------------+|
|                       +------------------------+p / [PageDown]:Page Down  |
|+- System Date and Time ---------------------------------------------------+|
```

- On the **Date and Time** screen, set an IP addresses of NTP servers.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-NTP(Disable)--------------------------------------------------------------+|
|| NTP Server 1  XXX.XXX.XXX.XXX                                             ||
|| NTP Server 2  XXX.XXX.XXX.XXX                                             ||
|+--------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, place the cursor on **NTP** and press **Enter** to open the subscreen. Select **Setting** and press **Enter**.

```
||  7                    +------------------------+                       ||
||  8                    | Select Setting Display |                       ||
||  9                    |                        |                       ||
|| 10                    |         Setting        |                       ||
|+-----------------------|         NTP            |-----------------------+|
|                       +------------------------+p / [PageDown]:Page Down  |
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-------------------------------------------------------------------+|
|| Import Config None                                                        ||
|| TimeSync      Disable                                                     ||
|+--------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, place the cursor on **Timesync** and press **Enter** to open the subscreen. Select **NTP** and press **Enter**.

```
||  7                      +------------------+                          ||
||  8                      | Select NTP Server |                          ||
||  9                      |                  |                          ||
|| 10                      |      Disable     |                          ||
|+-------------------------|      NTP         |--------------------------+|
|                         |      SVP         |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+-----------------+--------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-----------------------------------------------------------------+|
|| Import Config None                                                      ||
|| TimeSync      Disable                                                   ||
|+------------------------------------------------------------------------+|--+
```

- On the System Service State screen, confirm that the NTP state is SYNC.

```
|+- System Service--------------++-- Virtual LAN Segment State----------------+|
||  SVP Access   : RUN          ||   PORT#/NIC# :  V  1  2  3  4  5  6  7  8  ||
||  BSM Access   : RUN          ||       a      :  D  A  D                    ||
||  HA Monitor   : RUN          ||       b      :  D  A  D                    ||
||  NTP          : SYNC         ||       c      :  D                          ||
||                              ||       d      :  D                          ||
```

- On the **Date and Time** screen, synchronize the LPAR time using **Adjust LPAR Time**.

```
|+- System Date and Time ---------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-----------------------------------------------------------------+|
|| Import Config None                                                      ||
|| TimeSync      SVP                                                       ||
|+------------------------------------------------------------------------+|
```

- On the **Menu** screen, press **F9:Save Configuration** to save the configuration.

```
||               +---------------------------------------+               | |
|+---------------| LP configuration is saved successfully  |---------------+ |
|                +---------------------------------------+                 |
```

(10)How to operate LPAR manager with Not using NTP

LPAR manager firmware version 58-7X/78-7X or later

- On the **Date and Time** screen, place the cursor on **TymeSync** and press **Enter** to open the subscreen. Select **Disable** and press **Enter**.

```
||  7                      +------------------+                          ||
||  8                      | Select NTP Server |                          ||
||  9                      |                  |                          ||
|| 10                      |      Disable     |                          ||
|+-------------------------|      NTP         |--------------------------+|
|                         |      SVP         |e Up / [PageDown]:Page Down  |
|+- System Date and Time ----+-----------------+--------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting-----------------------------------------------------------------+|
|| Import Config None                                                      ||
|| TimeSync      Disable                                                   ||
|+------------------------------------------------------------------------+|
```

- On the **Menu** screen, press **F9:Save Configuration** to save the configuration.

```
||               +----------------------------------------+               | |
|+---------------| LP configuration is saved successfully |---------------+ |
|                +----------------------------------------+                 |
```

(11) How to set an IP address of NTP servers

LPAR manager firmware version 58-7X/78-7X or later

Display the **Date and Time** screen. Place the cursor on **NTP Server 1** or **NTP Server 2** and press **Enter** to display a subscreen. On the subscreen, type an IP address of the NTP server and press **Enter**.

If you type anything other than the IP address format string: XXX.XXX.XXX.XXX, the error occurs. To cancel an NTP server setting, delete the IPaddress of the NTP server and press **Enter**. When the setting is cancelled, None is shown.



Check if NTP server settings and the time zone setting have no problem before setting an IP address to the NTP server.

(12) How to change the LPAR manager display time

Display the **Date and Time** screen. Press **F6: Change System Date and Time** to display a subscreen showing the current time. Type any time you need and press **Enter**. AD year is limited from 2000 to 2099.

(13) How to change the LPAR manager system time zone

Display the **Date and Time** screen. Press **F7: Change System Time Zone** to display a subscreen for selecting a system time zone. With arrow keys [↑], [↓], [←], [→], **PageUp**, and **PageDown**, select a system time zone you need and press **Enter**.

- Shut down all OSs.
- On the **Date and Time** screen, place the cursor on **LPAR RTC** and press **Enter** to open the subscreen. Select **LPAR SEL Time** and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR RTC          -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                  ||
||  1 LPAR1    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
||  2 LPAR2    Dea -----------  yyyy/mm/dd hh:mm:ss  ------                     ||
||  3                                                                          ||
||  4                                                                          ||
||  5                +---------------------------------+                       ||
||  6                |       Select Display Time       |                       ||
||  7                |                                 |                       ||
||  8                |  LPAR RTC                       |                       ||
||  9                |  LPAR SEL Time                  |                       ||
|| 10                |  Last Activated                 |                       ||
|+--------------------|  Last Deactivated               |---------------------+||
|                     |  RTC Last Modified              |[PageDown]:Page Down   |
|+- System Date and Tim+---------------------------------+---------------------+|
|| Date and Time    yyy|  Display LPAR SEL Time         |0   Adjust LPAR Time ||
|+-Setting-------------+---------------------------------+---------------------+|
|| Import Config None                                                         ||
|| TimeSync      Disable                                                      ||
|+-------------------------------------------------------------------------------+|
|                                                                               |
+-------------------------------------------------------------------------------+
|  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
+-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, place the cursor on **Time Zone** and press **Enter** to open the subscreen. Set your time zone and press **Enter**.

```
+-------------------------------------------------------------------------------+
|+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
```

- On the **Date and Time** screen, place the cursor on LP**AR SEL Time** and press **Enter** to open the subscreen. Select LPAR **RTC and press Enter.**

```
 +-------------------------------------------------------------------------------+
 |+- Logical Partition(LPAR) Date and Time ---------------- LPAR SEL Time     -+|
 ||  # Name     Sta Time Mode    Date and Time        Time Zone                 ||
 ||  1 LPAR1    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
 ||  2 LPAR2    Dea Local-Time   yyyy/mm/dd hh:mm:ss  + 9:00                    ||
 ||  3                                                                         ||
 ||  4                                                                         ||
 ||  5                 +--------------------------------+                      ||
 ||  6                 |       Select Display Time      |                      ||
 ||  7                 |                                |                      ||
 ||  8                 |  LPAR RTC                      |                      ||
 ||  9                 |  LPAR SEL Time                 |                      ||
 || 10                 |  Last Activated                |                      ||
 |+---------------------|  Last Deactivated              |----------------------+|
 |                       |  RTC Last Modified             |[PageDown]:Page Down  |
 |+- System Date and Tim+--------------------------------+----------------------+|
 || Date and Time    yyy|  Display LPAR RTC              |0   Adjust LPAR Time ||
 |+-Setting-------------+--------------------------------+----------------------+|
 || Import Config None                                                         ||
 || TimeSync      Disable                                                      ||
 |+-------------------------------------------------------------------------------+|
 |                                                                               |
 +-------------------------------------------------------------------------------+
 |  F6:Change System Date and Time  F7:Change System Time Zone         Esc:Menu |
 +-------------------------------------------------------------------------------+
```

- On the **Date and Time** screen, press **F7: Change System Time Zone** to open the subscreen. Set your time zone and press **Enter**.

```
|+- System Date and Time -------------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting---------------------------------------------------------------------+|
|| Import Config None                                                          ||
|| TimeSync      Disable                                                       ||
|+-------------------------------------------------------------------------------+|
```

- On the **Date and Time** screen, synchronize the LPAR time using **Adjust LPAR Time**.

```
|+- System Date and Time -------------------------------------------------------+|
|| Date and Time    yyyy/mm/dd hh:mm:ss  Time Zone  + 9:00   Adjust LPAR Time ||
|+-Setting---------------------------------------------------------------------+|
|| Import Config None                                                          ||
|| TimeSync      Disable                                                       ||
|+-------------------------------------------------------------------------------+|
```

- On the **Menu** screen, press F**9:Save Configuration** to save the configuration.

```
||                +----------------------------------------+               | |
|+----------------| LP configuration is saved successfully |---------------+ |
|                 +----------------------------------------+                 |
```



- When you change the LPAR manager display time without synchronizing the LPAR manager system time with NTP server, the LPAR manager display time and LPAR manager system time is different. Thus, you cannot determine the time for Adjust LPAR Time on the LPAR manager screen.
- Changing the LPAR manager display time does not affect the LPAR manager system time. To change the LPAR manager system time, change the system equipment time or synchronize the LPAR manager system time with the NTP server.
- Before starting LPAR manager, we recommend that you set your server's system date to a year between 2000 and 2037. Otherwise, we cannot guarantee normal operation of the date and time configuration on this screen.
  LPAR's SEL time and LPAR manager display time can be set at any year between 2000 and 2099 AD. We cannot fully guarantee normal operations of LPAR manager date and time processing if a year later than 2037 is set. Therefore, make sure to set a year to 2037 or earlier for any type of date and time settings while you are running LPAR manager.
- Set a system time zone to the SEL time zone. If not, the SEL time of an LPAR might display a different time, which causes an incorrect time for a failure.

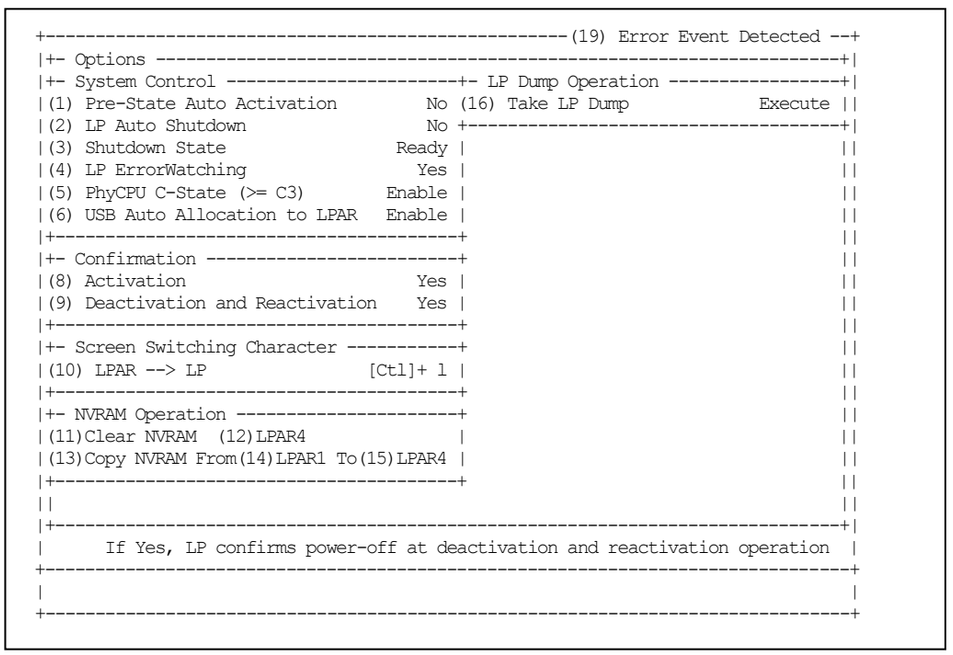
❑ Options

The following functions are available in the LP Options screen.

- Specifies Pre-State Auto Activation or LP Auto Shutdown.
- Enables or Disables the power capping.
- Enables or Disables USB Auto Allocation.
- Enables or Disables Save Changed Config Format.
- LP TimerCounter Base.
- Enables or Disables Save Time Config.
- Specifies whether or not to display the confirmation prompt subscreen when an LPAR is activated.
- Specifies whether or not to display the confirmation prompt subscreen when an LPAR is deactivated or reactivated.
- Sets the character combination used to switch from an LPAR guest screen to the LPAR manager screen.
- Initializes an LPAR's NVRAM (non-volatile RAM).
- Copies NVRAM between LPARs
- Collects the LPAR manager dump
- Specifies the LPAR manager hang-up detection.

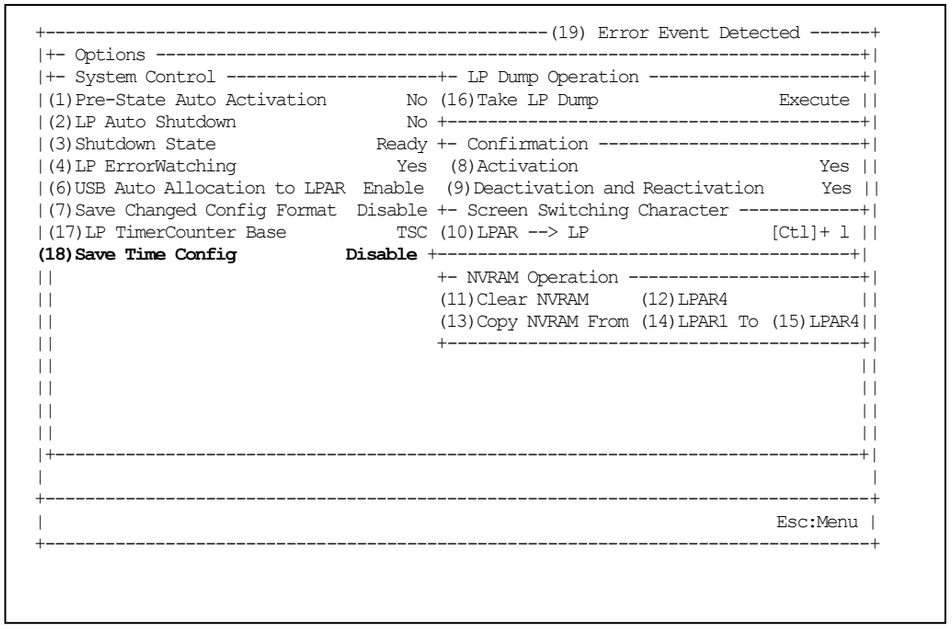
Standard server blade with LPAR manager firmware version 58-8X or earlier

High-performance server blade with LPAR manager firmware version 78-8X or earlier



Standard server blade with LPAR manager firmware version 59-0X or later

High-performance server blade with LPAR manager firmware version 79-0X or later



The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	Pre-State Auto Activation	Pre-State Auto Activation	Specifies whether or not to return the LPARs to their status before rebooting when LPAR manager is rebooted without shutting down the LPAR manager system. Yes: Restores the LPAR to the status it had before the LPAR manager system reboots. No: Does not restore the LPAR to the status it had before the LPAR manager system reboots.	No
(2)	LP Auto Shutdown	LP Auto Shutdown	Specifies whether or not to shut down the LPAR manager system if all LPARs have become deactivated. Yes: Shuts down the LPAR manager system. No: Does not shut down the LPAR manager system. When turning off the system power with UPS, set LP AutoShutdown to “Yes”. When LPAR migration is performed, LP Auto Shutdown is disabled, the same as when the value is “No”.	No

#	Title	Official Name	Description	Initial Value
(3)	Shutdown State	Shutdown State	Displays the LP system shutdown status. Ready: The LPAR manager system is running. InProgress: The LPAR manager system is shutting down. When the LPAR manager system is shut down using the power control schedule of ServerConductor / Blade Server Manager, the shutdown state becomes InProgress when the shutdown time arrives. In this case, it is possible to cancel the shutdown then.	-
(4)	LP ErrorWatching	LPAR manager hang-up detection	Sets whether or not to detect the hang-up of LPAR manager itself. Yes: Detects an LPAR manager hang-up. When detects it, automatically collects LPAR manager dump and restarts LPAR manager. No: Does not detect an LPAR manager hang-up.	Yes
(5)	PhyCPU C-State (>= C3)	Power capping	LPAR manager firmware version 58-7X/78-7X or later Sets whether to enable or disable the power capping. Enable: Enables the power capping function. Disable: Disables the power capping function.	Enable
(6)	USB auto Allocation to LPAR	USB auto Allocation to LPAR	LPAR manager firmware version 59-0X/79-0X or later Enables or Disables USB Auto Allocation. Enable: USB is automatically attached to an LPAR when the LPAR is activated. Disable: USB is automatically attached to only the LPAR specified.	Enable
(7)	Save Changed Config Format	Save Changed Config Format	LPAR manager firmware version 59-0X/79-0X or later Sets whether or not to save a format changed at LPAR manager boot or information that is not yet saved at LPAR manager halt. Enable: Saves the changed configuration format. Disable: Not save the changed configuration format.	Disable
(8)	Activation	Activation confirmation	Specifies the display of a confirmation prompt subscreen when activating an LPAR from the LPAR manager screen. Yes: Displays the confirmation prompt subscreen. No: Does not display the confirmation prompt screen.	Yes
(9)	Deactivation and Reactivation	Deactivation and reactivation confirmation	Specifies the display of a confirmation prompt subscreen when deactivating or reactivating an LPAR from the LPAR manager screen. Yes: Displays the confirmation prompt subscreen. No: Does not display the confirmation prompt screen.	Yes
(10)	Screen Switching Character	Screen switching character	Sets the character used to switch from a guest screen to the LPAR manager screen. "l" (the lower case "L") is set as the default. You can use all lower case letters except for b, h, i, j, m, g, s and z.	l

<table>
<tr><th>#</th><th>Title</th><th>Official Name</th><th>Description</th><th>Initial Value</th></tr>
<tr><td>(11)</td><td>Clear NVRAM</td><td>NVRAM initialization</td><td>Initializes the NVRAM of the LPAR specified by (12).
This operation cannot be performed if "Select" is displayed in (12). (The cursor cannot move over this column.)<table><tr><th>Item</th><th>Behavior when Clear NVRAM performed</th></tr><tr><td>EFI driver settings</td><td>Not initialized</td></tr><tr><td>Boot order</td><td>Initialized</td></tr></table></td><td>-</td></tr>
<tr><td>(12)</td><td>-</td><td>NVRAM initialization LPAR</td><td>Displays the LPAR on which the NVRAM is to be initialized.
You can specify only a deactivated LPAR. "Select" will be displayed if no LPARs have been defined, or if LPARs had been defined, but all LPARs have been activated.
If the specified LPAR has been activated, this column will automatically change to a LPAR that has been deactivated.</td><td>-</td></tr>
<tr><td>(13)</td><td>Copy NVRAM</td><td>Copy NVRAM</td><td>Copies the contents of the NVRAM of the LPAR specified by (14) to the LPAR specified by (15).
This operation cannot be performed if "Select" is displayed in (14) or (15). (The cursor cannot move over this column.)<table><tr><th>Item</th><th>Behavior when Copy NVRAM performed</th></tr><tr><td>EFI driver settings</td><td>Not copied</td></tr><tr><td>Boot order</td><td>copied</td></tr></table></td><td>-</td></tr>
<tr><td>(14)</td><td>-</td><td>LPAR from which the NVRAM is copied</td><td>Displays the LPAR from which the NVRAM will be copied.
"Select" will be displayed if no LPARs have been defined.</td><td>-</td></tr>
<tr><td>(15)</td><td>-</td><td>LPAR to which the NVRAM is copied</td><td>Displays the LPAR to which the NVRAM will be copied.
You can specify only a deactivated LPAR. "Select" will be displayed if no LPARs have been defined, or if LPARs had been defined, but all LPARs have been activated.
If the specified LPAR has been activated, this column will automatically change to a LPAR that has been deactivated.</td><td>-</td></tr>
<tr><td>(16)</td><td>Take LP Dump</td><td>Take LPAR manager dump</td><td>Collects the LPAR manager dump.
The LPAR manager dump collected with this operation is used to analyze failures when they occur.
In normal operation, there is no need to collect the LPAR manager dump. If a problem appears in the equipment, it might become necessary to collect the LPAR manager dump.</td><td>Execute</td></tr>
</table>

#	Title	Official Name	Description	Initial Value
(17)	LP TimerCounter Base	Timer counter base	LPAR manager firmware version 59-2X/79-2X or later Sets a value for timer counter calculation. TSC: Based on TSC (default) CPU frequency: Based on CPU frequency * TSC is the default value due to compatibility with the former LPAR manager firmware version. CPU frequency has a higher precision basically, but precision depends on the system environment. Select a more precise one when operating the system.	TSC
(18)	Save Time Config	Saving time configuration automatically	LPAR manager firmware version 59-41/79-41 or later Sets whether or not to automatically save adjusted time configuration of LPAR manager system time and LPAR time in physical RTC and LPAR manager configuration information. Enable: Enables the Save Time Config. Disable: Disables the Save Time Config.	
(19)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the **Esc** key with this screen or open the system logs screen.	-

(1) What is Pre-State Auto Activation?

Pre-State Auto Activation ascertains and saves the activated/deactivated status of LPARs. In the event of an LPAR manager reboot following a power supply failure or forced shutdown of the server blade, the LPARs can be automatically activated to the same status they were in before the LPAR manager reboot.

When the LPAR manager system is normally shut down, even if Pre-State Auto Activation is set to 'Yes', the LPAR is not automatically activated.

Pre-State Auto Activation automatically activates LPARs in ascending order, where the Auto Activation Order setting is ignored. When node numbers are specified to MN: memory node on the Logical Partition Configuration screen, those LPARs with node number specified are automatically activated first and then other LPARs without specified node numbers are activated.

If for any reason (such as a failure to obtain the allocated memory) the Auto Activation of any LPAR fails, the subsequent LPARs will not be activated automatically.

(2) How to change Pre-State Auto Activation

Display the **LP Options** screen.

Place the cursor on Pre-State **Auto Activation** under **System Control** and press **Enter** to display a subscreen. Use the arrow keys ([↑] or [↓]) to select 'Yes' or 'No', and press **Enter**.

(3) How to change LP Auto Shutdown

Display the **LP Options** screen.

Place the cursor on **LP Auto Shutdown** under **System Control** and press **Enter** to display a subscreen. Use the arrow keys ([↑] or [↓]) to move the cursor to select 'Yes' or 'No', and press **Enter**.



When LPAR migration is performed, LP Auto Shutdown is disabled, the same as when the value is "No".

(4) How to cancel shutdown processing due to the power control schedule

When the LPAR manager system is shut down using the power control schedule of ServerConductor/Blade Server Manager, the shutdown state changes from Ready to In Progress when the shutdown time arrives, and shutdown processing begins. At this time, operations to activate LPARs are suppressed. To cancel this shutdown processing, follow the steps below.

Display the **LP Options** screen.

Place the cursor on **Shutdown State** under **System Control** and press **Enter** to display a subscreen. Use the arrow keys ([↑] or [↓]) to select **Yes**, and press **Enter**.

If all the LPARs are not deactivated within 30 minutes from the start of shutdown processing, the shutdown processing is canceled and the shutdown status returns to Ready. This also removes the suppression of LPAR activation.

(5) How to set LPAR manager hang-up detection

Display the **Options** screen.

Position the cursor on **LP ErrorWatching** of **System Control** and press **Enter** to display a subscreen. Move the cursor with arrow keys ([↑] or [↓]) to select 'Yes' or 'No' and press **Enter**.

(6) How to change the power capping function

LPAR manager firmware version 58-7X/78-7X or later

Make sure deactivate all LPARs before changing the power capping settings.

Display the **LP Options** screen.

Place the cursor on **PhyCPU C-State (>= C3)** and press **Enter** to display a subscreen. On the subscreen, select Enable or Disable by moving the cursor with arrow keys ([↑] or [↓]) and press **Enter**.



When all three conditions described below are met, the OS system time lag might get larger. If so, disable the power saving function.

- With LPAR manager firmware version 58-12 or later/78-12 or later, which the power saving function is added to: supporting C6 state.
- With Windows Server 2008 or Windows Server 2008 R2 or later as a guest OS.
- Operating an application, such as Media Player, which uses the multimedia timer.

(7) How to change the USB Auto Allocation to LPAR

LPAR manager firmware version 59-0X/79-0X or later

Place the cursor on **USB Auto Allocation to LPAR**, and press **Enter** to display a subscreen. Select Enable or Disable on the subscreen and press **Enter**.

See the PCI Device Assignment screen for setting details.

(8) How to change Save Changed Config Format

LPAR manager firmware version 59-0X/79-0X or later

Save Changed Config Format automatically saves a changed configuration format change at LPAR manager boot and unsaved configuration at LPAR manager halt.

This is not a periodical automatic save function.

(a) Saving configuration at LPAR manager boot

The following table describes behaviors depending on the setting when a configuration format is changed at LPAR manager boot.

#	Save Changed Config Format		Version supported
	Disable	Enable	
(1)	Sends an alert reporting a change in configuration formats when LPAR manager initialization is complete.		59-0X/79-0X or later
(2)	Shows the following message to prevent operation until configuration is saved. "Because the Configuration	Saves configuration automatically.	Not supported

#	Save Changed Config Format		Version supported
	Disable	Enable	
	format was updated, saving the Configuration is necessary. Please press the F9 key."		
(3)	Sends an alert to save configuration when the **F9** key is pressed.		59-0X/79-0X or later

(b) Saving configuration automatically at LPAR manager halt

The following table describes behaviors depending on the setting when configuration has not been saved at LPAR manager halt.

#	Save Changed Config Format		Version supported
	Disable	Enable	
(1)	The following menu item is shown in the "**Alt + r** menu: Config save and Shutdown	Selecting "Shutdown" automatically saves the information and then performs shutdown.	Not supported
(2)	Selecting "Config save and Shutdown" saves the information and then performs shutdown. Selecting "Shutdown" performs shutdown without saving configuration.	-	Not supported

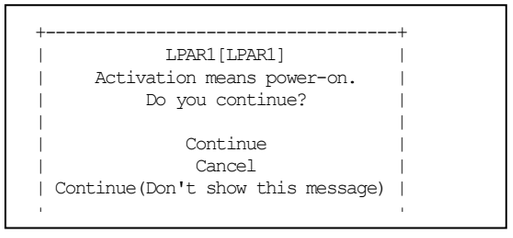
Place the cursor on **Save Changed Config Format** and press **Enter** to show a subscreen. On the subscreen, select Enable or Disable and press **Enter**.

(9) How to skip the confirmation prompt subscreen when activating a LPAR

Display the **LP Options** screen.

Place the cursor on **Activation** below **Confirmation**, and press **Enter** to display a subscreen. Place the cursor on **No**, and press **Enter**. To display the confirmation prompt subscreen, select **Yes**.

You can also stop displaying the confirmation prompt subscreen by activating the LPAR, selecting **Continue: Don't show this message** on the confirmation prompt subscreen and pressing **Enter**.

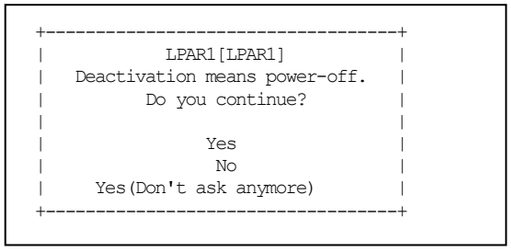


(10) How to skip the confirmation prompt subscreen when deactivating or reactivating an LPAR

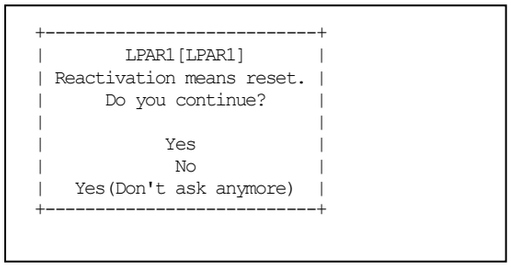
Display the **LP Options** screen.

Place the cursor on **Deactivation and Reactivation** below **Confirmation**, and press **Enter**. Place the cursor on **No**, and press **Enter**. To display the confirmation prompt subscreen, select **Yes**.

You can also stop displaying the confirmation prompt subscreen by deactivating the LPAR, selecting **Yes: Don't ask anymore** on the confirmation prompt subscreen, and pressing **Enter**.



You can also stop displaying the confirmation prompt subscreen by reactivating the LPAR, selecting **Yes: Don't ask anymore** on the confirmation prompt subscreen, and pressing **Enter**.



(11) How to change Screen Switching Character

Display the **LP Options** screen.

Place the cursor on **Ctrl + I,** and press **Enter** to open a subscreen. Enter the new character on the subscreen, and press **Enter**.

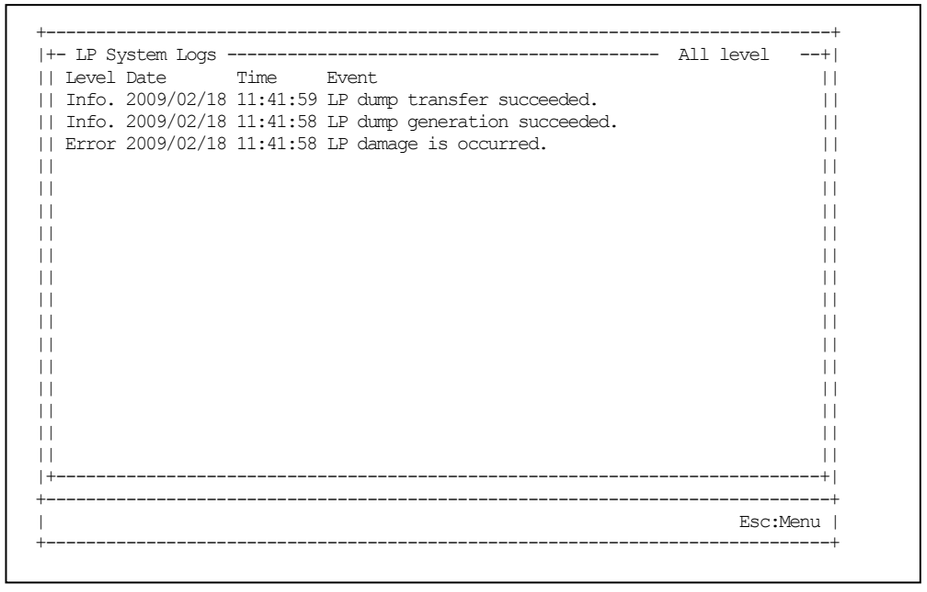
You can use all lower-case letters except for b, h, i, j, m, g, s and z.

(12)How to collect the LPAR manager dump

> ***NOTICE***
>
> The LPAR manager dump is saved in the non-volatile storage of a management module. If a failure occurs, the dump may be automatically collected. Therefore, check if the LPAR manager dump has been automatically collected beforehand to prevent the dump from being overwritten by the operation. Rebooting LPAR manager is not required after dump collection.

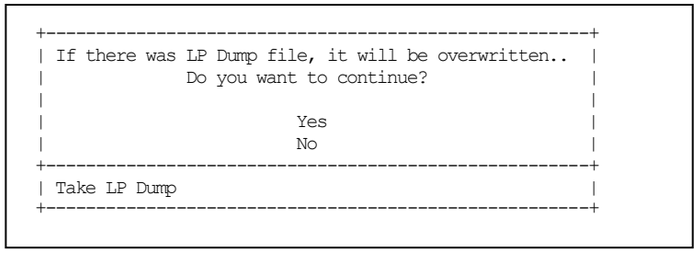
To check whether the LPAR manager dump has been automatically collected or not, follow the steps below.

- Display the **LP System Logs** screen.
- Set the level selection to **All level**.
- Check that there is no LP system log entry that displays “LPAR manager dump generation succeeded.”

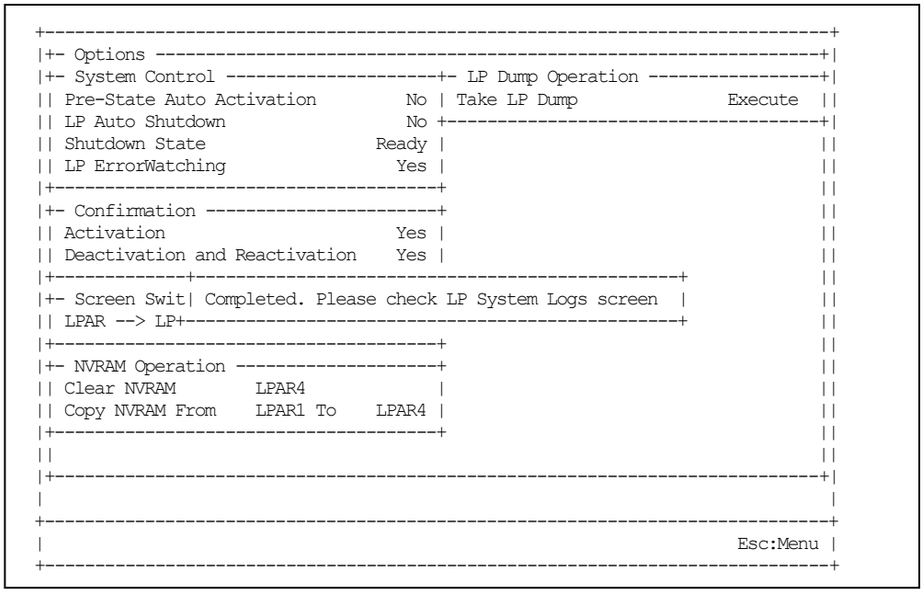


If there is an LP system log entry indicating “LPAR manager dump generation succeeded", contact maintenance personnel. If that kind of LP system log entry has not been obtained, follow the instructions below.

- Display the **Options** screen.
  - Place the cursor on the **Execute** field under **Take LP Dump** and press **Enter** to display a subscreen. Select **Yes** on the subscreen.

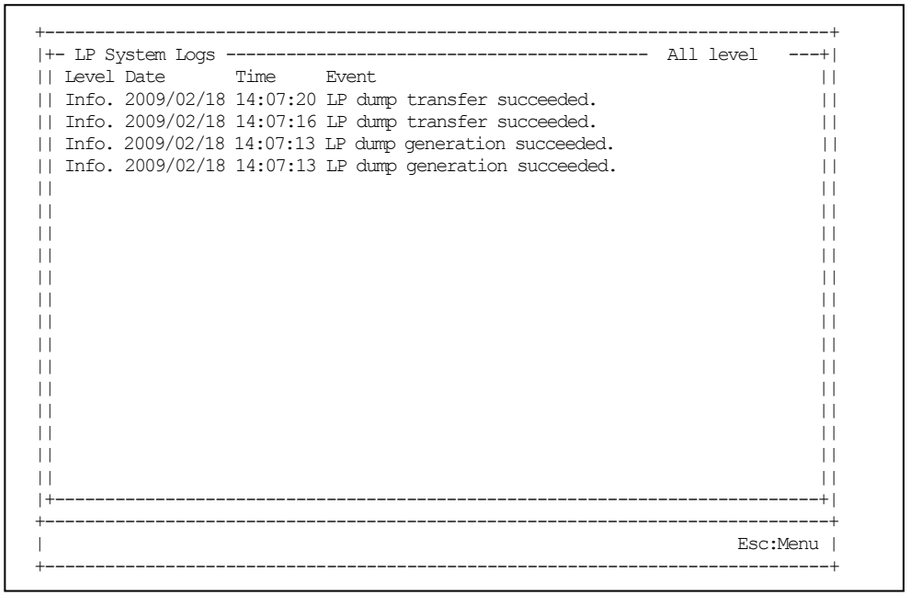


Check that the subscreen shown below appears.



The display shown above indicates that the LPAR manager dump collection has been completed. Follow the steps below to check that the LPAR manager dump has been correctly generated and written to the non-volatile storage of the Management Module.

- Display the **LP System Logs** screen.
- Set the level selection to **All level**.
- Check that there are two LP system log entries when you performed the LPAR manager dump collection indicating “LPAR manager dump transfer succeeded.”



If there are two LP system log entries indicating “LPAR manager dump transfer succeeded”, see “DL Commands” in Chapter 6 and create a failure analysis log file following the instructions in “D. Dump log to file”. Then export that log file to an external medium, and contact the reseller from which you purchased the equipment or maintenance personnel.

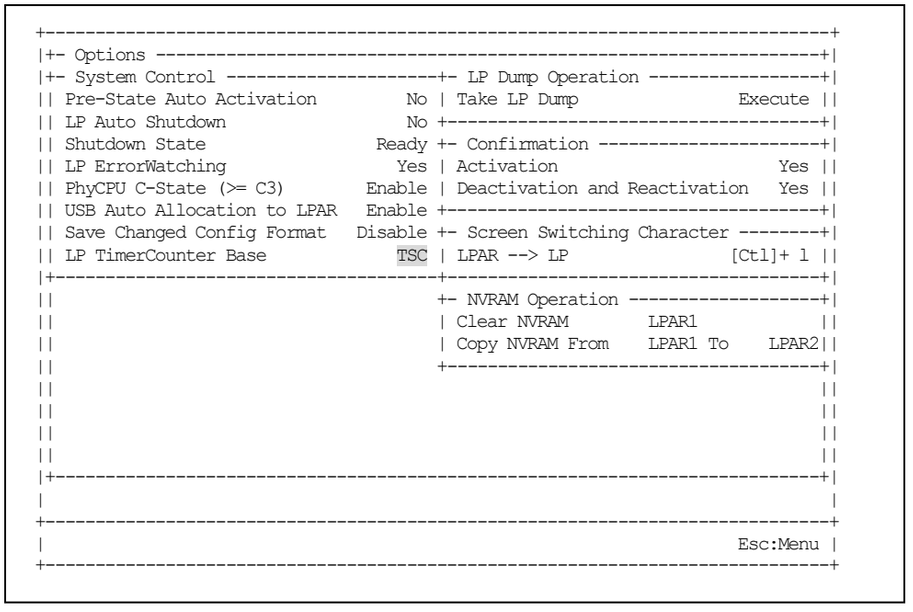
The "LPAR manager dump transfer succeeded” LP system log entry is normally obtained approximately 10 to 20 seconds after the LPAR manager dump collection operation is performed. If you do not get this log entry, press the **Esc** key to display the LPAR manager Menu screen and then redisplay the LP System Logs screen. That is because the LP System Logs screen does not automatically update. If you do not get the two “LPAR manager dump transfer succeeded” LP system log entries after 10 minutes or more, or if you get the “LPAR manager dump transfer failed” log entry, another failure might have occurred. Contact maintenance personnel.

Repeat this operation to obtain multiple LPAR manager dumps.

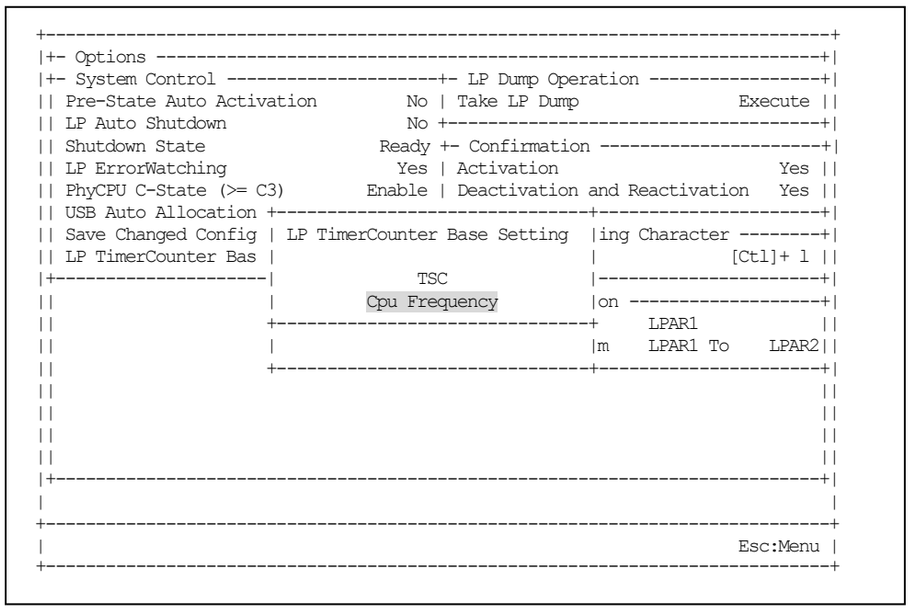
(13) How to change a value to be based for timer counter calculation
LPAR manager firmware version 59-2X/79-2X or later

You need to deactivate all LPARs for changing a value to be based for timer counter calculation.

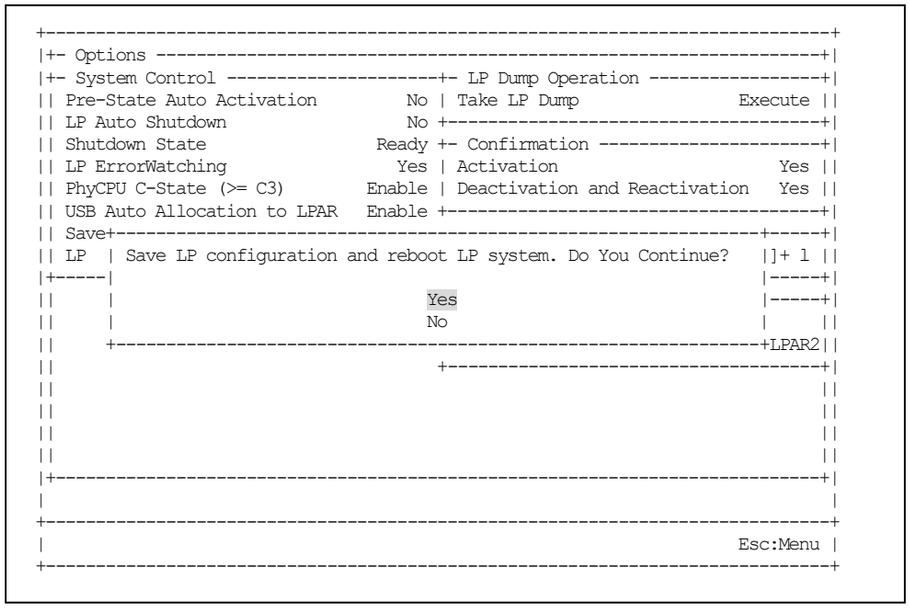
Place the cursor on **LP TimerCounter Base** and press **Enter**.



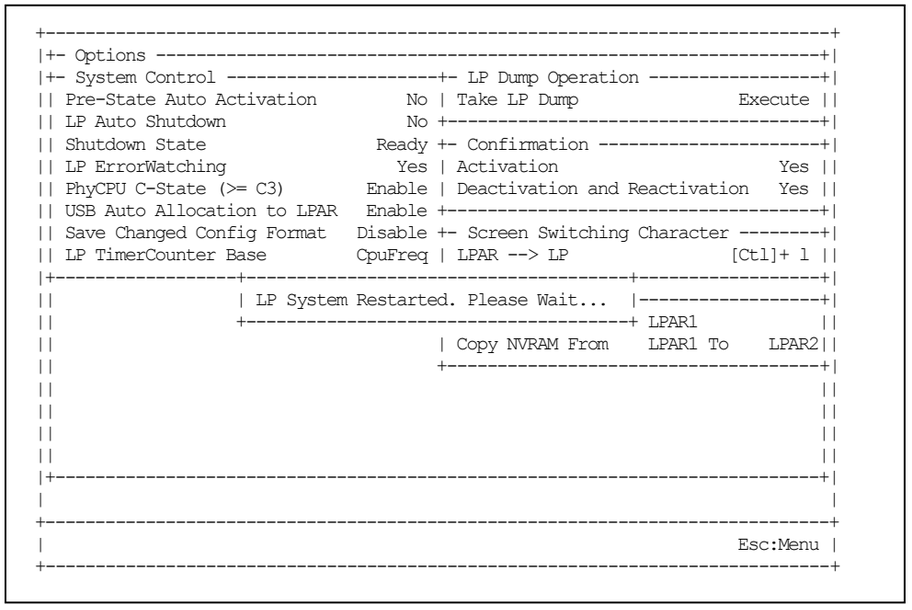
When the subscreen appears, select **TSC/Cpu Frequency** and press **Enter**.



Select TSC or Cpu Frequency to open another subscreen. Select Yes or No and press **Enter**. When Yes is selected, the configuration is saved. When No is selected, saving configuration is cancelled.



When configuration has been completely saved, reboot is executed.

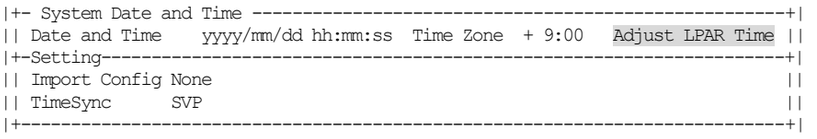


(14) How to change the setting for Save Time Config

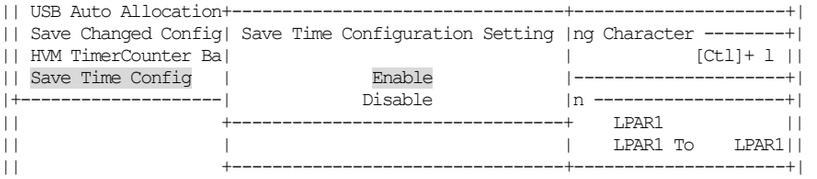
LPAR manager firmware version 59-41/79-41 or later

(a) Using NTP

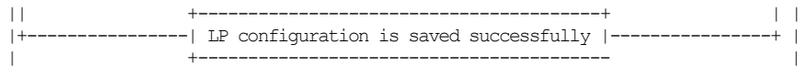
- Check LPAR manager system time on the **Date and Time** screen. If the LPAR manager system time is not synchronized, adjust the LPAR manager system time by restoring the NTP server network state.
- Adjust deactivated LPAR time using Adjust LPAR Time for LPAR System Time, Specified Zone, and UTC, on the Date and Time screen. Check the guest OS timezone, and perform Adjust LPAR Time with the same timezone as the guest OS. For activated LPARs, adjust the time by using the guest OS or NTP time synchronization for the guest OS.



- Enable the **Save Time Config** on the **Options** screen.



- On the **Menu** screen, press **F9: Save Configuration** to save the configuration.



(b) Not using NTP

- Check LPAR manager system time on the **Date and Time** screen. If it is not the expected one, set the LPAR manager system time zone using **F7: Change System Time Zone**.
- Check LPAR manager system time on the **Date and Time** screen. If the LPAR manager system time is not synchronized, adjust the LPAR manager system time by **F6: Change System Date and Tim**e.
- Adjust deactivated LPAR time using Adjust LPAR Time for LPAR System Time, Specified Zone, and UTC, on the **Date and Time** screen. Check the guest OS time zone, and perform Adjust LPAR Time with the same time zone as the guest OS. For activated LPARs, adjust the time by using the guest OS or NTP time synchronization for the guest OS.
- Enable the **Save Time Config** on the **Options** screen.
- Save the configuration on the **Menu** screen using **F9: Save Configuration**.



With LPAR manager firmware version 59-41/79-41 or later, enabling “Save Time Config” is recommended. You can change settings for “Save Time Config” while LPAR manager is running.

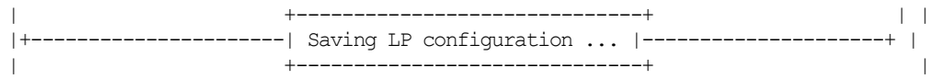
If you reboot LPAR manager after operating it for a long time with “Save Time Config” disabled, or if a system failure in LPAR manager or failover with N+M cold standby unexpectedly occurs, a time lag occurs in the guest OS.



If changing LPAR manager configuration or LPAR configuration with “Save Time Config” enabled, make sure to press the **F9** key at the end of the setting change. Although LPAR manager configuration is saved at time adjustment with “Save Time Config” enabled, the timing cannot be specified.

When LPAR manager configuration is saved at time adjustment, LPAR manager screen appears; system event logs are collected; the alert is notified. Those operations can be prevented by disabling “Save Time Config”.

<LPAR manager screen>



<System event log>

```
|+- LP System Logs ----------------------------------------  All level   --+|
|| Level Date       Time     Event                                         ||
|| Info. yyyy/mm/dd hh:mm:ss HVM saved configuration.                       ||
```

<Alert>

Alert ID: 0x1531

Message: HVM configuration was saved. (RC=6)

❑ LPAR usage

The following functions are available in the LPAR Usage screen.

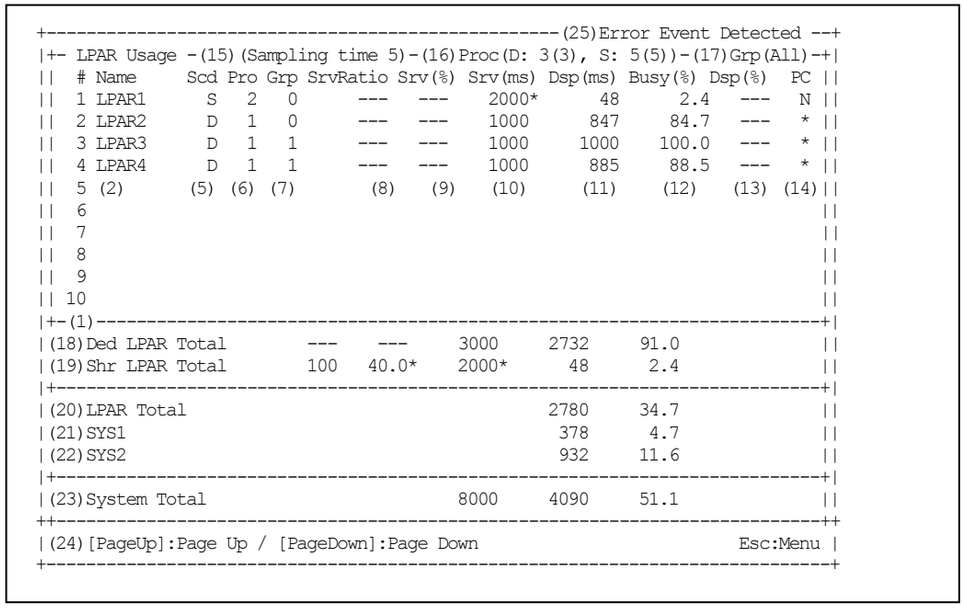
- Displays the service ratio and service time of each LPAR.
- Displays the execution time and busy ratio of each LPAR.
- Displays the number of dedicated/shared processors and the Processor Capping status of each LPAR.
- Displays the LPAR manager system's execution time and busy ratio.
- Changes this screen's refresh interval.

The cursor displayed in this screen might be unstable because the screen refreshes at a rate specified by the Sampling time.

For: Standard server blades with LPAR manager firmware version 58-2X or earlier versions;
High-performance server blades with LPAR manager firmware 78-2X or earlier versions

```
+-------------------------------------------------(25)Error Event Detected --+
|+- LPAR Usage -----(15)(Sampling time 5 )--(16)Proc(D: 3( 3) , S: 5( 5) )----+|
||  # Name     Shr Ded SrvRatio Srv(%)  Srv(ms)  Dsp(ms)  Busy(%)  Dsp(%)  PC ||
||  1 LPAR1      2   -     100   40.0*    2000*      48      2.4     0.9    N ||
||  2 LPAR2      -   1     ---    ---     1000      847     84.7     ---    * ||
||  3 LPAR3      -   1     ---    ---     1000     1000    100.0     ---    * ||
||  4 LPAR4      -   1     ---    ---     1000      885     88.5     ---    * ||
||  5 (2)      (3) (4)     (8)   (9)       (10)     (11)     (12)    (13)  (14)||
||  6                                                                        ||
||  7                                                                        ||
||  8                                                                        ||
||  9                                                                        ||
|| 10                                                                        ||
|+-(1)-------------------------------------------------------------------------+|
|(18)Ded LPAR Total        ---    ---     3000     2732     91.0             ||
|(19)Shr LPAR Total        100   40.0*    2000*      48      2.4             ||
|+-----------------------------------------------------------------------------+|
|(20)LPAR Total                                    2780     34.7             ||
|(21)SYS1                                           378      4.7             ||
|(22)SYS2                                           932     11.6             ||
|+-----------------------------------------------------------------------------+|
|(23)System Total                          8000     4090     51.1             ||
++-----------------------------------------------------------------------------++
|(24)[PageUp]:Page Up / [PageDown]:Page Down                        Esc:Menu |
+-----------------------------------------------------------------------------+
```

For: Standard server blades with LPAR manager firmware version 58-3X or later versions;
High-performance server blades with LPAR manager firmware version 78-3X or later versions



```
+-------------------------------------------------(25)Error Event Detected --+
|+- LPAR Usage -(15)(Sampling time 5)-(16)Proc(D: 3(3), S: 5(5))-(17)Grp(All)-+|
||  # Name     Scd Pro Grp SrvRatio Srv(%) Srv(ms) Dsp(ms) Busy(%) Dsp(%)   PC ||
||  1 LPAR1      S   2   0      ---   ---    2000*      48      2.4   ---    N ||
||  2 LPAR2      D   1   0      ---   ---    1000      847     84.7   ---    * ||
||  3 LPAR3      D   1   1      ---   ---    1000     1000    100.0   ---    * ||
||  4 LPAR4      D   1   1      ---   ---    1000      885     88.5   ---    * ||
||  5 (2)      (5)  (6) (7)       (8)   (9)   (10)     (11)    (12)   (13)  (14)||
||  6                                                                        ||
||  7                                                                        ||
||  8                                                                        ||
||  9                                                                        ||
|| 10                                                                        ||
|+-(1)-------------------------------------------------------------------------+|
|(18)Ded LPAR Total        ---    ---     3000     2732     91.0             ||
|(19)Shr LPAR Total        100   40.0*    2000*      48      2.4             ||
|+-----------------------------------------------------------------------------+|
|(20)LPAR Total                                    2780     34.7             ||
|(21)SYS1                                           378      4.7             ||
|(22)SYS2                                           932     11.6             ||
|+-----------------------------------------------------------------------------+|
|(23)System Total                          8000     4090     51.1             ||
++-----------------------------------------------------------------------------++
|(24)[PageUp]:Page Up / [PageDown]:Page Down                        Esc:Menu |
+-----------------------------------------------------------------------------+
```

The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	#	LPAR number	Displays the LPAR numbers between 1 and 16.	-
(2)	Name	LPAR name	Displays the LPAR name.	NO_NAME
(3)	Shr	Number of shared processors	Displays the number of shared processors when the LPAR is in the shared mode. Displays "-" when the LPAR is in the dedicated mode.	-
(4)	Ded	Number of dedicated processors	Displays the number of dedicated processors when the LPAR is in the dedicated mode. Displays "-" when the LPAR is in the shared mode.	-
(5)	Scd	Scheduling Mode	Displays a scheduling mode. S: Shared mode D: Dedicated mode	-
(6)	Pro	Logical Processors	Displays the number of logical processors.	-
(7)	Grp	Processor Group	Displays a processor group number	-
(8)	SrvRatio	Service Ratio	Displays the service ratio of the LPAR when the LPAR is in the shared mode. The values in the field are set with Service Ratio (Srv) on the LPAR Configuration screen. Grp (ALL): “---“ is displayed Displays "---" when the LPAR is in the dedicated mode. Grp (ALL): “---“ is displayed	---
(9)	Srv(%)	Service Percentage	Displays the proportion of the LPAR's service time to the service time of physical processors running correctly that are assigned to the shared mode LPAR. If the Service Percentage calculated inside LPAR manager does not match, the specified Service Ratio, "*" is displayed on the right side. If it does match, "*" is not displayed. Grp (ALL): “---“ is displayed Displays "---" when the LPAR is in the dedicated mode. Grp (ALL): “---“ is displayed	---
(10)	Srv(ms)	Service time (ms)	Displays the total service time of the LPAR in milliseconds. If the LPAR is in the dedicated mode, this value is obtained by the following formula. Srv(ms) = the number of physical processors running properly on the LPAR x 1000ms If the LPAR is in the shared mode, this value is obtained by the following formula. Srv(ms) = the number of shared physical processors running properly x Srv(%) of the LPAR x 1000ms If the LPAR is in the shared mode and Srv(%) is displayed with "*", "*" will be also displayed in the right side of this field.	---
(11)	Dsp(ms)	Dispatch time (ms)	Displays the execution time of the LPAR in milliseconds. This value is the total execution time of the logical processors on the LPAR.	---
(12)	Busy(%)	LPAR Busy (%)	Displays the busy ratio of the LPAR. This value is the proportion of execution time to the LPAR's service time, and is obtained by the following formula.	---

#	Title	Official Name	Description	Initial Value
			Busy (%) = the LPAR's Dsp(ms) ÷ the LPAR's Srv (ms) x 100 The value of this field is used as the yardstick for resource changes. If this value exceeds 100%, it means that the LPAR has insufficient resources. If Processor Capping becomes enabled, the LPAR Busy ratio is controlled so as not to exceed 100%. Therefore this value cannot be used as a yardstick for changing resources anymore. Note: Even if the processor capping function is on, the LPAR manager allocation rate control allows a tolerance of 1% for each unit of processor-time. A shared mode LPAR is allocated a maximum processor-time that is 1% greater than the total service time of the physical processors assigned to it, and this value might exceed 100%.	
(13)	Dsp(%)	Dispatch Percentage	Displays the proportion of the LPAR's service time to the total service time of all shared mode physical processors when the LPAR is in shared mode. This value is obtained by the following formula. Dsp(%) = the LPAR's run time ÷ service time of all shared physical processors running properly x 100 Grp (ALL): “---“ is displayed Displays "---" when the LPAR is in the dedicated mode. Grp (ALL): “---“ is displayed	---
(14)	PC	Processor Capping	Displays the enabled/disabled status of the Processor Capping function as configured in the LPAR Configuration screen. Y: Processor Capping has been enabled. N: Processor Capping has been disabled. *: The LPAR is in the dedicated mode. -: The LPAR has not been activated.	-
(15)	Sampling time	Sampling time	Sets the refresh rate of the screen in units of seconds. The default setting is 5 seconds, but this can be changed to anything between 1 and 60.	5
(16)	Proc(D: S:)	Number of physical processors	Displays the number of physical processors assigned to the dedicated mode and the shared mode. D: The number of physical processors assigned to the LPAR in the dedicated mode. Format is n or m. n: Total number of physical processors assigned to the LPAR running properly in the dedicated mode m: Total number of all processors assigned to LPAR in the dedicated mode. S: The number of physical processors assigned to the LPAR in the shared mode. Format is n or m. n: Total number of physical processors assigned to the LPAR running properly in the shared mode m: Total number of all processors assigned to LPAR in the shared mode. (S: = total number of physical processors – total number of physical processors assigned to the dedicated mode LPARs)	---

#	Title	Official Name	Description	Initial Value
(17)	Grp	Selecting processor groups to display	Selects processor groups to display. All: Displays the entire system The number of a processor group: Displays specified processor groups Note: When a processor group number is specified, information on the group is displayed.	All
(18)	Ded LPAR Total	Dedicated LPAR Total	Displays various totals of LPARs in the dedicated mode.	---
			"---" is displayed for SrvRatio and Srv(%).	
			Srv(ms) displays the total service time of LPARs in the dedicated mode.	
			Dsp(ms) displays the total execution time of LPARs in dedicated mode.	
			Busy(%) displays the busy ratio of all LPARs in the dedicated mode. this value is obtained by the following formula. Busy(%) = All execution time of LPARs in the dedicated mode ÷ All service time of LPARs in the dedicated mode x 100	
(19)	Shr LPAR Total	Shared LPAR Total	Displays various totals of LPARs in the shared mode.	---
			SrvRatio displays SrvRatio totals of LPARs in the shared mode.	
			Srv(%) displays Srv(%) total value of LPARs in the shared mode. If the displayed values include Srv(ms) with '*' in LPARs in the shared mode, this value has '*'.	
			Srv(ms) displays the total service time of LPARs in shared mode. when SRV(%) with * is included, * is displayed in that value.	
			Dsp(ms) displays the total execution time of LPARs in shared mode.	
			Busy(%) displays the busy ratio of all LPARs in the shared mode. This value is obtained by the following formula. Busy(%) = the total execution time of all LPARs in the shared mode ÷ Service time of all LPARs in the dedicated mode x 100	
(20)	LPAR Total	LPAR Total	Displays various totals of all LPARs.	---
			Dsp(ms) displays the total execution time of LPARs.	
			Busy (%) displays the total busy ratio value of all LPARs. Busy (%) = total execution time of all LPARs ÷ system service time x 100	
(21)	SYS1	SYS1	Displays the execution time and the busy ratio of the LPAR manager System1. LPAR manager System1 refers to the processing by the kernel of the LPAR manager. Note: The busy ratio and execution time of the faulty processor isolated are contained in SYS1.	---
			Dsp(ms) displays the execution time of the LPAR manager System1.	
			Busy(%) displays the busy ratio of the LPAR manager System1. This value is obtained by the following formula. Busy(%) = execution time of the LPAR manager System1 ÷ system service time x 100	

#	Title	Official Name	Description	Initial Value
(22)	SYS2	SYS2	Displays the execution time and the busy ratio of the LPAR manager System2. LPAR manager System2 refers to the processes for the LPAR manager's communication and service control.	---
			Dsp(ms) displays the execution time of the LPAR manager System2.	
			Busy(%) displays the busy ratio of the LPAR manager System2. This value is obtained by the following formula. Busy(%) = execution time of the LPAR manager System2 ÷ system service time x 100	
(23)	System Total	System Total	Displays the system service time, the system busy time, and the system busy ratio of the LPAR manager system.	---
			Srv(ms) displays the system service time. This value is the total service time that the physical processors running properly have in the LPAR manager system, and is obtained by the following formula. Srv(ms) = the number of physical processors running properly x 1000ms	
			Dsp(ms) displays the system busy time. The system busy time is the sum of the execution time of all LPARs, SYS1, and SYS2.	
			Busy(%) displays the system busy ratio. This value is the total busy ratio in the LPAR manager system and is obtained by the following formula. Busy(%) = system busy time ÷ system service time x 100	
(24)	PageUp / PageDown	Page Up / Page Down	Page Up: scrolls the LPAR Usage frame upwards. Page Down: scrolls the LPAR Usage frame downwards.	-
(25)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

(1) How to change Sampling time

Display the **LPAR Usage** screen.

Since the cursor is already placed on the **Sampling** time, just press **Enter** to display a subscreen. Enter the new number on the subscreen, and press **Enter**.

The entered number will be set as the Sampling time in units of seconds. You can set any number between 1 and 60.

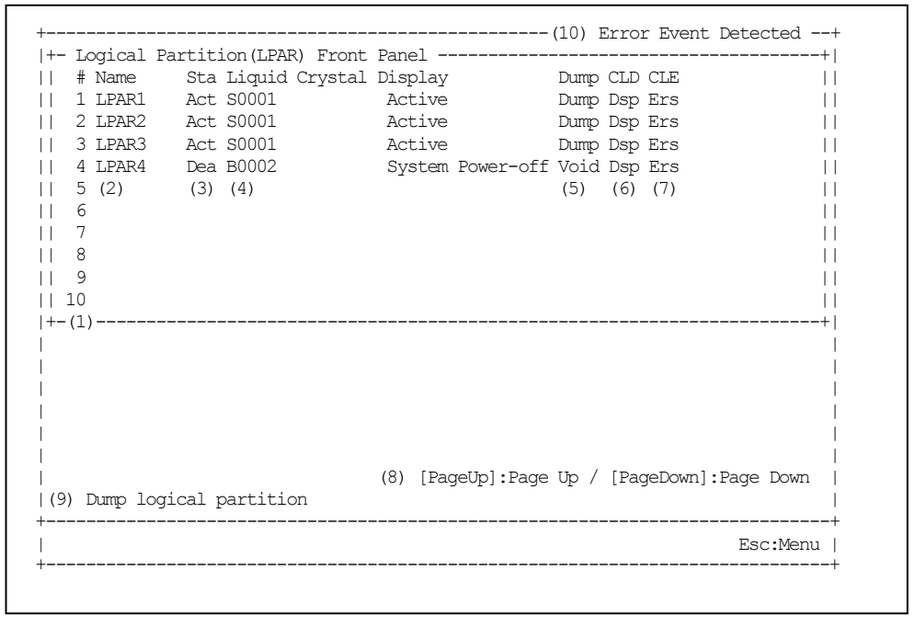
(2) How to display specified processor groups

Display the **LPAR Usage** screen. Place the cursor on **Grp** on the upper right, and press **Enter** to display a subscreen. Select the number of a processor group shown on the subscreen, and press **Enter**.

❑ Front panel

The following actions are possible in the Front Panel screen.

- Displays LPAR system status.
- Collects LPAR dump.
- Displays and deletes LPAR guest screen data (Console Log Data).



The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	#	LPAR number	Displays LPAR numbers.	-
(2)	Name	LPAR name	Displays the LPAR name.	NO_NAME
(3)	Sta	Status	Displays the LPAR power status. Act (Activate): The LPAR is powered on. Dea (Deactivate):The LPAR is powered off. Fai (Failure): The LPAR cannot be used due to an unrecoverable failure. Reboot the system when this happens.	Dea
(4)	Liquid Crystal Display	Liquid crystal	Displays the LPAR's system status and error information. Active: The power is on. System power-off: The power is off. Ignite dump: A state when a dump is collected MigrationFailed: LPAR migration fails, which requires LPAR recovery.	-
(5)	Dump	Dump	Commands a guest OS to collect dump. This can be used only when the LPAR is activated.	Void / Dump
(6)	CLD	Console Log Display	Displays the selected LPAR's guest screen data (console log data).	Dsp
(7)	CLE	Console Log Erase	Deletes the selected LPAR's guest screen data (console log data) from the buffer in LPAR manager.	Ers
(8)	PageUp / PageDown key	Page Up / Page Down	Page Up: scrolls the Front Panel frame upwards. Page Down: scrolls the Front Panel frame downwards.	-
(9)	Comment	Comments	Displays a brief description of the selected item.	-
(10)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

#	Title	Guest status			Remarks
		Activated	Deactivated	Failure	
(1)	#	-	-	-	Display only
(2)	Name	-	-	-	Display only
(3)	Sta	-	-	-	Display only
(4)	Liquid Crystal Display	-	-	-	Display only
(5)	Dump	✓	-	-	
(6)	CLD	✓	✓	✓	
(7)	CLE	✓	✓	✓	
(8)	PageUp / PageDown	-	-	-	Display only
(9)	Comment	-	-	-	Display only

✓: can be executed. -: cannot be executed.

(1) How to check LPAR system status

Display the **Front Panel** screen.

Check the remark displayed in the **Liquid Crystal Display** column in the LPAR row whose system status you want to check.

(2) How to collect guest OS dump

Display the **Front Panel** screen.

Place the cursor on the **Dump** column in the LPAR row whose dump you want to collect. Press **Enter** to display the subscreen to execute a dump. Place the cursor on **Yes** and press **Enter**. A subscreen that re-confirms the dump execution will be displayed. Place the cursor on **Yes** again and press **Enter**.

Dump collection is possible only when the relevant LPAR is activated.

With this operation, an INIT interrupt is issued to the LPAR for the IPF version LPAR manager and NMI is issued to the LPAR for the Xeon version LPAR manager to obtain the memory dump of the guest OS.

You could not be too careful when collecting dumps because that collecting dumps might damage the guest OS.

(3) What is Console log data?

Console log data is the screen data displayed when the guest OS on a LPAR is running. LPAR manager stores character data among the screen data in the internal buffer (up to 1,500 lines). If the console log data exceeds the number of lines in the buffer, it is overwritten sequentially from the oldest data.

(4) How to collect console log data

Display the **Front Panel** screen.

Place the cursor on the **CLD** column in the LPAR row whose console log data you would like to display. Press **Enter** to open a subscreen. Use the arrow keys ([↑] or [↓]) to select **Yes** on the subscreen, and press **Enter**.

It will take two to three minutes for the log to be completely displayed on the terminal screen. During the period, you will be unable to perform operations on LPAR manager.

With displaying console log data on the screen by this operation, you can collect and/or view the complete guest screen data as the Tera Term scroll buffer data.

If the LPAR's guest screen is updated while the console log is being displayed, such new content might not be included in the console log.

(5) How to delete console log data

Display the **Front Panel** screen. Place the cursor on the **CLE** column in the LPAR row whose console log data you want to delete. Press **Enter** to display a subscreen. Use the arrow keys ([↑] or [↓]) to select **Yes** on the subscreen and press **Enter**.

This will delete the LPAR's console log data from the buffer in LPAR manager.

(6) How to recover migration failed LPAR

Recover an LPAR with Migration Failed, if any. For the recovery procedure, see *HVM Navigator User's Guide Migration Functions*.

❑ LP system logs

The following functions are available in the LP System Logs screen.

- Changes the level of the LP system log to be displayed.
- Displays the details of the collected LP system log.

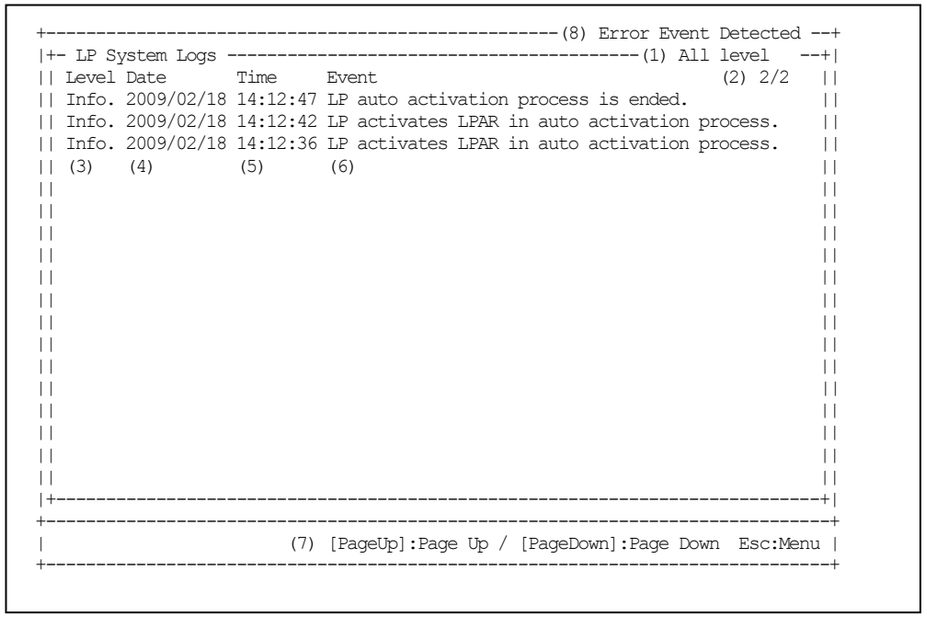
There are three levels of LP system logs as shown in the table below. The levels are Information, Warning, and Error, in rising order of threat level.

LPAR manager stores the latest 256 LP system logs. If the number of LP system logs exceeds 256, logs are overwritten in sequence, starting at the oldest log.

To display the detailed information, place the cursor on the LP system log and press **Enter**.

Levels of LP system logs

#	Level	Description	Action
1	Error	An LPAR manager system error occurred	See the action in LPAR manager system logs screen messages.
2	Warning	This is not an error, but you should pay attention to it.	
3	Information	This event does not apply to the above levels.	



The following table describes each item on this screen.

#	Title	Official Name	Description	Initial Value
(1)	Select Level	Level selection	Specifies the level of the LP system log to display. The initial setting is for all levels (All level) to be displayed. Error: displays error level problems. If you select this item, "Error only" will be displayed. Error/Warn: Displays warnings and more serious problems. If you select this item, "Over warning" will be displayed. Error/Warn/Info: displays all logs. If you select this item, "All level" will be displayed.	All level
(2)	Pages	Page	Displays the system log page information. Numerator: Displays the page number of the system log currently displayed. Denominator: Displays the total number of pages of the system logs. This item is displayed when the system log of two pages or more is retained.	-
(3)	Level	Level	Displays the level of the LP system log. Error: Indicates an error. Warn: Indicates a warning. Info.: Indicates information.	-
(4)	Date	Date	Displays the date when the LP system log was collected.	-
(5)	Time	Time	Displays the time when the LP system log was collected.	-
(6)	Event	Event	Displays the event of the LP system log.	-
(7)	PageUp / PageDown	PageUp / PageDown	Page Up: Scrolls a page up for the screen display. Page Down: Scrolls a page down for the screen display. This item is displayed when the system log of two pages or more is retained.	-
(8)	Error event detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.	-

(1) How to check the details of an event occurred in LPAR manager

Display the **LP System Logs** screen.

Place the cursor on **Select Level** in the upper-right hand and press **Enter** to display a subscreen for selecting an LP system log level. Place the cursor on the level of the LP system log to display and press **Enter**. To display the details of the relevant LP system log, place the cursor on the title of the LP system log to check and press **Enter**.

If the LP system log cannot be included in one page, scroll up or down using the Page Up or Page Down keys.

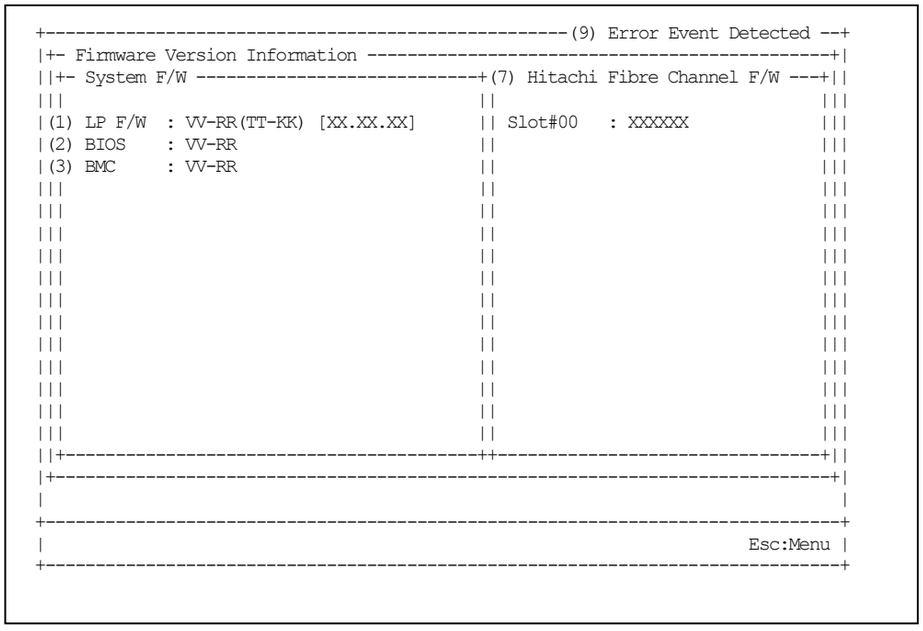
To analysis faults, we might check the messages displayed on the LP System Logs screen.

❑ Firmware version information

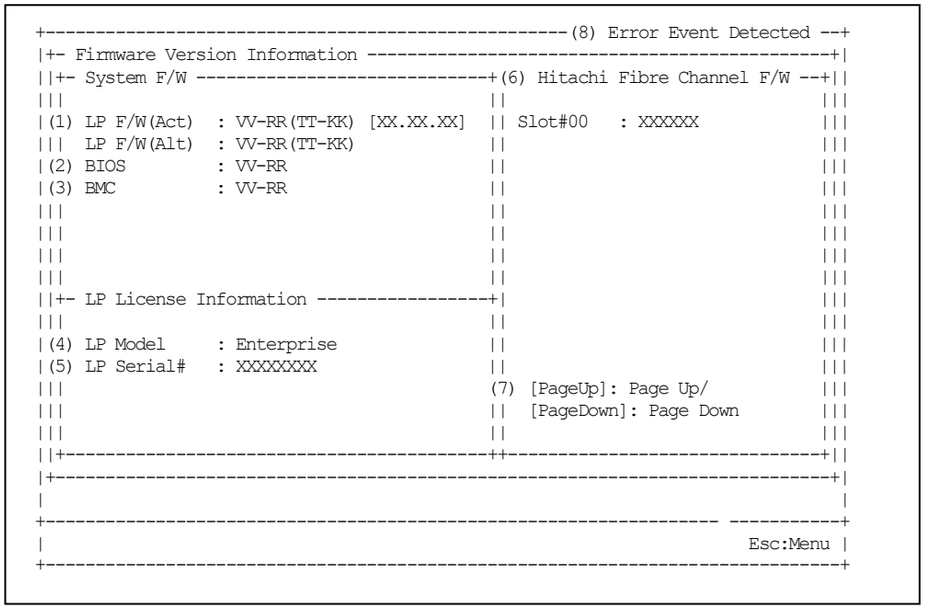
The following functions are available on the Firmware Version Information screen.

- Display the firmware version of each component.

LPAR manager firmware version 57-0X



LPAR manager firmware 57-10 or later versions

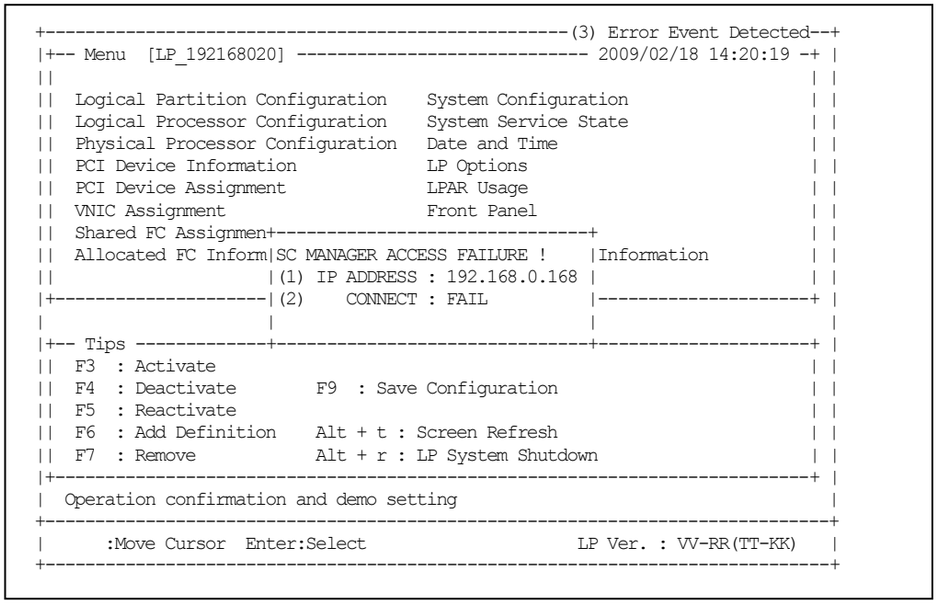


The following table describes each item on this screen.

#	Title	Official Name	Description
(1)	LPAR manager	LPAR manager Firmware Version	Displays the LPAR manager firmware version and LPAR manager firmware internal version.
(2)	BIOS	BIOS Firmware Version	Displays the BIOS firmware version.
(3)	BMC	BMC Firmware Version	Displays the BMC firmware version.
(4)	LP Model	LP Model	Displays the LP model. Essential: Essential model Enterprise: Enterprise model
(5)	LP Serial#	LP Serial Number	Displays the LP serial number.
(6)	Hitachi Fibre-channel F/W	Hitachi Fibre-channel Firmware Version	Displays the FC adapter firmware version of the slot number.
(7)	PageUp/ PageDown	Page Up/ Page Down	PageUp: Scrolls a page upward to show a screen. PageDown:Scrolls a page downward to show a screen.
(8)	Error Event Detected	Error event detection	Displays that LP system logs at the error level are detected. When this is displayed, check the LP system log in the LP System Logs screen. See LP system logs for checking LP system logs. To delete this display, press the Esc key with this screen or open the system logs screen.

❑ ServerConductor/Blade Server Manager access failure notification

Display the following subscreen if the connection with ServerConductor/Blade Server Manager is lost.

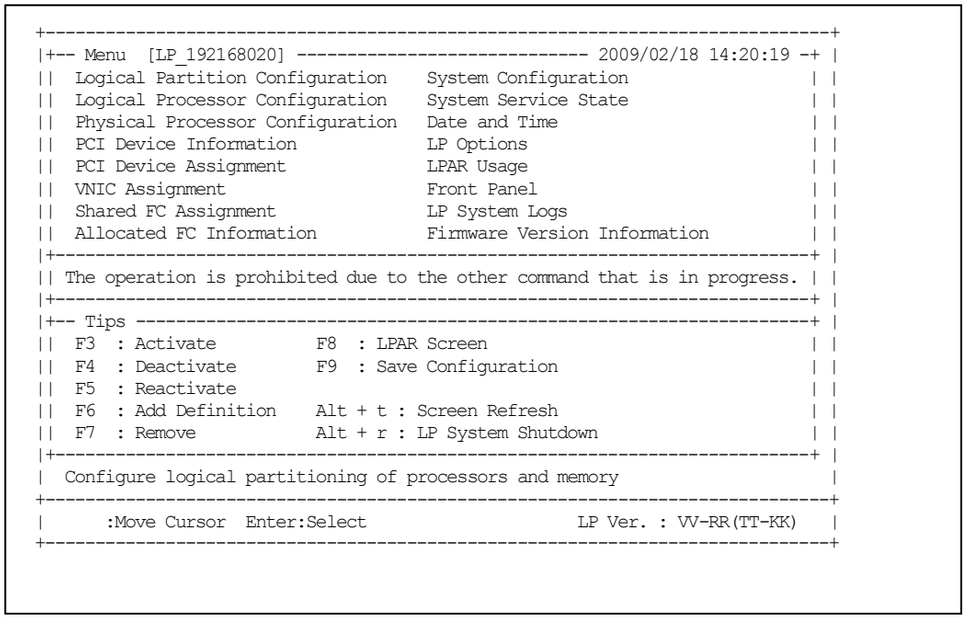


The following table describes each item on this screen.

#	Title	Official Name	Description
(1)	IP Address	ServerConductor/Blade Server Manager IP Address	Displays the IP address of the ServerConductor/Blade Server Manager to which connection failed.
(2)	CONNECT	Connection status	Displays the status of the connection with the ServerConductor/Blade Server Manager. SUCCEED: The ServerConductor/Blade Server Manager connection established FAIL: The ServerConductor/Blade Server Manager connection failed
(3)	Error Event Detected	Error Event Detected	Detected an LP system log at the error level. When this is displayed, check the LP system log on the LP system logs screen referring to LPAR manager system logs screen messages. To delete this message, press the Esc key on the LPAR manager menu screen or open the LP system logs screen.

❑ Notifying that requests from an external management console are being processed

The subscreen shown below appears while the LPAR manager is processing requests sent from an external management console such as ServerConductor/Blade Server Manager. Therefore, no operation is possible on the LPAR manager screen. This subscreen automatically closes when the LPAR manager completes the processing of the requests.

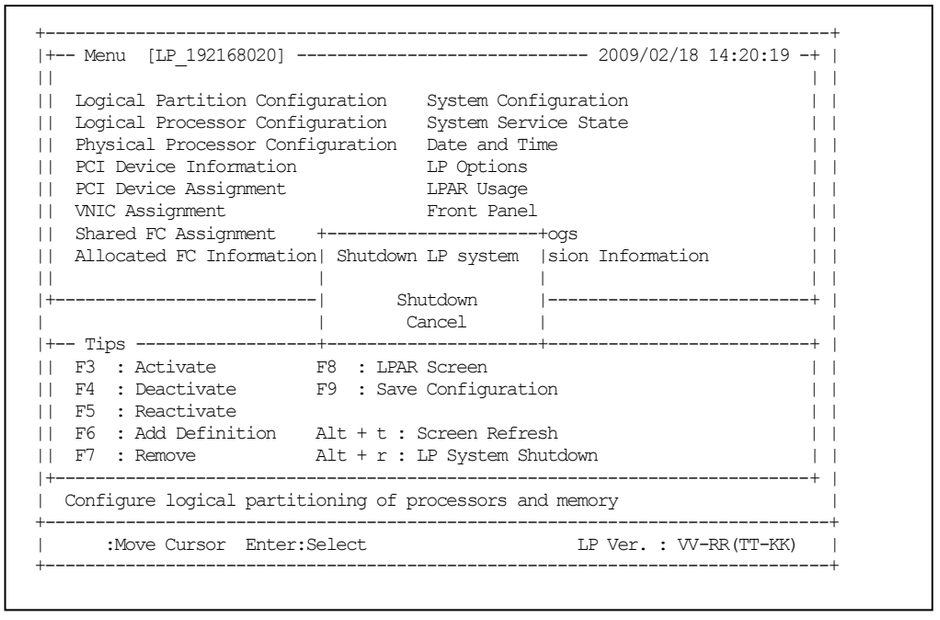


Quit LPAR manager

Shutting down the LPAR manager system

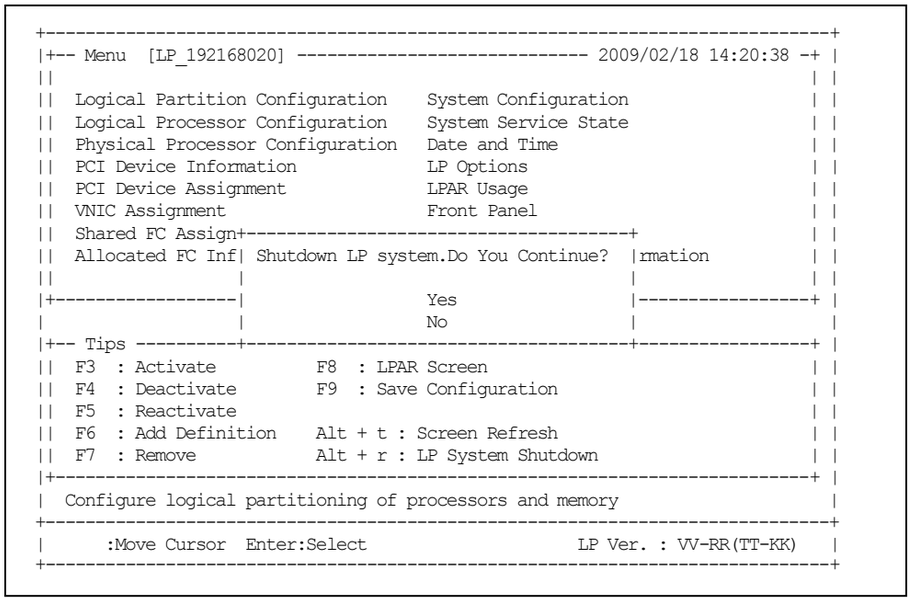
1 Deactivate all LPARs. For details on deactivating LPARs, see Shutdown guest OS and deactivate LPAR.

2 Press **Alt + r** on any screen.

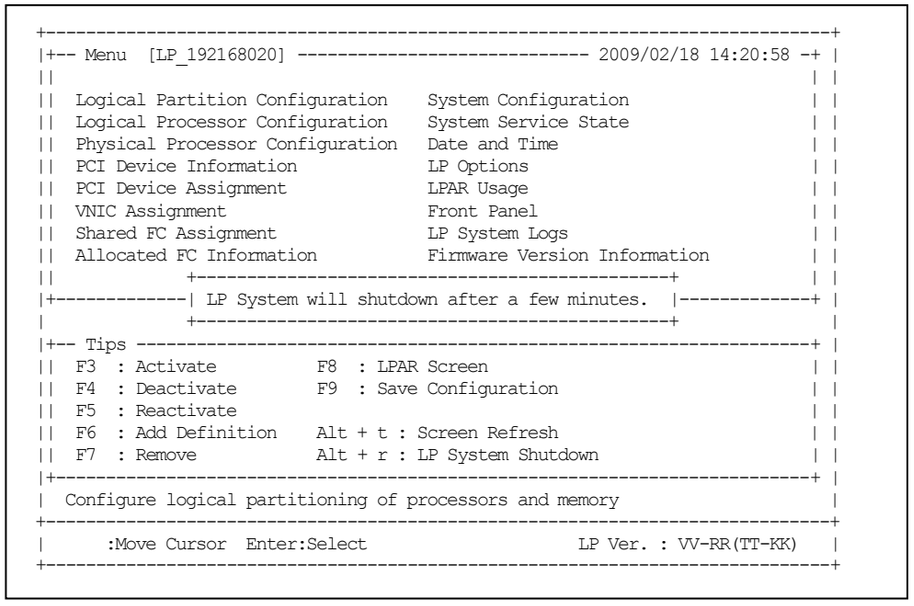


3 Select **Shutdown** on the subscreen and press **Enter**.

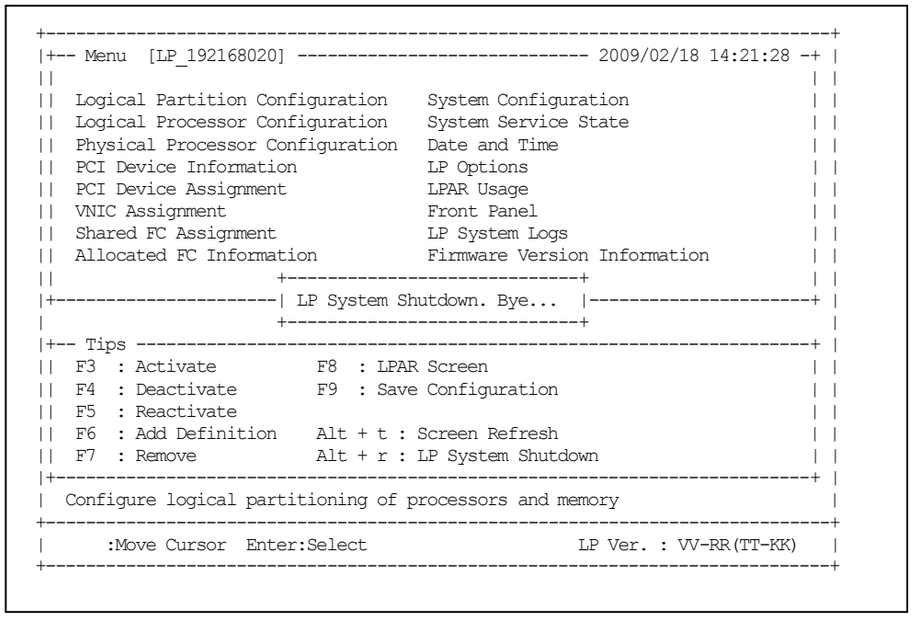
4 A subscreen will appear to confirm the shutdown of the LPAR manager system. Select **Yes** and press **Enter**.



5 A subscreen will appear, indicating that the LPAR manager system is shutting down. It will take a couple of minutes before the power supply for the server blade is shut off. Once the LPAR manager shutdown has begun, no operation on the LPAR manager screens is available.



6 A subscreen appears saying that the LP system shutdown is complete, and the power supply of the server blade shuts off.



Tip

- If LP Auto Shutdown is enabled, the LPAR manager system will automatically shut down once all the LPARs have been deactivated.
- It is also possible to shut down the LPAR manager system using ServerConductor/Blade Server Manager. For details, see the manuals for ServerConductor/Blade Server Manager.
- To shut down the LPAR manager system using the power control schedule of ServerConductor/Blade Server Manager, install ServerConductor/Advanced Agent to all the LPARs.

LPAR manager functions

Virtual NIC functions

❑ Overview of virtual NIC functions

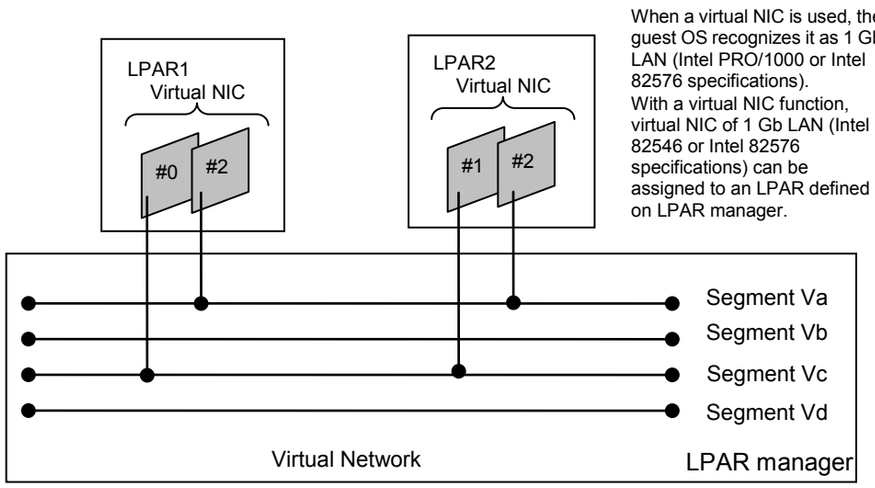
A virtual NIC function provides a virtual network interface card that can be used instead of a physical NIC. Virtual NICs offer the following two functions:

A virtual NIC provides functions equivalent to a physical LAN controller, but perfect interchangeability is not guaranteed. Note that a virtual NIC differs from a physical LAN controller in specifications and operation.

(1) Virtual NIC

With LPAR manager, up to four network segments can be set for virtual NICs. By defining connections between these network segments and virtual NICs, you can perform the Inter-LPAR Communication without using physical NICs. Network segments can be set on the Virtual NIC (VNIC) Assignment screen. The identifiers for the network segments to be defined are Va, Vb, Vc, and Vd.

Virtual NICs in the same network segment can communicate with each other, but virtual NICs in different network segments cannot communicate with each other.



Virtual NIC #0 of LPAR1 is assigned to segment Vc in the figure above. It can communicate with virtual NIC #1 of LPAR2 but cannot communicate with #2. Virtual NIC #2 of LPAR2 can communicate only with virtual NIC #2 of LPAR1 in the same segment Va.

(2) Shared NIC

With LPAR manager, network segments for shared NICs can be set to the physical LAN controller assigned to shared mode. By defining connections between these network segments and the shared NICs, you can perform communication with external networks. Network segments for shared NICs can be set on the Virtual NIC (VNIC) Assignment screen.

In these network segments, shared NICs connected to the same network segment can communicate without going through a physical LAN controller. However, communication among shared NICs in different network segments needs to use an external network via a physical LAN controller.

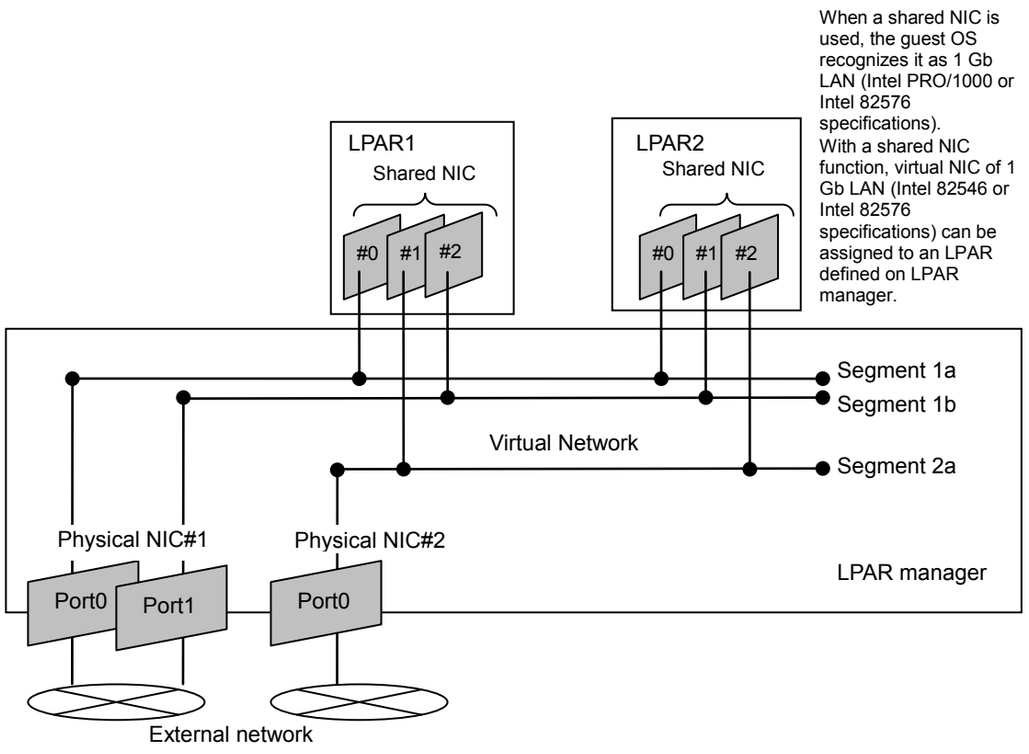
The following table shows the number of physical LAN controllers to be assigned to LPAR manager.

Item	LPAR manager firmware version	
	57-1X or later/ 78-1X or later	59-0X or later/ 79-0X or later
Max number of physical LAN controllers to be assigned to LPAR manager	6	8

The following table shows combinations of shared NIC numbers and network segment identifiers as examples.

Shared NIC No.	Port No.	Network Segment Identifier
1	0	1a
	1	1b
~		
8	0	8a
	1	8b

In the following figure, an external network should be used to establish communication between shared NIC #0 of LPAR1 assigned to segment 1a and shared NIC #1 of LPAR2 assigned to segment 1b or shared NIC #2 of LPAR2 assigned to segment 2a.



(3) VF NIC

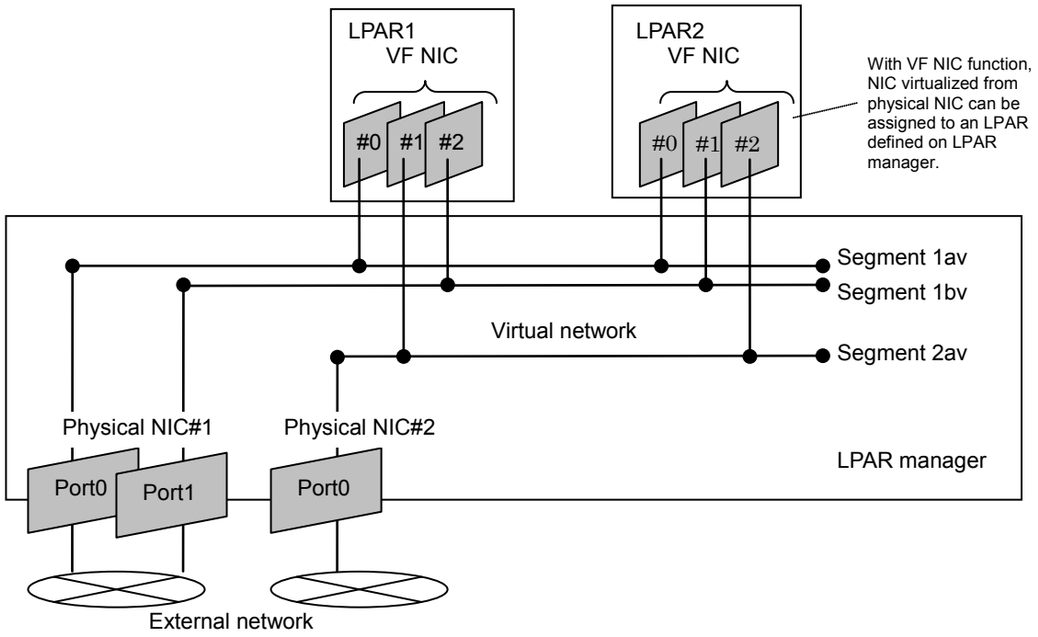
With LPAR manager, you can enable SR-IOV function of physical NICs and set a network segment for VF NIC to a physical LAN controller in shared mode. Defining connection between the network segment and VF NIC allows communication with external networks. Network segments can be set on the Virtual NIC (VNIC) assignment screen.

Communication is available between VF NICs connected to the same network segment without using external network. VF NICs connected to different network segments require an external network for communication.

Up to two physical LAN controllers can be assigned to LPAR manager.

The following table describes relation between the number of Shared NICs and network segment identifiers.

Shared NIC number	Port number	Network segment identifier
1	0	1av
	1	1bv
.....		
2	0	2av
	1	2bv



In the figure above, communication between Shared NIC #0 of LPAR1 assigned to Segment 1av and Shared NIC #1 of LPAR2 assigned to Segment 1bv or Shared NIC #2 of LPAR2 assigned to Segment 2av requires external networks.

❑ Using Virtual NIC Functions

- Virtual NIC/Shared NIC
  - Setting Shared mode

    On PCI device assignment screen for LPAR manager, set NIC scheduling mode to Shared mode. See PCI device assignment for details.
  - Assigning NIC

    On Virtual NIC (VNIC) assignment screen for LPAR manager, set the following items. See Virtual NIC (VNIC) assignment for details.

    - VNIC Device Type

    - Shared NIC such as 1a or Virtual NIC such as Va

    - VLAN
  - Installing LAN driver

    See *Hitachi Compute Blade 2000 SOFTWARE GUIDE* and *Server installation and monitoring tool OS Setup Guide* for details.
  - Setting checksum offload

    See *Hitachi Compute Blade 2000 SOFTWARE GUIDE* and *Server installation and monitoring tool OS Setup Guide* for details.
- VF NIC
  - Updating NIC firmware

    If your NIC firmware does not support SR-IOV, update it to the one that supports SR-IOV. Contact your reseller for details.



In LPAR manager mode, you cannot update NIC firmware.
Change to Basic mode before updating NIC firmware.

  - Setting SR-IOV

    See *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware* for details.
  - Setting LPAR manager expansion mode

    On System Configuration screen for LPAR manager, set the LPAR manager operating mode to LPAR manager expansion mode. See System configuration for details.
  - Setting Shared mode

    On PCI device assignment screen for LPAR manager, set the NIC scheduling mode to Shared mode. See PCI device assignment for details.
  - Assigning NIC

    On Virtual NIC (VNIC) assignment screen for LPAR manager, set the following items. See Virtual NIC (VNIC) assignment for details.

    - VF NIC such as 1av

    - VLAN

    - Transmission bandwidth limitation
  - Updating NIC driver

    If your NIC driver does not support SR-IOV, update it to the one that supports SR-IOV. See *Hitachi Compute Blade Emulex Adapter User's Guide for Driver* for details.

- Setting checksum offload

  See *Hitachi Compute Blade 2000 SOFTWARE GUIDE* and *Server installation and monitoring tool OS Setup Guide* for details.

❑ Assignment order for physical NIC and shared NIC

The following table describes the relation between physical NICs and external ports, and the order in which LPAR manager detects them and assigns a number to them.

Installed Slot/Port		External connection port	# Assigned to Shared NIC
On Board	Port0	LAN switch module port of the switch module slot0	1
	Port1	LAN switch module port of the switch module slot1	
PCI Slot0	Port0	Port0 of the PCI NIC0	4
	Port1	Port1 of the PCI NIC0	
	Port2	Port2 of the PCI NIC0	5
	Port3	Port3 of the PCI NIC0	
PCI Slot1	Port0	Port0 of the PCI NIC1	2
	Port1	Port1 of the PCI NIC1	
	Port2	Port2 of the PCI NIC1	3
	Port3	Port3 of the PCI NIC1	
Expansion Slot0	Port0	LAN switch module port of the switch module slot 2	6
	Port1	LAN switch module port of the switch module slot 3	
	Port2	LAN switch module port of the switch module slot 2	7
	Port3	LAN switch module port of the switch module slot 3	
Expansion Slot1	Port0	LAN switch module port of the switch module slot 4	8
	Port1	LAN switch module port of the switch module slot 5	
	Port2	LAN switch module port of the switch module slot 4	9
	Port3	LAN switch module port of the switch module slot 5	

The following table shows an example of the relation between physical NIC, the shared NIC number and Network segment identifier.

A shared NIC number is assigned to the shared NIC as the same numerical order as the NIC assigned by LPAR manager shown in the table above, which decides the segment identifier.

Installed location Slot/(Port)		NIC installation status (ex.1)			NIC installation status (ex.2)		
		Installed or not	Shared NIC #	Segment identifier	Installed or not	Shared NIC #	Segment identifier
On Board	Port0	Installed (Shared)	1	1a	Installed (shared)	1	1a
	Port1			1b			1b
PCI Slot0	Port0	installed （Shared）	2	2a	Installed (shared)	4	4a
	Port1			2b			4b
	Port2		3	3a		5	5a
	Port3			3b			5b
PCI Slot1	Port0	Not installed	-	-	Installed (Shared)	2	2a
	Port1			-			2b
	Port2		-	-		3	3a
	Port3			-			3b
Expansion Slot0	Port0	Installed (Dedicated)	-	-	Not installed	-	-
	Port1			-			-
	Port2		-	-		-	-
	Port3			-			-
Expansion Slot1	Port0	Installed (Shared)	4	4a	Not Installed	-	-
	Port1			4b			-
	Port2		5	5a		-	-
	Port3			5b			-

❑ Virtual NIC Function Specifications

(1) MAC addresses

Virtual NIC system number: 0 to 128 with LPAR manager standard mode

The MAC addresses are provided in the following format. These MAC addresses are automatically generated by LPAR manager.

MAC address format: XX.XX.XX.YY.YY.ZZ

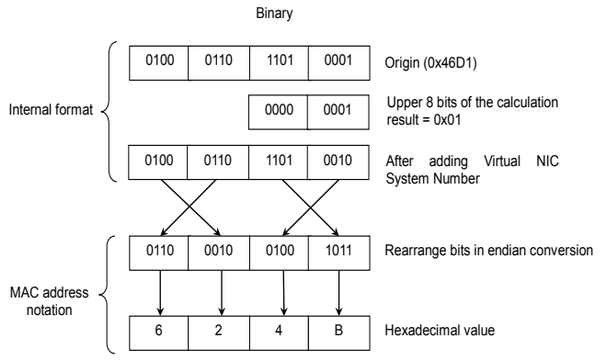
Calculate the offset value from the base point with the following to generate a MAC address.

1. LPAR 1 to 32 (0x0100 to 0x80FF)
   Virtual NIC system number x 256 + (LPAR number – 1) x 8 + virtual NIC number
2. LPAR 33 to 60 (0x8100 to 0xF0FF)
   0x8100 + (Virtual NIC system number – 1) x 224 + (LPAR number – 33) x 8 + Virtual NIC number

Value	Automatically generated by LPAR manager*1	User specified*2
XX.XX.XX (Vendor ID)	Fixed at 00.00.87 to indicate Hitachi	Between 00.00.00 and FF.FF.FF
YY.YY	Eight higher order bits of the offset value is taken out and added to 0x46D1. Then endian conversion is performed.	Between 00.00 and FF.FF Excluding the range generated by LPAR manager
ZZ	Eight lower order bits of the offset value	Between 00 and FF

*1: The MAC address format above is not applied to LPARs that have performed migration,

*2: The user cannot set a value that duplicates the MAC address automatically generated by LPAR manager. Do not set a multicast address and broad cast address.



Upper 8 bits	YY.YY value
1	62.4B
2	62.CB
3	62.2B
4	62.AB
|	|
45	62.7F
46	62.FF
47	E2.00
48	E2.80
|	|
127	E2.0A
128	E2.8A
|	|
247	E2.13

Virtual NIC system number: 0 to 128 with LPAR manager expansion mode

With LPAR manager expansion mode, up to 16 virtual NICs can be assigned to one LPAR. MAC addresses used by the system with Virtual NIC number 0 to 7, are identical to those with LPAR manager standard mode. MAC addresses used by the system with Virtual NIC number 8 to 15 are provided in the following string format. Those MAC addresses are automatically generated by LPAR manager.

MAC address format: XX.XX.XX.YY.YY.ZZ

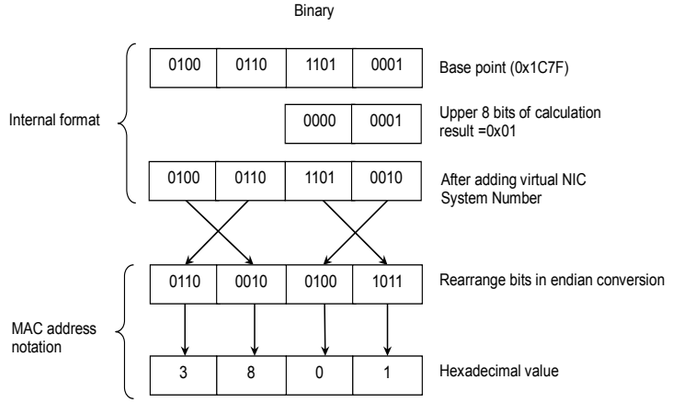
Calculate the offset value from the base point with the followings to generate a MAC address.

1. LPAR 1 to 32 (0x0100 to 0x80FF)
   Virtual NIC system number x 256 + (LPAR number – 1) x 8 + (Virtual NIC number – 8)
2. LPAR 33 to 60 (0x8100 to 0xF0FF)
   0x8100 + (Virtual NIC system number – 1) x 224 + (LPAR number – 33) x 8 + (Virtual NIC number – 8)

Value	Automatically generated by LPAR manager*1	User specified*2
XX.XX.XX (Vendor ID)	Fixed at 00.00.87 to indicate Hitachi	Between 00.00.00 and FF.FF.FF
YY.YY	Eight higher order bits of the offset value is taken out and added to 0x1C7F. Then endian conversion is performed.	Between 00.00 and FF.FF Excluding the range generated by LPAR manager
ZZ	Eight lower order bits of the offset value	Between 00 and FF

*1: The MAC address format above is not applied to LPARs that have performed migration,

*2: The user cannot set a value that duplicates the MAC address automatically generated by LPAR manager. Do not set a multicast address and broad cast address.



Upper 8 bits	YY.YY value
1	38.01
2	38.81
3	38.41
4	38.C1
~	~
45	38.35
46	38.B5
47	38.75
48	38.F5
~	~
127	38.7F
128	38.FF
~	~
247	B8.6E

Virtual NIC system number: 129 or greater with LPAR manager standard mode/expansion mode

MAC address is provided in the following format in the system with Virtual NIC number 129 or greater. MAC address is automatically created by LPAR manager.

MAC address format: XX.XX.XX.YY.YY.ZZ

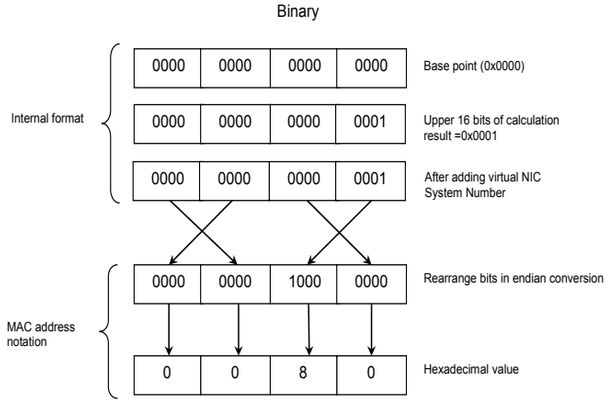
Calculate the offset value from the base point with the followings to generate a MAC address.

1. LPAR 1 to 16
   (Virtual NIC system number - 129) x 1024 + (LPAR number – 1) x 16 + Virtual NIC number
2. LPAR 17 to 32
   (Virtual NIC system number - 129) x 1024 + 256 + (LPAR number – 17) x 16 + Virtual NIC number
3. LPAR 33 to 48
   (Virtual NIC system number - 129) x 1024 + 512 + (LPAR number – 33) x 16 + Virtual NIC number
4. LPAR 49 to 60
   (Virtual NIC system number - 129) x 1024 + 768 + (LPAR number – 49) x 16 + Virtual NIC number

Value	automatically created by LPAR manager *1	Specified by the user*2
XX.XX.XX (vendor ID)	F8:48:97 Fixed value for Hitachi, Ltd.	00.00.00 to FF.FF.FF
YY.YY	Value as a result that higher-order 16 bits of the offset value is taken out, 0x0000 is added to it, and endian conversion is performed.	00.00 to FF.FF Except the range for automatically created by LPAR manager
ZZ	8 lower-order bits of the offset value	00 to FF

*1: The MAC address format above is not applied to LPARs that have performed migration,

*2: The user cannot set a value that duplicates the MAC address automatically generated by LPAR manager. Do not set a multicast address and broad cast address.



Upper 16 bits	YY.YY value
0	00.00
1	00.80
2	00.40
3	00.C0
4	00.20
~	~
7679	B8.FF
7680	78.00
~	~
8187	F8.DF
8188	F8.3F
8189	F8.BF
8190	F8.7F
8191	F8.FF



- It is not recommended to change the MAC address. .If the MAC addresses are changed, make sure that it is not the same MAC address port on the network. If there is more than one identical MAC address on a network, the fatal failure may occur on the network.
- With LPAR manager expansion mode, the virtual NIC number expansion causes Mac addresses, which are automatically generated by LPAR manager, to be also expanded. MAC addresses assigned to the expansion portion can be assigned manually with LPAR manager standard mode. Thus, this may cause MAC addresses to overlap when you change LPAR manager standard mode to LPAR manager expansion mode, which you should note.
- When the version is downgraded to a version not supporting virtual NIC system number expansion, the virtual NIC system number is initialized to 0 if 129 or a larger number is set. When the virtual NIC system number is set to 1 to 128, the number is taken over as it is.

(2) Differences between physical and virtual LAN controllers

LPAR manager provides functions equivalent to installed physical LAN controller, but does not guarantee the same specifications, performance, and compatibility as the physical LAN controller

The following table summarizes the differences from physical LAN controllers.

Item	Difference compared to physical NIC
WoL (Wakeup on LAN) function	WoL function is supported only by shared NICs. Supported items are as follows: - Power control via WoL of ServerConductor/Deployment Manager, ServerConductor/Blade Server Manager, or HCSM - Booting NETM/DM with client control With LPAR manager firmware version 58-80/78-80 or lower, use shared NIC#0 thru #7.
Teaming functions	When using Intel Advanced Networking Services (ANS) for Windows, it is possible to use the adapter fault tolerance (AFT), switch fault tolerance (SFT), and adaptive load balancing (ALB) functions. When using Linux bonding, it is possible to use active-backup, balance-tlb, and balance-alb. For VF NIC, only active-backup is available. However, these functions should be used with communication packet monitoring (Probe and ARP monitoring) turned off and the delay before a team member is activated (Activation Delay, updelay) set to 60 or more. At less than 60, communication with external networks may become impossible upon activation.
Receiving operation when MTU (Maximum Transfer Unit) values are not the same	Always make sure that the MTU value for sender and recipient are the same. If they are not the same, the recipient may not be able to receive packets.
Unicast function	Unicast packet communication between NICs in the same virtual LAN segment does not use external networks. Therefore, monitoring from external networks, such as packet capture, is not available. To monitor all communication over networks, you need to monitor internal and external virtual LAN segments respectively.
PHY loopback function	NIC internal loopback function is not supported. Therefore, a self-diagnostic test of the loopback function will fail.
Jumbo frame	Maximum value for Windows/Linux when jumbo frame is used as follows: ・ Windows (jumbo frame): 9014 byes ・ Linux (MTU): 9000 bytes With LPAR manager firmware version 58-8X/78-8X or lower, do not use jumbo frame.

(3) Notes

- Virtual NIC function Network Performance

  The Virtual NIC function is actually implemented as a NIC emulated by LPAR manager. The network performance is lower than physical NICs, and may vary depending on conditions such as processor activity. When communicating with external networks, as the number of virtual NICs sharing a physical NIC increases, the virtual NIC network performance falls, and the overhead and its variation from the physical NIC become larger.

  Therefore, it is recommended that you use virtual NICs and physical NICs properly according to the environment in which virtual NICs are used or the requirements such as the bandwidth.

  With many physical LAN controllers or high-speed 10 Gb LAN controller installed, their bandwidth may not be fully used.

- Addition and Deletion of Shared NICs/VF NICs to/from the activated LPAR

  It is not possible to add or delete a shared NIC or VF NIC to/from the activated LPAR. To change the configuration, all the LPARs have to deactivate once. Configuration takes a few minutes.

  Therefore, it is recommended that you set the configuration before you activate LPARs.

- NIC Communication during Physical NIC Failure

  If a failure occurs in a physical NIC, the NICs sharing the failed physical LAN controller may become unable to communicate with the external servers and other LPARs.

  If an automatically recoverable hardware failure occurs, communication may be temporarily disabled for recovery. In such a case, communication is disabled for approximately 60 seconds, which may cause some applications to detect a communication error and terminate abnormally.

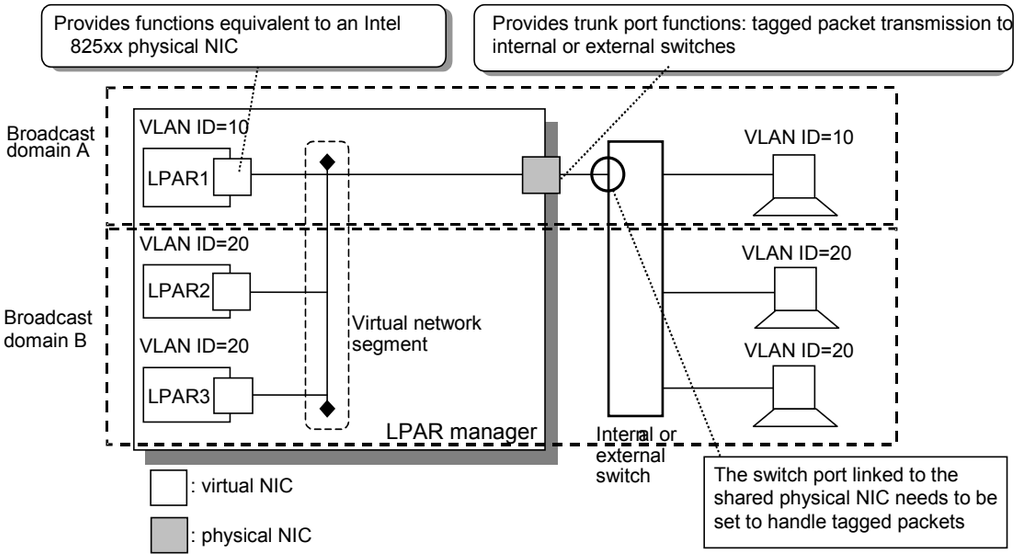
  It is recommended to set the communication failure recovery wait time to a sufficiently large value or make the system redundant.

❑ How to use the VLAN function

(1) Overview of the VLAN functions

Virtual NIC functions support the Tagged VLAN function, which complies with IEEE802.1Q. You can use the VLAN functions to achieve a flexible operating environment, such as:

- Creating multiple broadcast domains.
- Setting multiple VLAN IDs.
- Using an IEEE802.1Q format tag for the interface with the external switches.



(2) How to Use the VLAN Function

Virtual NIC functions provide two types of VLAN functions, and setting to one of them enables the function. You can make these settings for each virtual NIC from the Virtual NIC (VNIC) Assignment screen.

- Untagged port

This setting is for receiving untagged frames from one specified VLAN group.

A virtual NIC for which "untagged port" is specified receives only frames from the group with the same VLAN ID number, and these frames do not include tags. When transferring frames from a virtual NIC specified as an "untagged port" to an external switch or to a virtual NIC specified as a "tagged port" in the same VLAN group, the frames are tagged with the IEEE802.1Q format.

If "untagged" is specified, only one VLAN ID can be specified.

- Tagged port

This setting is for receiving tagged frames (IEEE802.1Q) from more than one specified VLAN group.

A virtual NIC for which "tagged port" is specified can receive both tagged frames with the specified VLAN ID and untagged frames. Tagged frames sent from a virtual NIC with the "tagged port" specification are sent to the same group as the VLAN ID in the tag, and untagged frames are sent to groups for which no VLAN has been set. When frames are transferred to external switches, they are transferred as they are, with or without tags.

When specifying "tagged" for a virtual NIC, you can set up to 16 VLAN IDs for one virtual NIC. To use more than 17, set "ALL" to allow all VLAN IDs to be received.

VLAN mode	Description	Configurable VLAN ID
Undef	VLAN is not used.	-
Tag	Judged that the virtual NIC is connected to the Tagged port (*1).	Up to 16 decimal values from 1 to 4094 or all IDs are allowed.
Untag	Judged that the virtual NIC is connected to the Untagged port (*2).	One out of the range from 1 to 4094

(*1): This port is a trunk port that can handle tagged packets and configure multiple VLAN IDs.

(*2): This port handles untagged packets and can configure one VLAND ID.

◆ Receiving Frames

When conditions for a received frame, VLAN mode configured to the port that receives frames, and VLAN ID correspond with each other, the port receives the frame. Filtering the receiving frames is described in the following table.

VLAN mode of receiving ports	Receiving frame		
	Untagged	Tagged (=VLAN ID)	Tagged (≠ VLAN ID)
Undef	Received	Rejected	Rejected
Tag	Received	Received	Rejected
Untag	Received * Give tags	Rejected	Rejected

◆ Sending Frames

MAC address table selects ports for transfer among ports in which conditions for received frames, VLAN mode, and VLAN ID correspond with each other. Then frames will be transferred.
Frames are sent from the port for transfer. Filtering the sending frames is described in the following table.

VLAN mode of sending port	Received frame		
	Untagged	Tagged (=VLAN ID) (*1)	Tagged (≠ VLAN ID) (*1)
Undef	Sent	- (*2)	- (*2)
Tag	Sent	Sent	- (*2)
Untag	- (*2)	Sent * Delete tags	- (*2)

(*1): Untagged frames are received at the Untagged ports. Tagged frames are included.

(*2): Not selected as the addressed port for frames.

By combining the above virtual NIC settings and guest OS VLAN settings, you can divide broadcast domains as follows.

- Divide a virtual network into multiple broadcast domains for each virtual NIC

  On the Virtual NIC (VNIC) Assignment screen, specify "untagged port" for the virtual NIC and the VLAN ID to which it belongs. There is no need to make VLAN settings in the guest OS because there will be no tags on the packets received by the virtual NIC.

  This means that the guest OS will not be aware of the VLAN, so you can divide the broadcast domain for each virtual NIC.

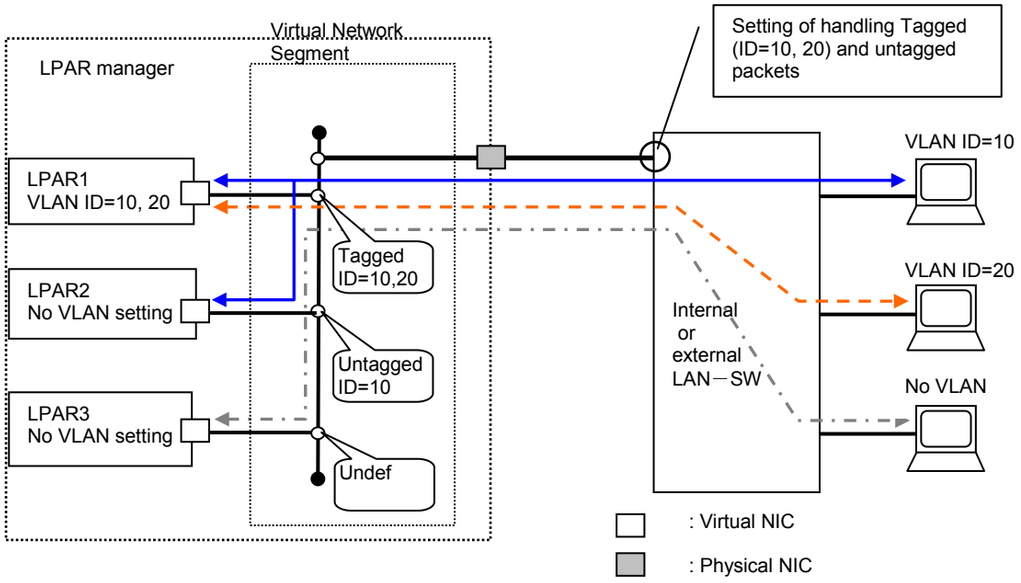
- Assign one virtual NIC to multiple broadcast domains within the same virtual network

  By making VLAN settings for the virtual NIC from the guest OS, you can use the functions equivalent to the physical NIC to operate tags and perform frame filtering. In addition, on the Virtual NIC (VNIC) Assignment screen, specify "tagged port" for the virtual NIC, and specify all the VLAN IDs specified for the virtual NIC in the guest OS.

  This will make it possible to handle more than one VLAN ID per virtual NIC and assign the virtual NIC to more than one broadcast domain.

(3) Example of VLAN Function

The following is an example of using VLAN functions.



<<Setting Example>>
- When setting TagVLAN on OS:
Set the Tagged mode and VLAN ID to the corresponding port on the Virtual NIC (VNIC) Assignment screen of LPAR manager.

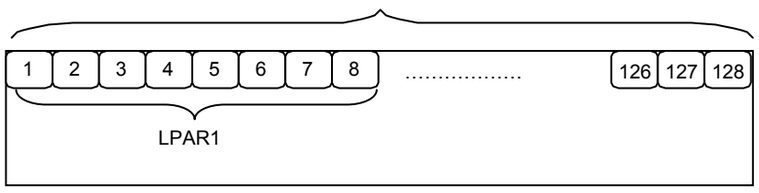
- When sending/receiving Tagged packets to/from the external switch without setting TagVLAN on OS:
Set the Untagged mode and VLAN ID to the corresponding port on the Virtual NIC (VNIC) Assignment screen of LPAR manager.

- When sending/receiving Untagged packets to/from the external switch without setting TagVLAN on OS:
Set the Undef mode (default) to the corresponding port on the Virtual NIC (VNIC) Assignment screen of LPAR manager.

(4) Virtual Switch Image

The following describes virtual switch images.

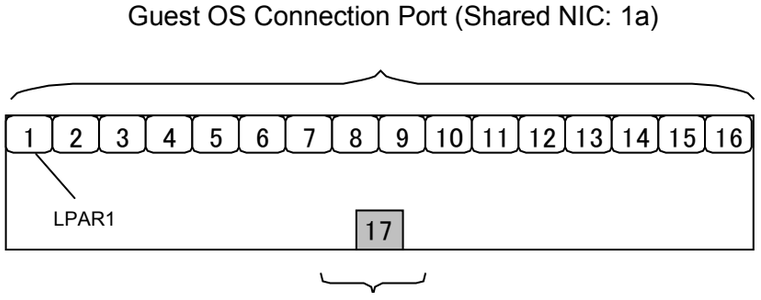
- Image of a virtual NIC switch:
  The following example is for 128-port (8 ports/LPAR) layer 2-switch with.16 LPARs and 8 virtual NICs per LPAR. Four switches can be installed to Va to Vd. All ports are configured with virtual NIC ports.



Setting Item	Targeted Port	Settings
Port connection	Port1 - Port128	Assign to LPAR on the Virtual NIC (VNIC) Assignment screen.
Port Speed	Port1 - Port128	Auto Negotiation (This setting cannot be changed.) - Supports 1000BASE-TX
VLAN mode and VLAN ID	Port1 - Port128	[VLAN mode] - Undef (default) - Tagged - Untagged * Only one (1) VLAN mode per port can be set [VLAN ID] - Tagged : Up to 16 VLAN IDs out of the range from 1 to 4094, or Assign all (ID). - Untagged: Only one (1) VLAN ID out of the range from 1 to 4094
Promiscuous mode	Port1 – Port 128	- Restricted Receives only packets addressed to the LPAR (MAC). - Through (default) Receives all packets in the same network.

◆ Image of a shared NIC switch

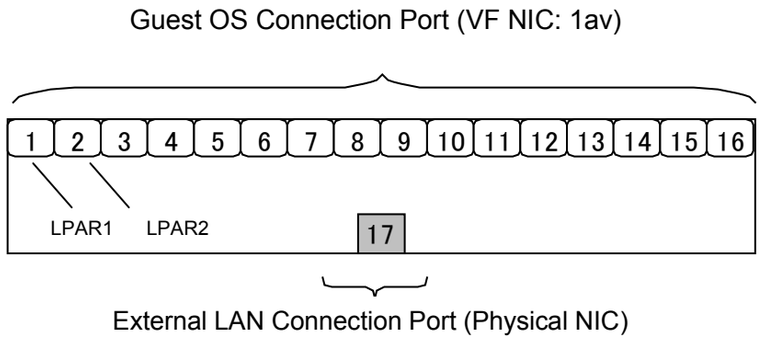
The following example is for 17-port (1 port/LPAR + physical NIC) layer 2-switch function with16 LPARs and 1 shared NIC per LPAR.
Up to 16 pieces of this switch can be mounted depending on the number of physical NICs with shared setting.
Ports 1 – 16 are configured by the shared NICs and Port17 by the physical NIC port.



Setting Item	Targeted Port	Settings
Port connection	Port1 - Port16	Assign to LPAR on the Virtual NIC (VNIC) Assignment screen.
	Port17	Connect to physical cables. * With the onboard NIC, no cable is required.
Port Speed	Port1 - Port16	Auto Negotiation (This setting cannot be changed.) - Supports 1000BASE-TX.
	Port17	Auto Negotiation (This setting cannot be changed.) - Supports 10/100/1000/10000BASE-TX\
VLAN mode and VLAN ID	Port1 - Port16	*[VLAN mode] (if the version of Emulex NIC firmware is 4.6.x.x)]* *- Undef (Default)* *- Tagged* *- Untagged* ** Only 1 VLAN mode can be set per LPAR.* [VLAN mode (if the version of Emulex NIC firmware is 10.2.x.x) - Tagged (default) - Untagged * Only 1 VLAN mode can be set per port *[VLAN ID]* *- Tagged : Up to 16 VLAN IDs out of the range from 1 to 4094, or Assign all (ID).* *- Untagged : Only one (1) VLAN ID out of the range from 1 to 4094*
	Port17	Tagged All (This setting cannot be changed.) * Configured to transmit all packets.
Promiscuous mode	Port1 – Port 16	- Restricted Receives only packets addressed to the LPAR (MAC). - Through (default) Receives all packets in the same network.

- Image of a VF NIC switch

  The following example is for 17-port (1 port/LPAR + physical NIC) layer 2-switch function with16 LPARs and 1 VF NIC per LPAR.
  Up to 16 pieces of this switch can be mounted depending on the number of physical NICs with shared setting.
  Ports 1 – 16 are configured by VF NICs and Port17 by the physical NIC port.



Setting Item	Targeted Port	Settings
Port connection	Port1 - Port16	Assign to LPAR on the Virtual NIC (VNIC) Assignment screen.
	Port17	Connect to physical cables.
Port Speed	Port1 - Port16	Auto Negotiation (This setting cannot be changed.) - 10GBASE-KR - 1000GBASE-KX
	Port17	Auto Negotiation (This setting cannot be changed.) - 10GBASE-KR - 1000GBASE-KX
VLAN mode and VLAN ID	Port1 - Port16	[VLAN mode] (When Emulex NIC firmware version is 4.6.x.x)] - Undef (Default) - Tagged - Untagged * Only 1 VLAN mode can be set per port. [VLAN mode (When Emulex NIC firmware version is 10.2.x.x)] - Tagged (Default) - Untagged * Only 1 VLAN mode can be set per port. [VLAN ID] - Tagged : Only [All] (ID) can be specified. - Untagged : Only one (1) VLAN ID out of the range from 1 to 4094
	Port17	Tagged All (This setting cannot be changed.) * Configured to transmit all packets.
Promiscuous mode	Port1 – Port 16	- Restricted (default): Receives only packets addressed to the LPAR (MAC). - Through: Not supported.

(5) Cautions

- Communication with external networks using VLANs

Because IEEE802.1Q tagged packets pass through the external physical switches, it is necessary to set the VLAN ID used by the virtual network corresponding to the shared NIC to physical switch port at the tagged port.

- Priority control in the IEEE802.1P format

Priority control in the IEEE802.1P format is not supported.

- Using VLAN functions and N+M cold standby at the same time

Switch	Description
LAN switch	Cm2/Network Element Configuration is required.
DCB switch	Automatic migration of port profiles (AMPP) function for the DCB switch is used.

❑ How to use Promiscuous function

(1) How to set the promiscuous mode

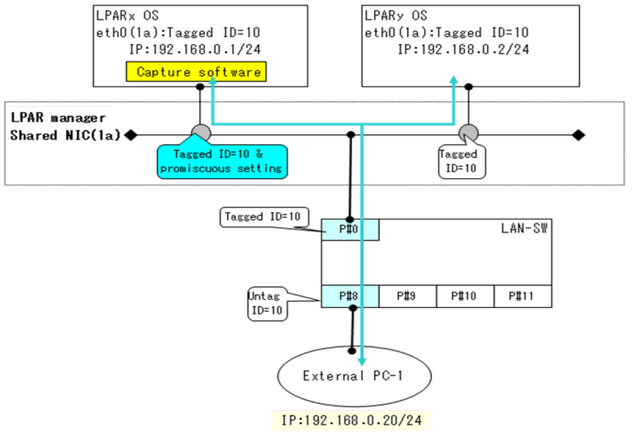
You can set the promiscuous mode to an LPAR on the Virtual NIC (VNIC) Assignment screen, one of the LPAR manager screens. See “(4) How to change the promiscuous mode” for details.

(2) Performance of packet capture

- Packet capture on the same network segment

When the promiscuous mode is Restricted, a unicast packet between LPARy and the external PC-1 cannot be captured.

When the promiscuous mode is Through, a unicast packet between LPARy and the external PC-1 can be captured.

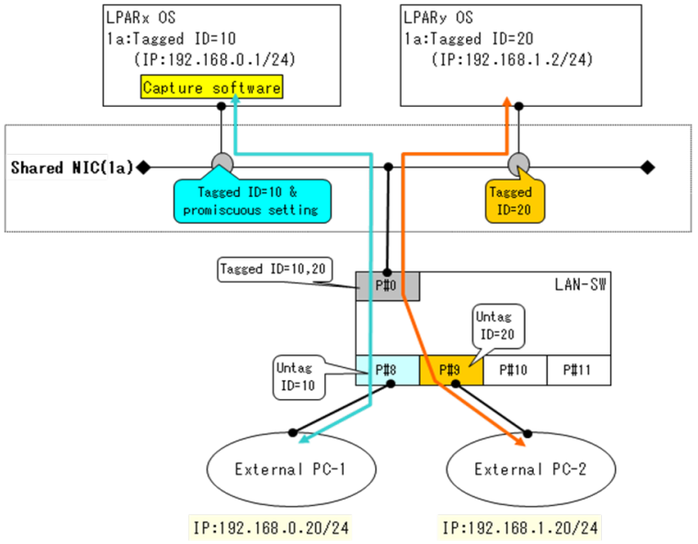


Communication route	Promiscuous mode	
	Restricted	Through
LPARx --> LPARy	✓	✓
LPARx → External PC-1	✓	✓
LPARx Broadcast	✓	✓
LPARy → LPARx	✓	✓
LPARy → External PC-1	-	✓
LPARy Broadcast	✓	✓

[✓]: can be captured [-]: cannot be captured

◆ Capturing packets on different network segment

Packets on the different network segment cannot be captured, even if it is on the same VNIC segment.



Communication route	Promiscuous mode	
	Restricted	Through
LPARx --> LPARy	None	None
LPARx → External PC-1	✓	✓
LPARx Broadcast	✓	✓
LPARy → LPARx	None	None
LPARy → External PC-1	-	-
LPARy Broadcast	-	-

[✓]: can be captured; [-]: cannot be captured: [None]: no packet

(3) Examples of promiscuous mode

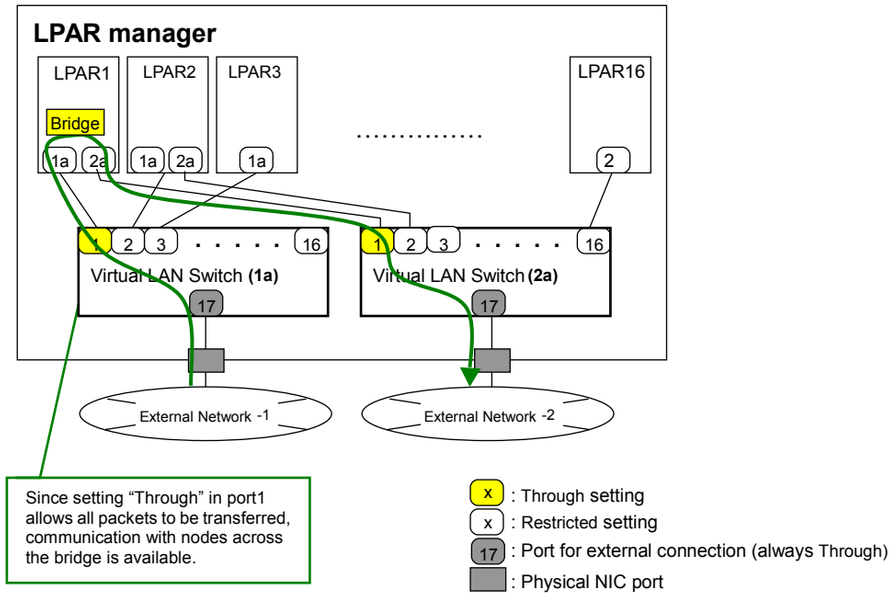
Set the promiscuous mode to “Through” in the following environment.

#	Environment	Behavior with promiscuous mode “Restricted”
(a)	Bridge is implemented in a guest OS.	Cannot transfer any packet.
(b)	MAC address is changed in a guest OS.	Cannot transfer any packet.
(c)	Load balancing using the MAC address shared by multiple NICs is used.	Load balancing (redundancy function) does not work properly.

(a) Bridge is implemented in a guest OS:

When implementing the bridge in a guest OS, make sure to set the promiscuous mode to “Through” for the internal virtual switch of LPAR manager connected to the guest OS.

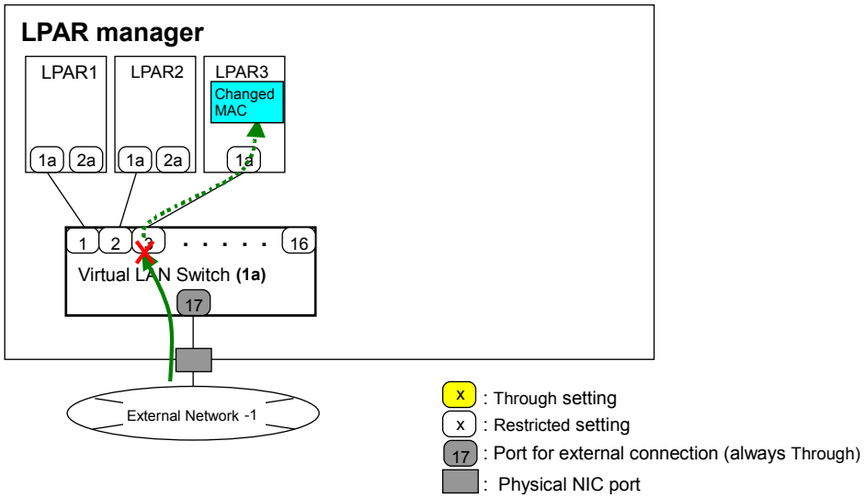
The following figure shows how to transfer a packet when the bridge is implemented in the guest OS. When the promiscuous mode is set to Through for each port1 of the virtual LAN switch (1a) and (2a), communication with nodes is available across the bridge. That is because port1 of both virtual LAN switches can transfer packets not to the MAC address of LPAR1 NIC.



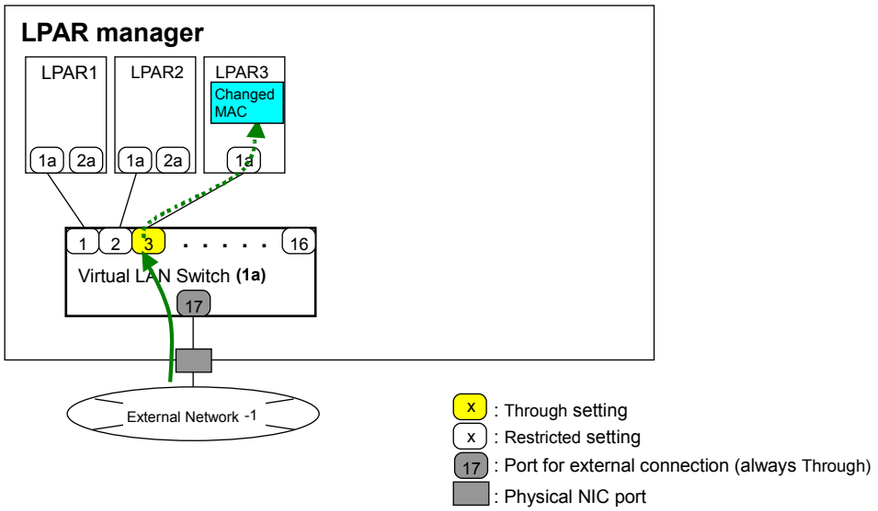
(b) MAC address is changed in a guest OS.

When a MAC address is changed in a guest OS, make sure to set the promiscuous mode to “Through” for the internal virtual switch of LPAR manager connected to the guest OS. The following figure shows how to transfer a packet when the MAC address is changed in the guest OS.

When promiscuous mode is not set to Through, port3 of the virtual LAN switch 1a transfer packets only for the former MAC address of LPAR3 NIC 1a and cannot communicate with external nodes.



When the promiscuous mode is set to “Through”, LPAR3 can communicate with external nodes. That is because port3 of the virtual LAN switch 1a can transfer packets to the changed MAC address of LPAR3 NIC 1a.



(c) Load balancing using the MAC address shared by multiple NIC cards is used.

When using teaming and/or load balancing, it is recommended to verify the operation in advance or set promiscuous mode to “Through”.

See “LAN Advanced Function Manual”, Appendix in *Hitachi Compute Blade 2000 SOFTWARE GUIDE* for details of teaming and load balancing.

Shared FC Functions

❑ Overview of the Shared FC Function

The following two Fibre Channel (FC) functions are supported by LPAR manager.

- Dedicated FC

  In this mode, an FC adapter, by the unit of a PCI card, is allocated to an LPAR and used by the LPAR. Multiple LPARs cannot use a single FC adapter at the same time. This is for an environment where data transmission performance is important.

- Shared FC

  In this mode, a single FC adapter can be allocated to and shared by multiple LPARs, and they can use the adapter simultaneously. In the shared FC, there are two ways in which the FC adapter can be shared.

  - FC Port assigned respectively to an LPAR

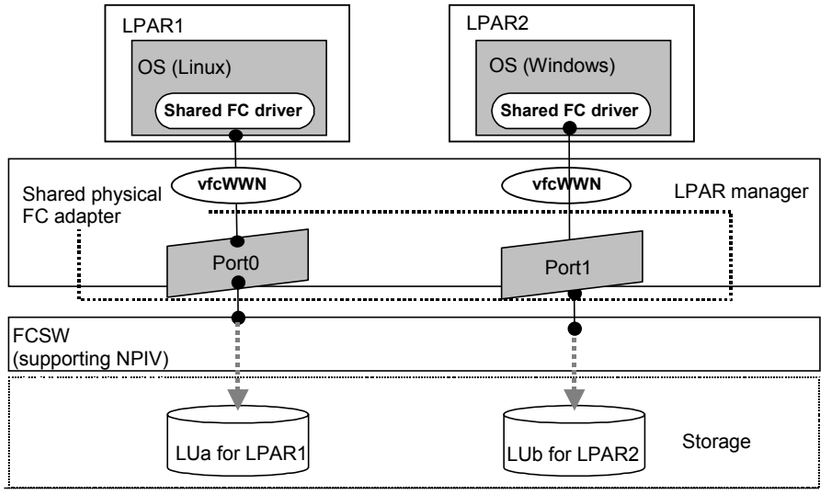
    This method involves assigning one LPAR exclusively to a port on a FC adapter that has two or more ports.

    Thus, by using the FC Port Partition function with a FC adapter with two ports, two LPARs can share a FC adapter.

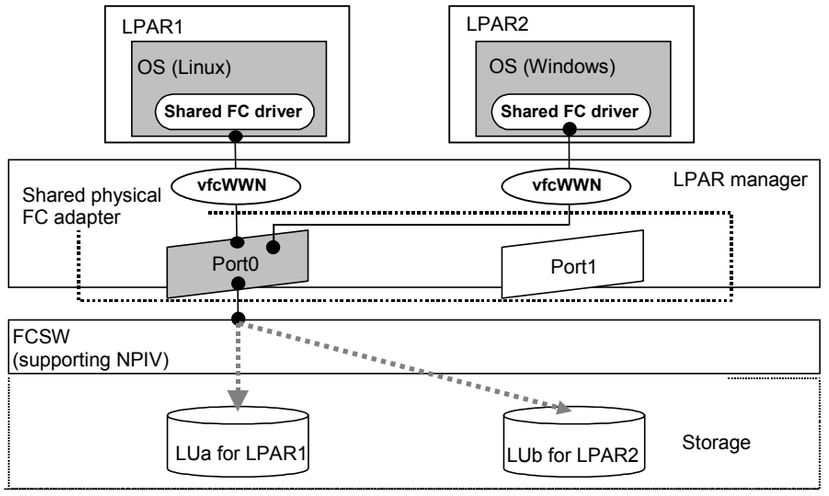
  - FC Port assigned to multiple LPARs

    One port of the FC adapter can be assigned to multiple LPARs.

    The following figure shows an image of FC Port assigned respectively to an LPAR.



The following figure shows an image of FC Port assigned to multiple LPARs.



❑ FC Adapter Sequences Recognized by LPAR manager

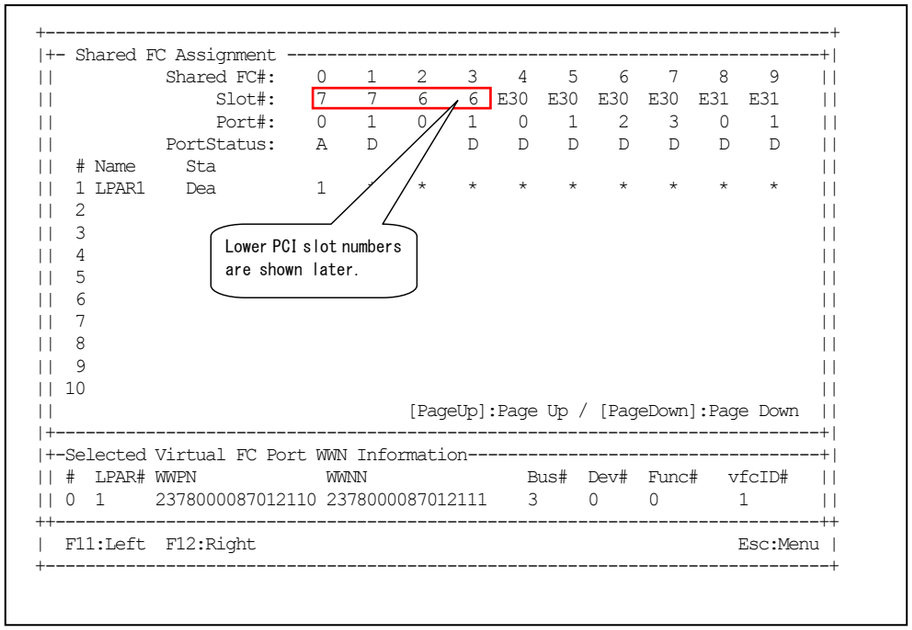
This section describes connections between FC adapter switch modules and ports, and sequences recognized by LPAR manager.

The following table takes server blade 3 with FC adapters as an example. For server blade 1, replace each slot number, such as replacing PCI Slot6 with PCI Slot2 and PCI Slot7 with PCI slot3. For other server blades, do it the same way.

Slot / Port installed		Switch module port for connection	Sequence recognized by LPAR manager
PCI Slot6	Port0	FC switch module port0 in I/O board module slot6	2 *1
	Port1	FC switch module port1 in I/O board module slot6	
PCI Slot7	Port0	FC switch module port0 in I/O board module slot7	1 *1
	Port1	FC switch module port1 in I/O board module slot7	
Expansion Slot0	Port0	FC switch module port in switch module slot2	3
	Port1	FC switch module port in switch module slot2	
	Port2	FC switch module port in switch module slot3	
	Port3	FC switch module port in switch module slot3	
Expansion Slot1	Port0	FC switch module port in switch module slot4	4
	Port1	FC switch module port in switch module slot4	
	Port2	FC switch module port in switch module slot5	
	Port3	FC switch module port in switch module slot5	

*1 Since PCI slot sequence is recognized in reverse order, PCI slot numbers are shown in reverse order on screens such as PCI Device Information and Shared FC Assignment.

Numbers shown on the LPAR manager screen are as follows:



❑ How to use the shared FC function (I) with connection to storage via FC switch with NPIV support

(1) Set shared FC on LPAR manager screen

The settings for sharing a FC adapter can be made on the PCI Device Assignment screen and Shared FC Assignment screen. See Assign PCI devices to LPARs and Assign shared FCs to LPARs for details.

- Set the scheduling mode of the FC card to the shared mode on the PCI Device Assignment screen.
- Set the following information on the Shared FC Assignment screen.
  - Shared FC port to assign to the user LPAR
  - WWN identifier (vfcID) to assign to the shared FC

(2) Set Shared FC for storage/FCSW

No special setting is required for the storage/FCSW (Fibre Channel Switch), but the FCSW you are using needs to support the NPIV (N_Port ID Virtualization) function.

For the storage, set the virtual WWPN / WWNN (hereafter referred to as vfcWWPN / vfcWWNN).

The vfcWWPN / vfcWWNN is created by LPAR manager from the vfcID set in the Shared FC Assignment screen. You can check the created vfcWWPN / vfcWWNN on the LPAR manager Shared FC Assignment screen and the Allocated FC Information screen.

(3) Set Adapter Performance Parameter

You can set each performance parameter of the FC adapter using the EFI driver on the LPAR. See *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*.

❑ How to use the shared FC function (II) with connection directly to storage

With 8 Gbps fibre channel adapter, an LPAR can be connected directly to storage. To use this connection, set Loop connection as a connection type with the EFI driver on the LPAR.

(1) Set FC to Dedicated on LPAR manager Screen

Set the scheduling mode of FC adapter to Dedicated on the PCI Device Assignment screen of LPAR manager screens. See Assign PCI devices to LPARs for details. On the PCI Device Assignment screen, set the FC adapter's scheduling mode to the dedicated.

(2) Set Loop Connection with EFI Driver

Set loop connection with the EFI driver on an LPAR. See *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*. Connection types cannot be changed unless the scheduling mode of FC adapter is in dedicated mode.

- With the EFI driver, set the connection type to Loop only.

```
hfccfg.XXXXXXXXXXXXXXX>set
  Base Settings:
       :
       :
    ** Connection Type = Auto Detection
       change? (y/[n]) -->y
           0 - Auto Detection -[default]
           1 - Point to Point Only
           2 - Loop Only
           c - cancel
       please select -->2
    ** Data Rate = Auto Detection
       :
       :
hfccfg.XXXXXXXXXXXXXXX>
```

(3) Set Shared Mode on LPAR manager Screen

Set FC adapters in shared mode on the PCI Device Assignment screen and Shared FC Assignment screen of LPAR manager. See Assign PCI devices to LPARs and Assign shared FCs to LPARs for details.

- Set the scheduling mode of FC adapters in shared mode on the PCI Device Assignment screen.
- Set the followings on the Shared FC Assignment screen.

  Shared FC ports to be assigned to user LPARs

  WWN identifier to be assigned to shared FC (vfcID)

(4) Set storage and FC Switch to Share FC

Set the SAN security with which the virtual WWPN/WWNN, hereinafter referred to as vfcWWPN/vfcWWNN, can access the FC. LPAR manager creates vfcWWPN/vfcWWNN using vfcID configured on the Shared FC Assignment screen. Those created vfcWWPN/vfcWWNN can be found on the Shared FC Assignment screen and Allocated FC Information screen of LPAR manager.

(5) Set FC Adapter Performance Parameter

Set each performance parameter of FC adapters with the EFI driver on LPARs. See *HITACHI Gigabit Fibre Channel Adapter User's Guide (BIOS/EFI Edition)*.

❑ Specifications of the Shared FC Function

(1) WWPN / WWNN for a Shared FC

The WWPN / WWNN (World Wide Port Name / World Wide Node Name) used by a shared FC is provided in the following format. This WWPN / WWNN address is automatically generated by the LPAR manager from the vfcID value that you set on the LPAR manager control screen.

WWPN / WWNN format (64 bits):

0010 UUUU LLCC CLLL 0000 0000 0000 0000 1000 0111 LLLL LLLL LLLF FFFF FRED DDDJ

WWPN/ WWNN	Field explanation	Value generated by LPAR manager (bit)
C (3 bits)	Platform ID	010
D (4 bits)	vfcID (enter on the Shared FC Assignment screen)	vfcID
E (1 bit)	FC port No. on FC card	Port0: 0 Port1: 1 Port2: 0 Port3: 1
F (6 bits)	Relative slot No. in which FC card is installed	・ Mezzanine card slot 0 Port0: 111111 Port1: 111111 Port2: 111110 Port3: 111110 ・ Mezzanine card slot 1 Port0: 111101 Port1: 111101 Port2: 111100 Port3: 111100 For the relative slot number for PCI card slots, see Relative slot numbers.
J (1 bit)	WWPN or WWNN (0 = WWPN, 1 = WWNN)	WWPN: 0 WWNN: 1
L (16 bits)	Serial No. given to LPAR manager (hexadecimal digits)	Last 4 digits of LP serial No.
R (1 bit)	Reservation	0
U (4 bit)	Vendor management No.	0011

Note: The WWPN/WWNN format above cannot be applied to LPARs that have performed migration.

(2) Notes

- Addition or Deletion of a Shared FC Adapter to the activated LPAR

  It is not possible to add or delete a shared FC adapter to the activated LPAR. To change the configuration of a shared FC adapter, all LPARs have to be deactivated. Changing the configuration of a shared FC adapter may take a few minutes.

  Therefore, it is recommended that you set the configuration of the shared FC adapter before you activate LPARs.

- Communication in the event of a failure in the shared FC adapter

  If a failure occurs in a shared FC adapter, all the LPARs sharing the failed physical FC adapter will become unable to use it to communicate.

- Detection of the unallocated FC ports by guest OSs (when the FC Port is assigned respectively to an LPAR)

  With the shared FC function, you can use a 2-port FC adapter such that you allocate only one port of it to a LPAR but do not allocate another port to any LPARs. When you boot a guest OS on such LPAR, the guest OS may detect the unallocated port as follows, but the OS activity will not be affected.

  Microsoft Windows:

  SCSI described as “Unassigned Hitachi Shared FC Device” and a RAID controller device can be seen from the device manager.

  Linux

  By inputting the lspci command, the following device is informed (the head “bb:dd.f” may be different depending on the PCI slot location).

  bb:dd.f Fibre Channel: Hitachi, Ltd: Unknown device 3017

- Port in the FC Shared function

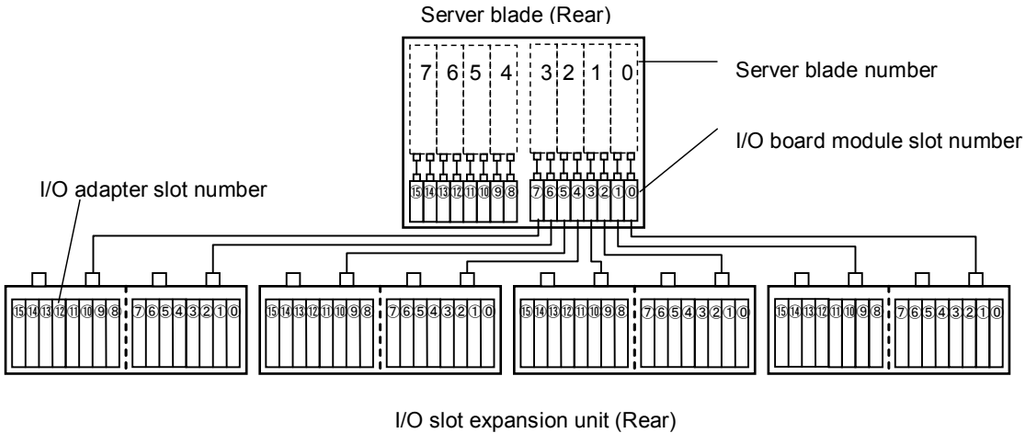
  In the FC shared function, the LPAR manager FC shared management port logs in the FC switch using the virtual WWPN (2300000087xxxxxx) vfcID=0.

  Therefore, the port of the FC switch connected to the FC shared port can see the log-in status of by the virtual WWPN vfcID=0 as well as the WWPN used on the guest OS.
  Virtual NIC Function Specifications

❑ Relative slot numbers

Relative slot numbers are uniquely defined in each system configuration.

The following figure shows slot locations on each unit.



The following table shows an example without an I/O slot expansion unit connected:

Without an I/O slot expansion unit

server blade		Relative slot number
Server blade number	Slot number of I/O board module	
0	0	0
	1	1
1	2	0
	3	1
2	4	0
	5	1
3	6	0
	7	1
4	8	0
	9	1
5	10	0
	11	1
6	12	0
	13	1
7	14	0
	15	1

The following table shows an example with an I/O slot expansion unit connected to server blade 0. With server blade 1, replace slot numbers of I/O board modules 0-1 with slot numbers 2-3. Replace I/O adapter slot numbers as well.

With an I/O slot expansion unit connected to one server blade

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
0	0	0	8	8	-
		1	9	9	-
		2	10	-	10
		3	11	-	11
		4	12	12	-
		5	13	13	-
		6	14	-	14
		7	15	-	15
	1	8	16	16	-
		9	17	17	-
		10	18	-	18
		11	19	-	19
		12	20	20	-

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
		13	21	21	-
		14	22	-	22
		15	23	-	23

The following table shows an example with I/O slot expansion units connected to server blades 0 and 1 in 2-blade SMP configuration. With server blades 2 and 3, replace slot numbers of I/O board modules 0-3 with slot numbers 4-7. Replace I/O adapter slot numbers as well.

With I/O slot expansion units in 2-blade SMP configuration

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
0	0	0	8	8	-
		1	9	9	-
		2	10	-	10
		3	11	-	11
		4	12	12	-
		5	13	13	-
		6	14	-	14
		7	15	-	15
	1	8	16	16	-
		9	17	17	-
		10	18	-	18
		11	19	-	19
		12	20	20	-
		13	21	21	-
		14	22	-	22
		15	23	-	23
1	2	0	24	24	-
		1	25	25	-
		2	26	-	26
		3	27	-	27
		4	28	28	-
		5	29	29	-
		6	30	-	30
		7	31	-	31
	3	8	32	32	-
		9	33	33	-

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
		10	34	-	34
		11	35	-	35
		12	36	36	-
		13	37	37	-
		14	38	-	38
		15	39	-	39

The following table shows an example with I/O slot expansion units connected to server blades 0, 1, 2, and 3 in 4-blade SMP configuration. With the server blade 4, 5, 6, and 7, replace slot numbers of I/O board modules 0-7 with slot numbers 8-15. Replace I/O adapter slot numbers as well.

With I/O slot expansion units in 4-blade SMP configuration

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
0	0	0	8	8	-
		1	9	9	-
		2	10	-	10
		3	11	-	11
		4	12	12	-
		5	13	13	-
		6	14	-	14
		7	15	-	15
	1	8	16	16	-
		9	17	17	-
		10	18	-	18
		11	19	-	19
		12	20	20	-
		13	21	21	-
		14	22	-	22
		15	23	-	23
1	2	0	24	24	-
		1	25	25	-
		2	26	-	26
		3	27	-	27
		4	28	28	-
		5	29	29	-
		6	30	-	30

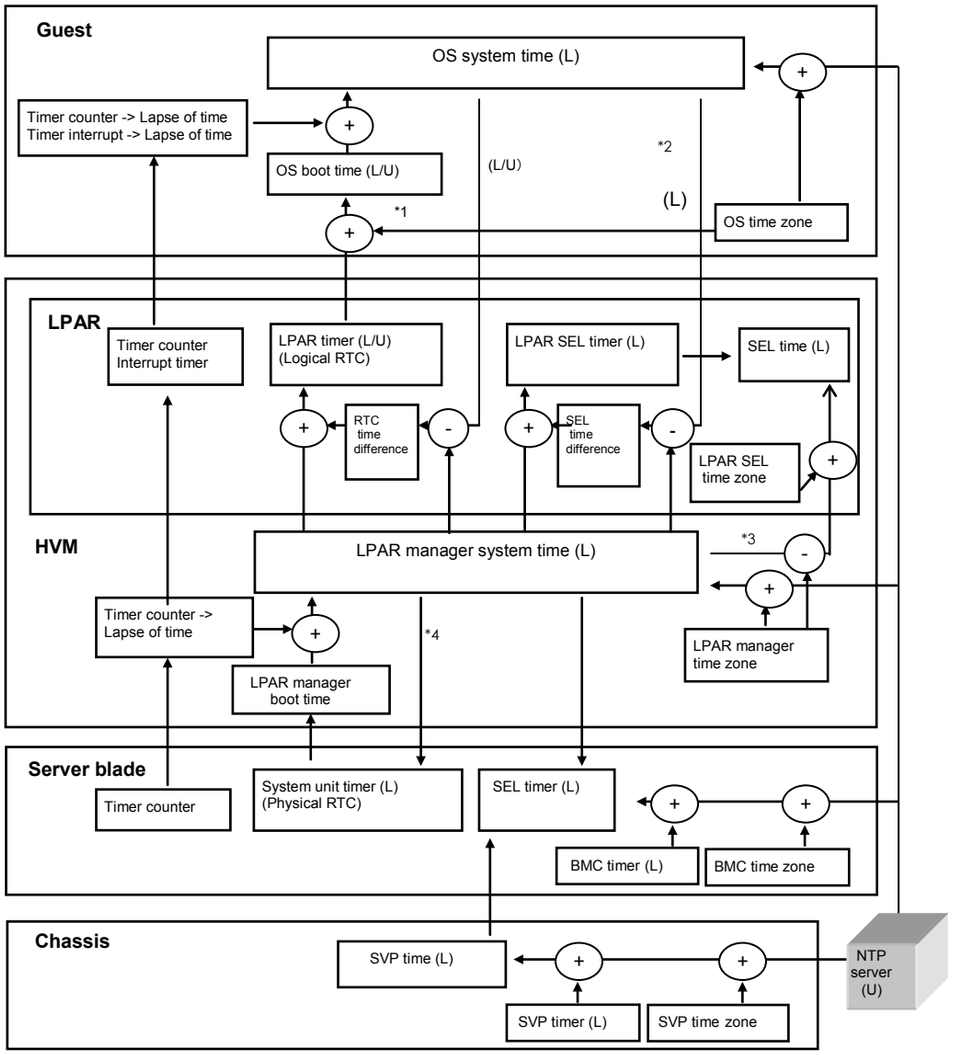
Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
		7	31	-	31
	3	8	32	32	-
		9	33	33	-
		10	34	-	34
		11	35	-	35
		12	36	36	-
		13	37	37	-
		14	38	-	38
		15	39	-	39
2	4	0	72	72	-
		1	73	73	-
		2	74	-	74
		3	75	-	75
		4	76	76	-
		5	77	77	-
		6	78	-	78
		7	79	-	79
	5	8	80	80	-
		9	81	81	-
		10	82	-	82
		11	83	-	83
		12	84	84	-
		13	85	85	-
		14	86	-	86
		15	87	-	87
3	6	0	88	88	-
		1	89	89	-
		2	90	-	90
		3	91	-	91
		4	92	92	-
		5	93	93	-
		6	94	-	94
		7	95	-	95
	7	8	96	96	-
		9	97	97	-
		10	98	-	98
		11	99	-	99
		12	100	100	-
		13	101	101	-
		14	102	-	102

Slot number of server blade		I/O slot expansion unit	Relative slot number		
Server blade number	Slot number of I/O board module	I/O adapter slot number	1:8 mode	1:4 mode (port 0)	1:4 mode (port 1)
		15	103	-	103

Timer functions

❑ Timer function overview

The following figure shows how LPAR manager calculates time and relations among timers.



Terms

RTC: Real Time Clock

SEL: System Event Log

U/L: UTC (Universal Coordinated Time)/Local time

*1 When UTC is adopted for LPAR timer, add the time zone.

*2 When SEL is created with SC/BSM during DST (daylight saving time), there is a DST difference between the SEL time and OS system time.

*3 This route is used only when LPAR manager creates LPAR SEL.

*4 When NTP server is used, the system unit timer is updated.

The following table describes timers and relations with each time.

Timer	Description	Support for		
		Local time	UTC	DST
SVP timer	Implemented in SVP.	✓	✓	✓
BMC timer	Implemented in BMC. BMC time is used for the time field in SEL.	✓	✓	✓
System unit timer	Implemented in a server blade. With no time zone LPAR manager only supports local time (*1)	✓		
NTP server	Distributes time to devices on a network. Provides UTC time.		✓	✓
LPAR manager system time	Time of LPAR manager on a server blade Calculated by adding time shown by the system unit timer at LPAR manager boot and a lapse of time on the timer counter.	✓	-	-
LPAR timer	Used as the reference for OS system time. Virtualized system unit timer: differential time between LPAR manger system time and OS system time. (*2)	✓		
LPAR SEL timer	Used as the reference for LPAR SEL time. Virtualized SEL timer: differential time between LPAR manager system time and OS system time. (*2)	✓	✓	-
LPAR SEL time zone	Time zone for LPAR SEL time Used when LPAR manager creates SEL.			-
OS system time	Guest OS time Calculated by adding time shown at LPAR manager boot and a lapse of time on the LPAR timer at OS boot, a lapse of time calculated using the values on the timer counter, and the number of timer interrupts, and the time zone.	✓	✓	✓

✓: No action required.

-: Not supported.

\: Not defined in the architecture: Out of target

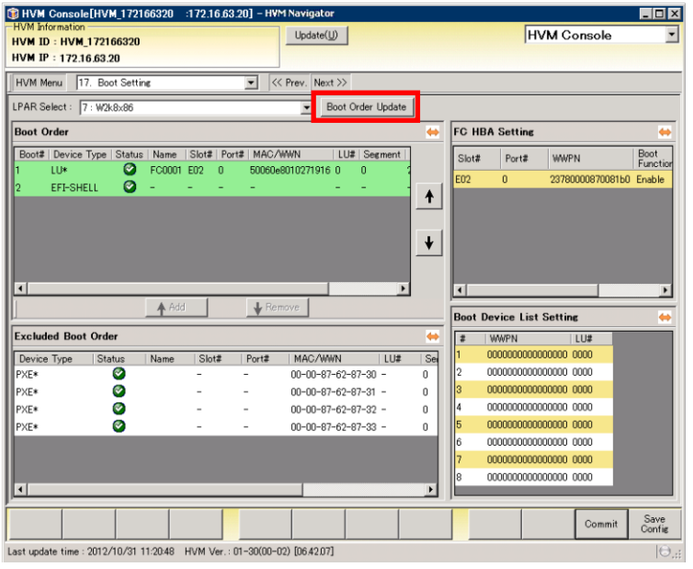
*1: System unit timer is updated when NTP server is used. If without NTP server, it is not updated.

*2: Differential time between LPAR timer and LPAR SEL timer is stored in the management module by saving it on the LPAR manager screen. Save it often. Especially save it when changing the OS time.

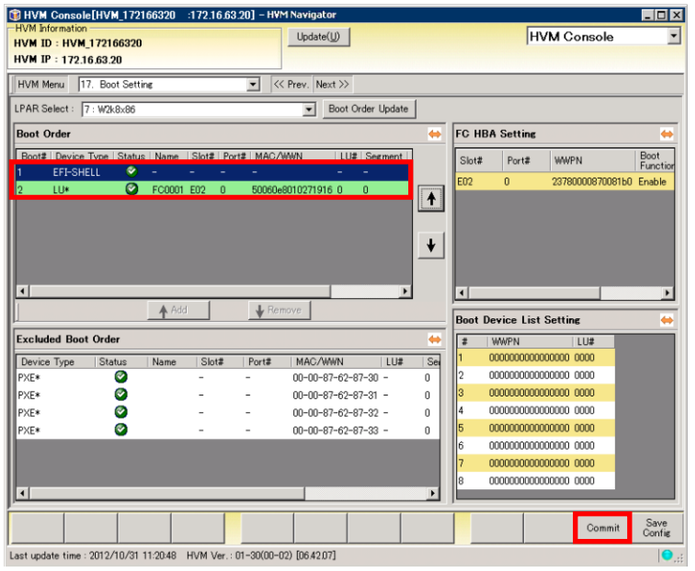
❑ Configuring the LPAR Timer

The following steps show how to configure the LPAR timer with HVM Navigator, which is recommended because it is easy to operate. You can also configure the LPAR timer with EFI on the LPAR manager screen. See the *HVM Navigator User's Guide* for details.

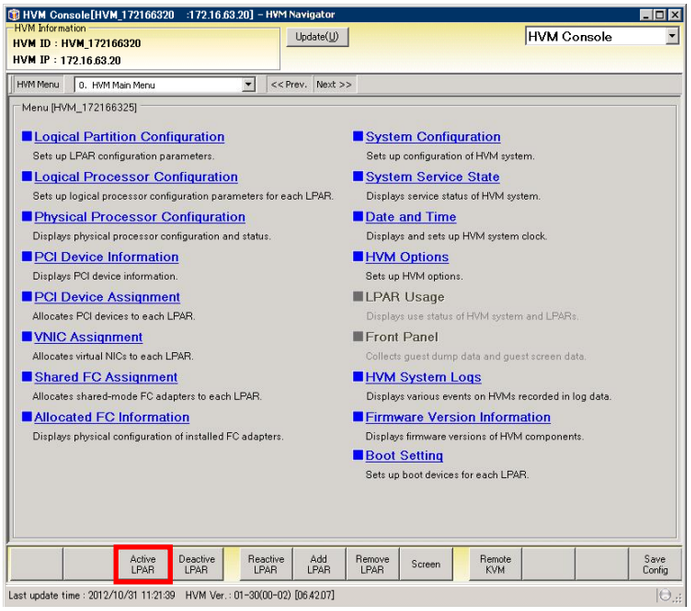
1. Open **Boot Setting Menu on HVM Console**, and click **Boot Order Update**.



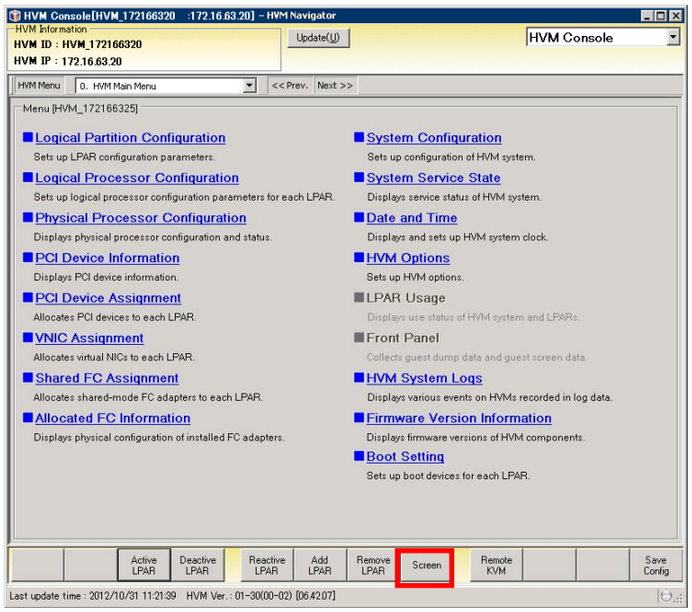
2. Place EFI-SHELL on the top in the Boot Order pane, and click **Commit**. Click the arrow button to **HVM Menu** to select **0. HVM Main Menu** from the drop-down list.



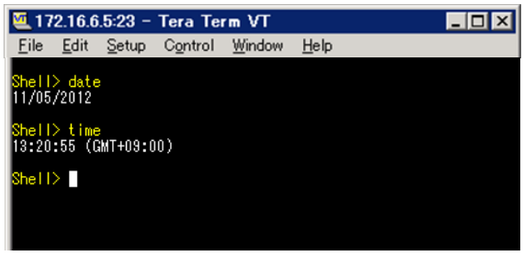
3. When the HVM Main Menu is displayed, click **Activate LPAR** to activate the target LPAR.



4. Click **Screen** to open the activated LPAR screen.



5. Set the date and time on the EFI-SHELL.



<Time input format>

date

time

timezone

<Time setting input format>

date: mm/dd/yyyy

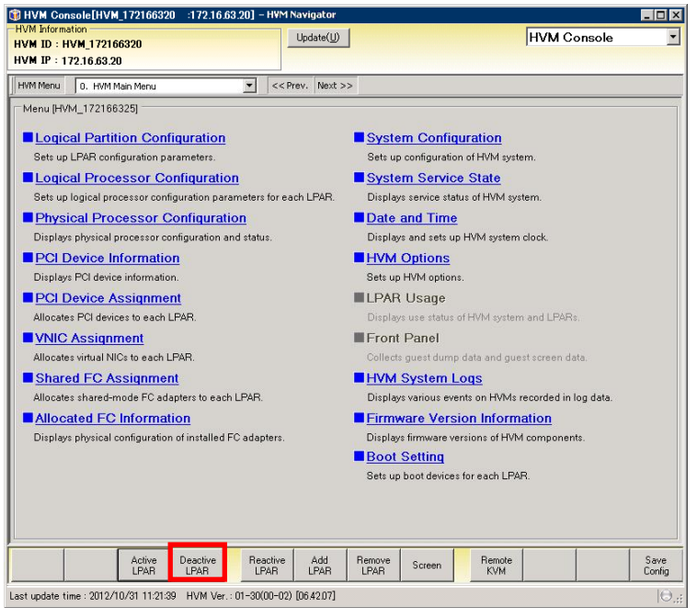
time: hh:mm:ss

timezone: -s hh:mm

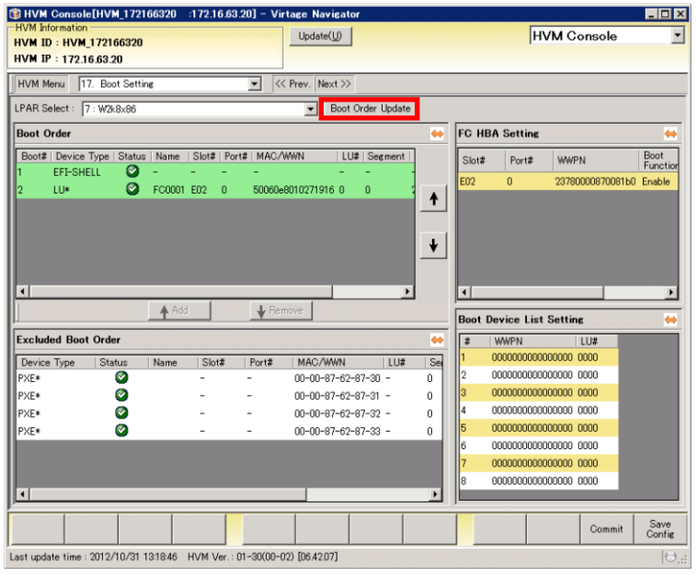
Set the local time with the time command.

The Timezone command shows the timezone, which will not affect EFI or OS behavior. The Timezone setting is not essential.

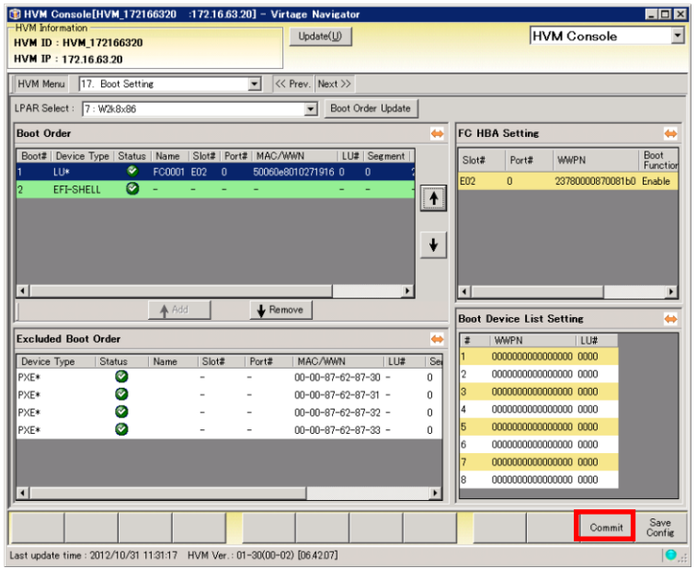
6. Click **Deactivate LPAR** on **HVM Main Menu** to deactivate the target LPAR.



7. Open **Boot Setting Menu on HVM Console**, and click **Boot Order Update**.



8. Place **LU** to boot on the top in the **Boot Order** pane, and click **Commit**.



LPAR manager operating mode

❑ Overview of LPAR manager operating mode

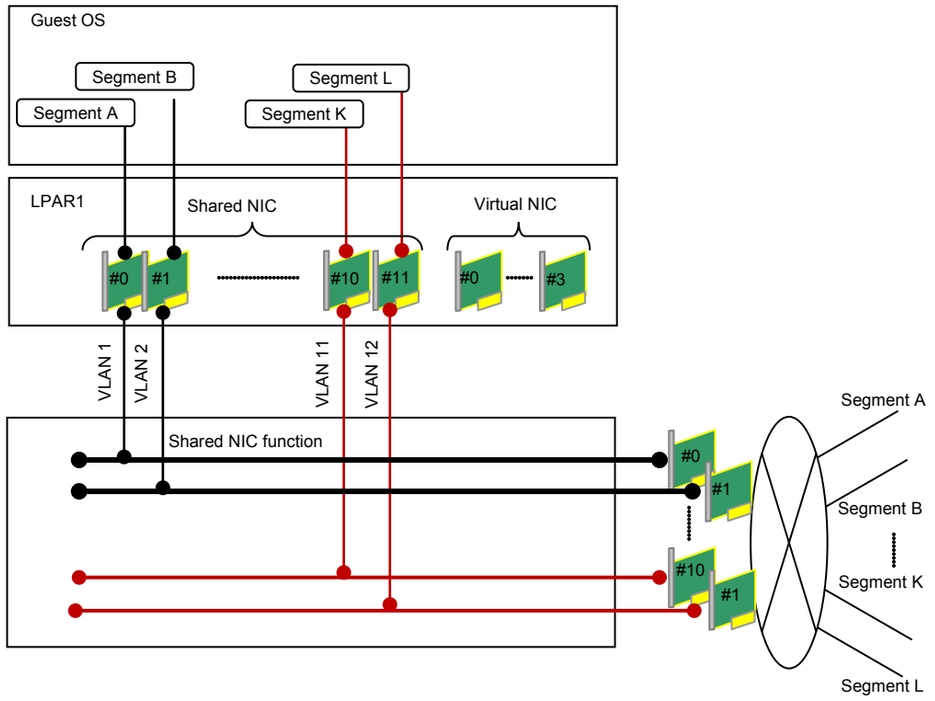
LPAR manager operating modes consist of two modes: LPAR manager standard mode and LPAR manager expansion mode. You can change modes with LPAR manager screens, HvmSh command, or HVM Navigator.

See System Configuration > How to change the LPAR manager Operating Mode for how to change LPAR manager operating modes on the LPAR manager screen.

Item	Standard server blade		High-performance server blade	
	LPAR manager standard mode	LPAR manager expansion mode	LPAR manager standard mode	LPAR manager expansion mode
Max number of LPARs to be activated	16	16 (58-7X or later) 30 (58-8X or later)	60	60
Memory used by LPAR manager	1280 MB	1536 MB	1536 MB	1536 MB
Max total number of shared NICs and virtual NICs to be assigned to one LPAR	8	16	8	16
Overlapped port assignment for shared NIC	-	✓	-	✓
Shared NIC port assigned respectively to an LPAR	-	✓	-	✓
SR-IOV function	-	59-7X or later	-	79-7X or later

❑ Expanding the number of shared NICs/virtual NICs

This function can assign up to 16 NICs including shared NICs and virtual NICs to an LPAR.



(1) This function is available only with LPAR manager expansion mode. With LPAR manager standard mode, LPAR manager system memory is increased by 256 MB, which reduces the memory available for the user by 256 MB.

(2) Make sure to deactivate all LPARs before changing LPAR manager operating modes: changing from LPAR manager standard mode to LPAR manager expansion mode, or from LPAR manager expansion mode to LPAR manager standard mode. When you select Yes to “Save LPAR manager configuration and reboot LPAR manager system. Do You Continue? ”, LPAR manager will be automatically rebooted.

(3) When LPAR manager expansion mode is changed to LPAR manager standard mode, assignment of virtual NICs 8 to 15 will be forcibly initialized, which cancels all assignment.

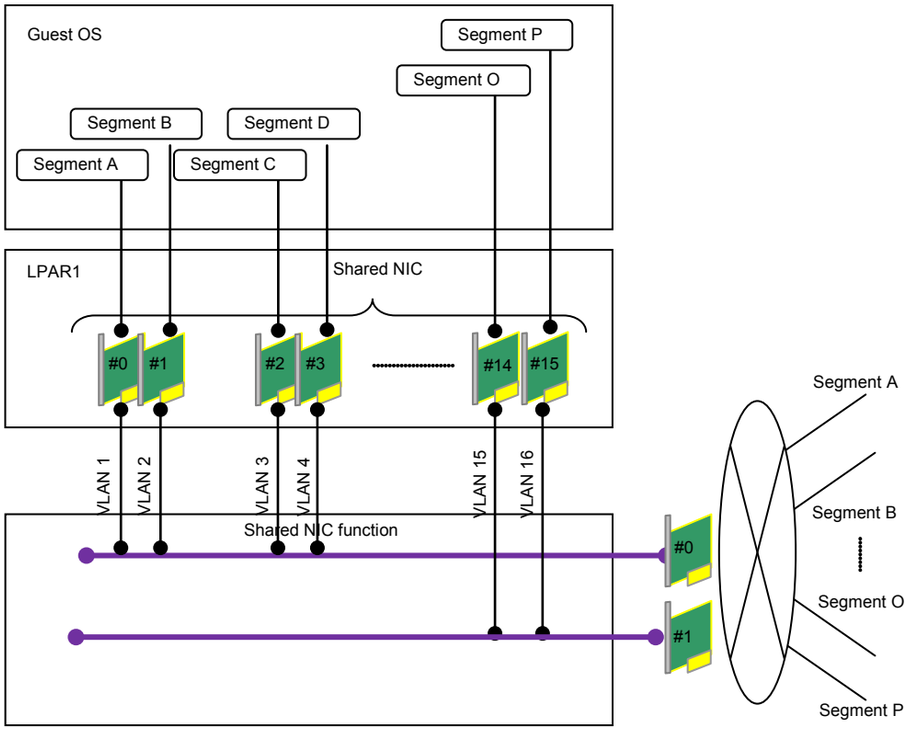
(4) You can configure this setting with the LPAR manager screen, HvmSh command, or HVM Navigator.

(5) Version downgrade by switching LPAR manager firmware banks is not supported.

(6) In LPAR migration, an LPAR cannot migrate to LPAR manager in the different operating mode.

❑ Assigning a NIC port respectively to an LPAR

This function can assign a physical NIC port to an LPAR duplicately. More numbers of segments than that of physical NICs can be configured, which brings advantages to the system with a few NICs installed. Up to 16 shared NICs can be available when together with the function of expanding the number of shared NICs/virtual NICs.



(1) You can bind shared NICs into a physical NIC port in any combination as long as within the specified number of shared NICs and that of physical NICs.

(2) This function is available only with LPAR manager expansion mode. With LPAR manager standard mode, LPAR manager system memory is increased by 256 MB, which reduces the memory available for the user by 256 MB.

(3) Make sure to deactivate all LPARs before changing LPAR manager operating modes: changing from LPAR manager standard mode to LPAR manager expansion mode, or from LPAR manager expansion mode to LPAR manager standard mode. When you select Yes to “Save LPAR manager configuration and reboot LPAR manager system. Do You Continue? ”, LPAR manager will be automatically rebooted.

(4) The setting for assigning a segment duplicately can be available in LPAR manager expansion mode, while a segment is assigned not duplicately in LPAR manager standard mode.

(5) When you have assigned a segment duplicately in LPAR manager expansion mode, the settings remains even if the mode is changed to LPAR manager standard mode. To disable the duplicate assignment setting, cancel it with the Virtual NIC Assignment screen and then set the shared NIC again.

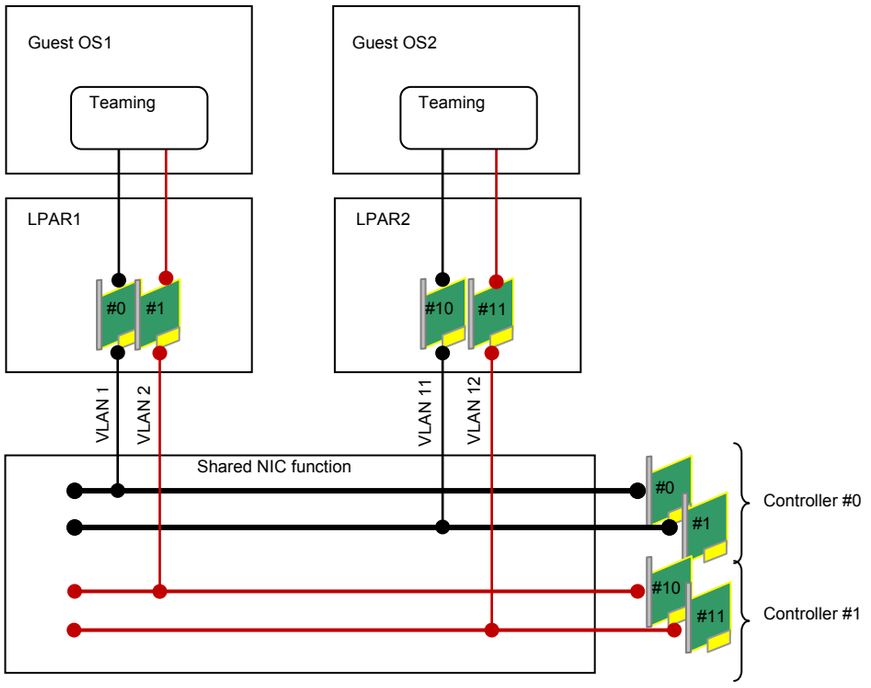
(6) You can configure this function with the LPAR manager screen, HvmSh command, or HVM Navigator.

(7) Version downgrade by switching LPAR manager firmware banks is not supported.

(8) In LPAR migration, an LPAR cannot migrate to LPAR manager in the different operating mode.

❑ Assigning NIC ports belonging to a controller individually

This function can assign physical NIC ports to an LPAR by the port. Dividing the physical controller for use can improve the guest OS availability.



(1) Shared mode and dedicated mode per port cannot coexist on a single controller.

(2) This function is available only with LPAR manager expansion mode. With LPAR manager standard mode, LPAR manager system memory is increased by 256 MB, which reduces the memory available for the user by 256 MB.

(3) Make sure to deactivate all LPARs before changing LPAR manager operating modes: changing from LPAR manager standard mode to LPAR manager expansion mode, or from LPAR manager expansion mode to LPAR manager standard mode. When you select Yes to “Save LPAR manager configuration and reboot LPAR manager system. Do You Continue? ”, LPAR manager will be automatically rebooted.

(4) A definition per port is provided with LPAR manager expansion mode; with LPAR manager standard mode, a definition per controller is provided.

(5) When you have defined a segment by the port in LPAR manager expansion mode, the settings remains even if the mode is changed to LPAR manager standard mode. To disable the definition by the port, cancel it with the Virtual NIC Assignment screen and then set the shared NIC again.

(6) You can configure this function with the LPAR manager screen, HvmSh command, or HVM Navigator.

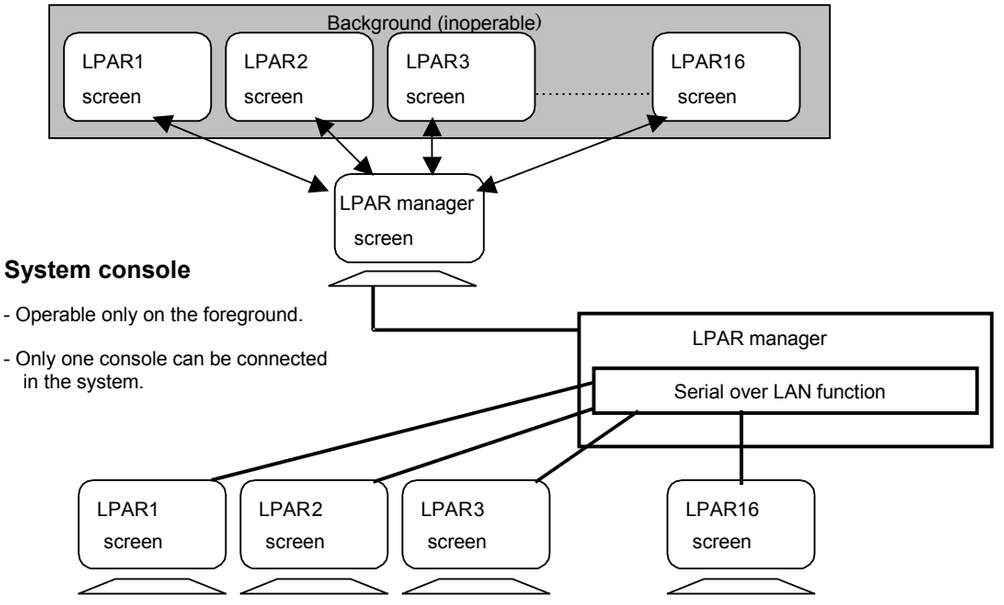
(7) Version downgrade by switching LPAR manager firmware banks is not supported.

(8) In LPAR migration, an LPAR cannot migrate to LPAR manager in the different operating mode.

Virtual COM console function

❑ Overview of Virtual COM console function

The conventional system console can select and operate one of the LPAR manager screens and guest screen. The virtual COM console can use a higher-speed console than the normal serial console for each LPAR with the serial over LAN function of the LPAR manager. Concurrent operation of multiple LPARs enabled the operating guest screens by using the virtual COM console instead of the system console. Up to 16 LPARs can be simultaneously connected to the virtual COM console.



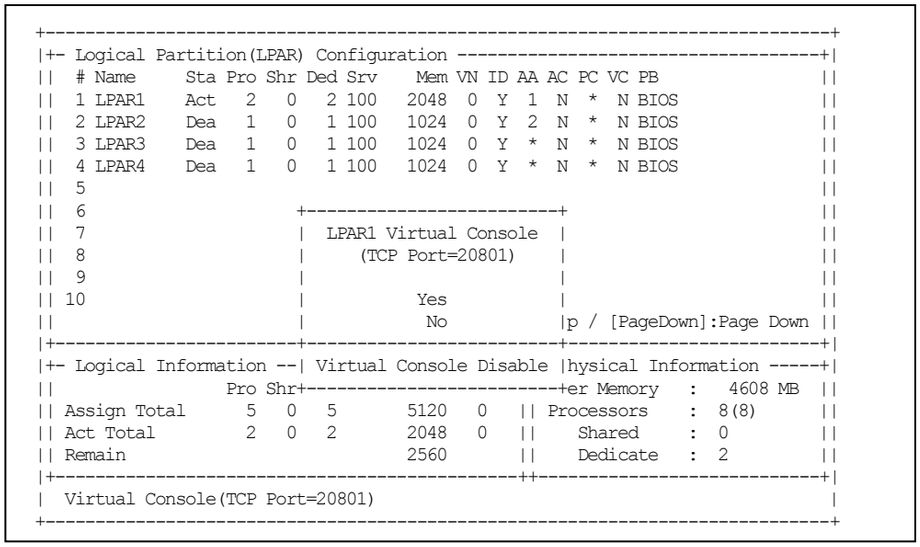
Virtual COM console

- Multiple LPARs can be operated
- One console can be connected for each LPAR.

Using Virtual COM consoles

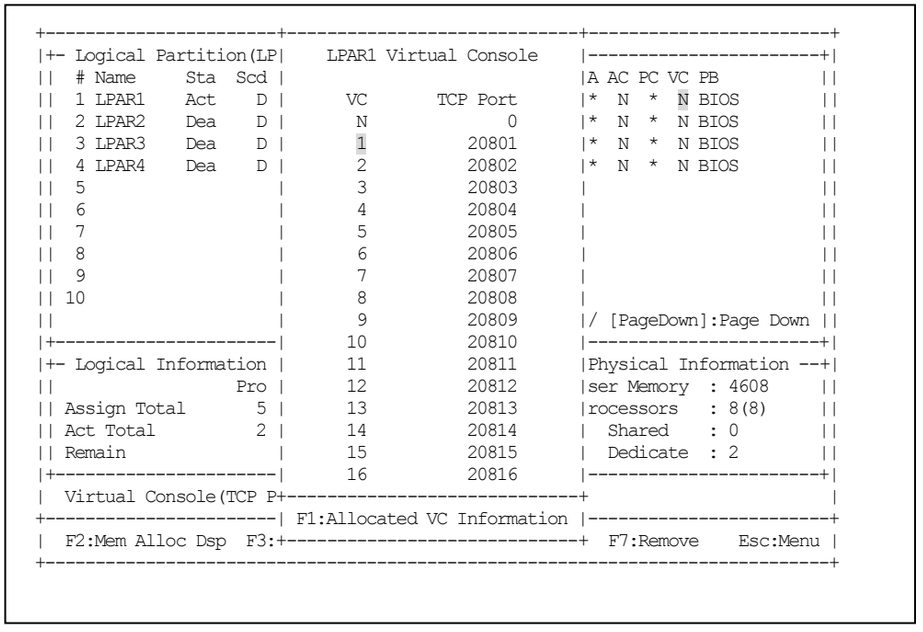
(1) Enabling Virtual COM console functions from the LPAR manager screen

Enable the virtual COM console function of LPARs on the Logical Partition Configuration screen in the LPAR manager screen. Position the cursor at the **VC** column in the LPAR line where the virtual COM console function is to be enabled, and then press **Enter** to open the sub-screen. Move the cursor with the arrow key [↑] or [↓], select **Yes** and then press **Enter**. This procedure allows the Telnet connection to the LPAR guest screen. TCP port used for Telnet connection is displayed in one of the following: 1. In a comment shown when the cursor is positioned at the VC column in the LPAR line; 2. In a subscreen shown when **Enter** is pressed with the cursor positioned at the VC column in the LPAR line. This TCP port is used in “(2) Connection to LPARs.” This operation is always available regardless of whether LPARs are active or inactive.



High-performance server blade with LPAR manager firmware version 78-4X or later versions

You can enable the virtual COM console for LPARs on Logical Partition configuration screen of LPAR manager screens. Place the cursor on the VC column of an LPAR line which you need to enable the virtual COM console, and press the **F1** key to display a subscreen. Select a VC number to connect by moving the cursor with arrow keys, [↑] or [↓], and press **Enter**. This allows you to connect to the LPAR guest screen via telnet. A TCP port is displayed, which is used to connect to Comment when you place the cursor the VC column of the LPAR line via telnet. This TCP port is used in “(2) Connecting to LPARs”. This operation can be done regardless of the status of an LPAR, active or deactive, at any time.



(2) Connecting to LPARs

To connect to LPARs, specify the TCP ports allocated to each LPAR, and make a Telnet connection to the IP address of the LPAR manager. TCP ports with a serial number starting from 20801 are allocated sequentially to LPAR1 to LPAR16 in the initial , which can be changed in “(4) Changing TCP Ports.” Currently allocated TCP ports can be checked in “(1) Enabling Virtual COM Console Function on the LPAR manager Screen. When using a virtual COM console, use terminal software as OS console. When using one or more virtual COM consoles, use Tera Term as in the case of the system console. Furthermore, for stable operation of Tera Term, it is recommended that the Scroll Buffer value be set to 2000 lines on the screen displayed by clicking **Settings(S) > Window(W)**.

1. On the **New Connection** screen at the boot of **Tera Term**, enter the LPAR manager IP address and TCP port. Then click **OK**.
2. The OS prompt will appear when the connection is successful. This is where you can operate the guest OS.
3 If the connection fails, a popup message informing “Error” will be displayed. Connection failures are as follows:

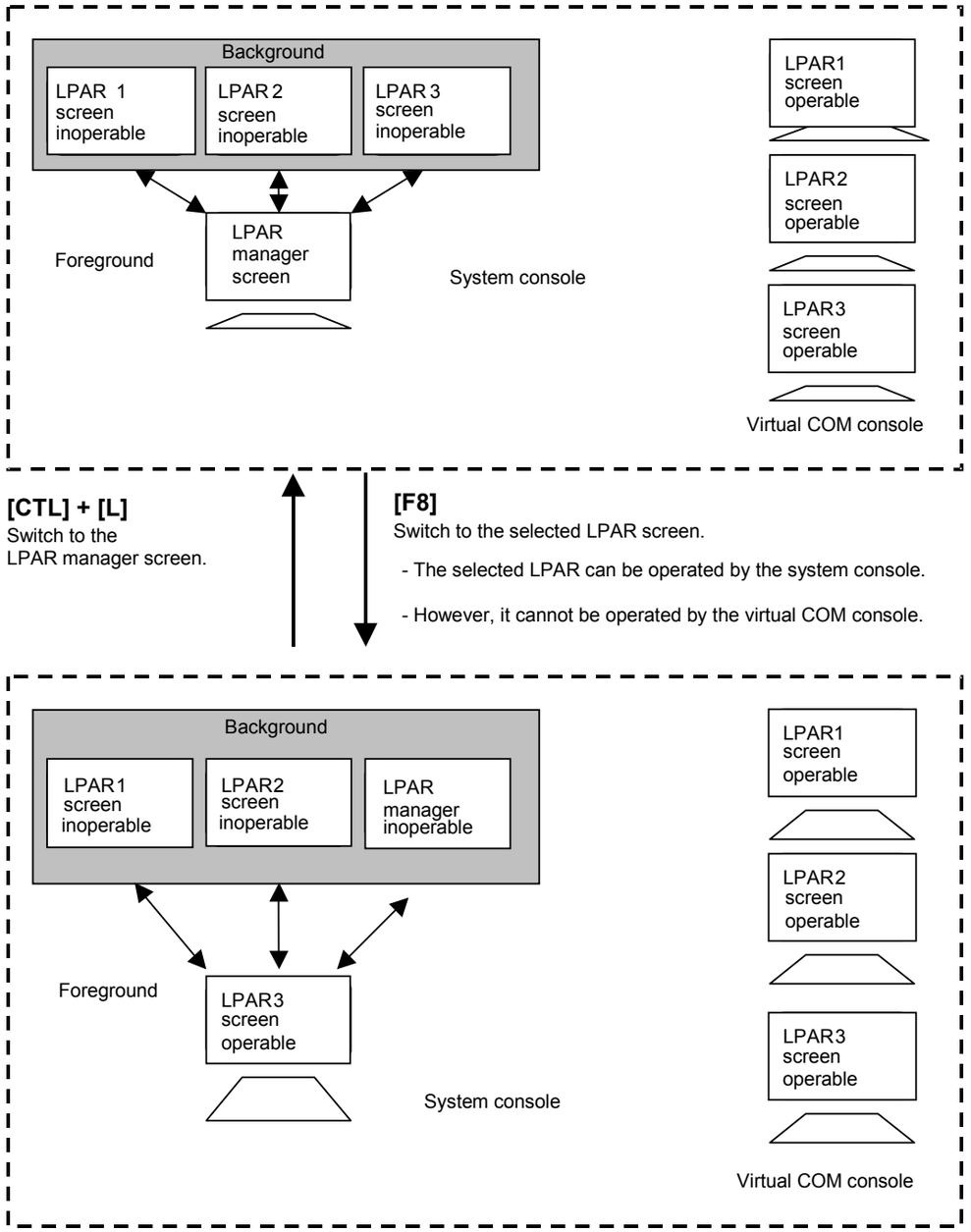
- TCP/IP communication to the LPAR manager IP address is unavailable. Check the path to the LPAR manager IP address.

- If changing a TCP port, the TCP port might not be connected depending on the terminal OS setting or account privilege. Confirm that the TCP port is available for connection on the terminal before changing a TCP port. It is recommended to use a TCP port with the default value that is verified enough.

- When trying to connect two or more terminals to one LPAR, the second terminal or later terminal cannot be connected.

(3) Switching the Virtual COM console and system console

The LPAR guest screens can be operated from either virtual COM console or conventional system console. These two types of consoles are exclusively available and operation by the conventional system console takes precedence. The virtual COM console can operate LPAR guest screens while the system console is displaying the LPAR manager screen. Consoles to operate LPAR guest screens can be selected by switching an LPAR guest screen and the LPAR manager screen on the system console.



(4) Changing TCP Ports

A TCP port to be specified when making a Telnet connection to an LPAR guest screen is set to the initial value determined by the LPAR manager during its startup procedure. This TCP port can be changed on the System Configuration screen, but we recommend that the initial value determined by the LPAR manager be used.

❑ Notes

(1) Notes on Telnet Connection

- You can change a port number to specify when connecting to a guest screen via Telnet, which needs to be different from a port number for LPAR manager. See Port numbers used by LPAR manager for details. Some port numbers may not be available depending on the OS settings, account privilege, installation software, or network environment. Check which port is available on the terminal and in the network environment before changing the port number. When there is no problem for use, it is recommended that you use a default port number among serial numbers starting from 20801 that have been thoroughly verified.
- Only one terminal per LPAR is permitted to operate guest screens from the virtual COM console. If a connection to two or more terminals is attempted, the connection to the second or additional terminals is disabled.
- If the screen shows nothing when connected to the virtual COM console, check the settings for the serial console.

(2) Notes on Guest Screen Operation

- Although the virtual COM console can operate multiple LPARs concurrently, the performance of consoles of other LPARs might decrease with an increase in output data. For this reason, operation with text data output of several hundreds of lines per second should not be performed simultaneously to three or more LPARs.
- If a large amount of characters are pasted to a guest screen, a part of characters might not be pasted. 256 or more characters per line for the Windows command prompt, and 1024 or more characters per line for Linux prompt cannot be pasted. In addition, if 1024 or more characters are pasted for the Linux prompt, Linux might hang up or unexpected screen operation might occur. The number of characters that can be pasted without being lost is less than 256 per line for the Windows command prompt, less than 1024 per line for the Linux prompt, and less than 10000 per line for editing programs including the Vi editor. When pasting characters, it is recommended that a large amount of characters be divided into several blocks (up to the upper limit of characters per block), and then be pasted.
- When you connect the system to the virtual COM console and boot the guest OS, Windows might halt its boot with the EFI screen; Linux might halt its boot in the grub console - though rarely. If it happens, press **Enter** to resume the boot.

(3) Notes on Operation

- Connect to the virtual COM console as necessary, and do not stay connected to it because input and output operation might halt. If this happens, re-connect the virtual COM console. We recommend that VC (virtual COM console) on the Logical Partition Configuration screen should be assigned to an LPAR when needed and the assignment should be released when not needed.
- If you repeatedly change settings for VC (virtual COM console) on the Logical Partition Configuration screen with the virtual COM console connected, the console screen might be disturbed. If so, perform **Edit (E) > Screen clear (S)** in TeraTerm to clear the screen, which can correct the screen disturbance.

Logical VGA snapshot

See *Hitachi Compute Blade Logical VGA SnapShot* for Logical VGA snapshot functions.

Cooperation with ServerConductor

Using ServerConductor, you can manage the virtualized logical server by LPAR manager as a physical server.

See the *ServerConductor* manual for the details.



- While LPAR manager is processing a request from SeverConductor, operation on the LPAR manager screen is not available. For further details, see Notifying that requests from an external management console are being processed.
- When using ServerConductor/Deployment Manager, make sure to set PXE boot (network boot). For further details, see Setting the extensible firmware interface (EFI) driver and Creating Boot Options.

Guest memory dump function

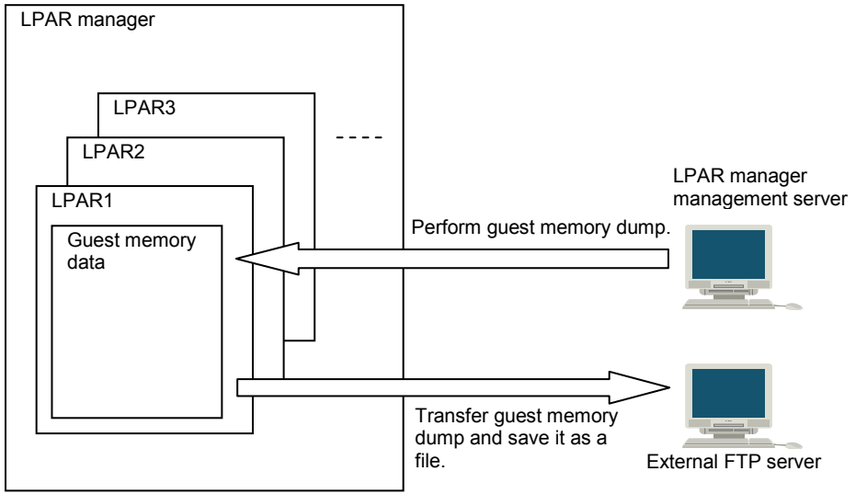
❑ Overview of guest memory dump function

(1) Overview

The guest memory dump function saves memory data as a file by executing the HVM Management Command (HvmSh) on the LPAR manager management server. The function collects memory data (memory dump) allocated to the specified guest (LPAR) on the LPAR manager side by executing HvmSh. Then it transfers the collected data to the external File Transfer Protocol (FTP) server to save it as a file.

This function allows memory dump even if a logical server error occurs, such as when OS dump data cannot be collected by the guest OS, and can be used for analyzing logical server errors.

The figure below shows a schematic diagram of the guest memory dump function.



(2) Details of support

The following table lists support items provided by the guest memory dump function.

No.	Item		Description
1	Dump target guest		LPAR's memory dump is enabled regardless of the type of guest OS.
2	User operation means		The guest memory dump collection command as an HVM management command is executed on the LPAR manager management server.
3	Dump output server		External FTP server specified by the guest memory dump collection command (The server that executes the guest memory dump collection command is also available.)
4	Dump data transfer method		Memory dump data are transferred from the LPAR manager machine to the external FTP server through the management LAN. Dump data file is created by the LPAR manager machine, and the file is transferred to the external FTP server using the FTP protocol.
5	Dump data format		The dump data format conforms to the Niko2Dump format.
6	Dump output file format		Binary format file of dump data based on the dump data format above
7	Dump output filename		gmdP#L#-YYMMDD-hhmmss-nnn.dat (Note) P#: Partition number: P0 to P7 L#: LPAR number: L01 to L60 YYMMDD: Collection date (in the order of year (2 digits), month (2 digits), and day (2 digits)) hhmmss: Collection time (24-hour notation in the order of hour (2 digits), minute (2 digits), and second (2 digits)) nnn: Serial number for file division with the unspecified number of digits (In the case of two digits or less, '0' is not attached at the high-order digits.) The LPAR manager's system time is used for collection date and time.
8	Command functions	Input information	Enter the following information when executing the guest memory dump start command. ・LP IP address ・Number of LPAR from which guest memory dump data is collected ・IP address of the external FTP server ・User ID of the external FTP server ・Password of the external FTP server ・Dump output file directory path of the external FTP server (specified directory path under FTP) Note: If a user ID or password contains a symbol, dump collection might fail.
9		Start operation	Starts memory dump. To prevent memory data from being rewritten during memory dump, all logical CPUs of the target LPAR stop automatically upon the start of memory dump, and remain inactive even after the memory dump is completed.
10		Stop operation	Stops memory dump. All the logical CPUs that were stopped by the start operation do not restart automatically, and still remain inactive.
11		Progress indication	The following contents of memory dump progress are displayed on the screen. ・Total volume, transferred data volume, and transfer percentage (transferred data volume / total volume × 100 (%))

No.	Item	Description
12	Memory dump region	The following three regions used by the OS are provided for memory dump within the memory area allocated to the target LPAR (No memory area in the LPAR can be specified.) DOS region: 00_0000_0000 to 00_0009_FFFF Low memory: 00_0010_0000 to 00_7FFF_FFFF High memory: 01_0000_0000 to MMCFG - 1 (Note) These regions are the same as those for Niko2Dump of Basic.
13	Maximum concurrent collection	One LPAR / LPAR manager machine (Another dump data collection request to the same LPAR manager machine cannot be accepted during memory dump even to another LPAR of the same LPAR manager machine.)
14	Condition for data collection	Memory dump data can be collected only when the target LPAR is activated.
15	Guest software operation	The guest memory dump function works as follows in relation to the guest software program: ・Memory dump data can be collected regardless of the operation of the guest software program (even when it can no longer operate due to an error during operation).

(3) Recommended FTP server

We recommend the following combinations of OSs and software programs providing the FTP server function as an external FTP server. If there is any combination other than those specified, the operation is not guaranteed.

OS	Software providing the FTP server function
Windows Server 2003	IIS 6.0
Windows XP Professional	IIS 5.1
Red Hat Enterprise Linux 4.5	vsftpd
Red Hat Enterprise Linux 5.1	vsftpd

❑ How to use the guest memory dump function

For the basic usage of HVM management commands that are essential when using the guest memory dump function, see the *HVM Management Command (HvmSh) User's Guide*. For how to use commands related to the guest memory dump function in HVM management commands, see "Starting Guest Memory Dump," "Stopping Guest Memory Dump," and "Acquiring Guest Memory Dump Progress" in the "LPAR manager Interface Individual Specifications" of the *HVM Management Command (HvmSh) User's Guide*.

❑ Precautions

Follow the precautions described below when using the guest memory dump function.

- After guest memory dump is started, all logical CPUs of the target LPAR stop, and logical server processing is not restarted. For this reason, use this function only when logical server processing can no longer be continued (such as when a logical server error has occurred).

- Therefore, if guest memory dump is started in the target LPAR during job processing, all the logical CPUs of the target LPAR stop, and the ongoing job stops accordingly. This is equivalent to a breakdown of the target LPAR that will occur when guest memory dump of the LPAR is started during job processing. For this reason, do not perform guest memory dump to a working LPAR.
- If “Deactivate” operation, “Reactivate” operation or logical server movement operation is performed to the target LPAR during guest memory dump, the operation takes precedence and the guest memory data is not retained. Therefore, guest memory dump can no longer be continued and the guest memory dump is cancelled. When guest memory dump is in progress, do not perform “Deactivate” operation, “Reactivate” operation, or logical server movement operation to the target LPAR.
- LPARs other than the target LPAR continue to work after guest memory dump is started, but those that use the LPAR manager management NIC as shared NIC might be affected as its network performance degrades.
- If Force Recovery is performed on the System Service State screen of the LPAR manager screen during guest memory dump, the memory dump operation is cancelled.
- If Update System Config is performed with the F10 key on the System Configuration screen of the LPAR manager screen during guest memory dump, the memory dump operation is cancelled.
- If the processing to automatically stop all logical CPUs of the target LPAR fails at the beginning of guest memory dump, the memory dump operation is cancelled and the target LPAR is deactivated forcibly. If this deactivation fails, the target LPAR is blocked. When this state occurs, contact the maintenance personnel.
- If an unrecoverable error occurs during guest memory dump in the LPAR manager machine that performs guest memory dump, the memory dump operation is cancelled. When this state occurs, contact the maintenance personnel.
- If an LPAR manager Assist error occurs during guest memory dump, the memory dump operation might be cancelled. When this state occurs, contact the maintenance personnel.
- If a communication error occurs in the network between LPAR manager machine and external FTP server during guest memory dump, the memory dump operation is cancelled. When this state occurs, check the network configuration between LPAR manager machine and external FTP server. If the problem is still not solved, check whether the FTP software program of the external FTP server is running correctly. If the problem still remains, contact the reseller from which you purchased this equipment or consult maintenance personnel.
- When guest memory dump processing and guest OS dump processing by the Dump operation on the Front Panel screen are performed simultaneously to one LPAR, all the logical CPUs of the LPAR stop due to guest memory dump and the guest OS processing stops accordingly. Therefore, the guest OS dump operation on the Front Panel screen is disabled, but the guest memory dump is enabled. Remove this precaution with the following operational procedure:

  1 When you find an abnormal operation of the guest OS and dump the guest memory data, perform guest OS dump first by the Dump operation on the Front Panel screen

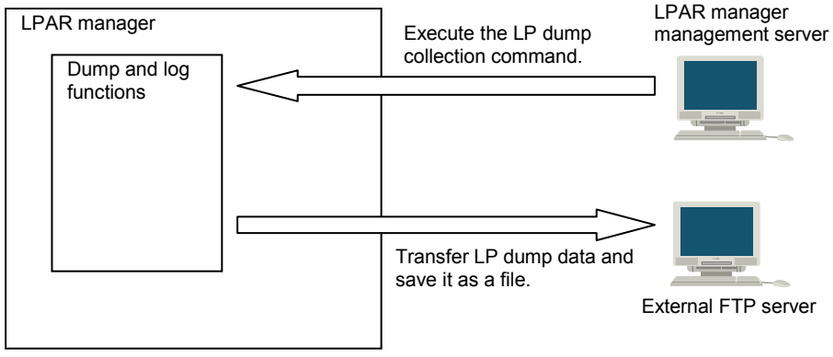
  2 If this guest OS dump operation fails, perform the guest memory dump using the guest memory dump function.

LPAR manager dump collection command

❑ Overview of LPAR manager dump collection command

(1) Overview

The LPAR manager dump collection command is included in HVM Management Command (HvmSh). When the LPAR manager dump collection command is executed on the LPAR manager management server, the LPAR manager performs LPAR manager dump and transfers the collected dump data to the external FTP server specified in the LPAR manager dump collection command to save it as a file. The figure below shows when the LPAR manager dump collection command is executed.



(2) Details of support

The following table lists support items provided by the guest memory dump function.

No.	Item	Support
1	Dump volume	Up to 16 MB
2	User operation means	The LPAR manager dump collection command is executed on the LPAR manager management server.
3	Dump output server	External FTP server specified by the LPAR manager dump collection command. (The server that executes the LPAR manager dump collection command is also available.)
4	Dump data transfer method	Memory dump data is transferred from the LPAR manager machine to the external FTP server through the management LAN. The LPAR manager dump data are compressed, and a GZIP file is created by the LPAR manager machine. The file is transferred to the external FTP server using the FTP protocol.
5	Dump data format	Same as the existing LPAR manager dump format
6	Dump output file format	GZIP format. Two files (two blocks of dump data) with the existing dump header (128 bytes) attached to the head of the GZIP-compressed data are output.
7	Dump output file name	First-block dump file: hvmdump-yyyymmdd-hhmmss-01 Second-block dump file: hvmdump-yyyymmdd-hhmmss-02 (Note) yyyymmdd: Collection date (in the order of year (4 digits), month (2 digits), and day (2 digits)) hhmmss: Collection time (in the order of hour (2 digits), minute (2 digits), and second (2 digits)) Collection date and time are the same for the first and second blocks.

No.	Item	Support
8	User input information	Enter the following information when executing the LPAR manager dump collection command. ・LP IP address ・IP address of the external FTP server ・User ID of the external FTP server ・Password of the external FTP server ・Dump output file directory path of the external FTP server (specified directory path under FTP) Note: If a user ID or password contains a symbol, dump collection might fail.
9	Maximum concurrent collection	1 (Another dump data collection request to the same LPAR manager machine cannot be accepted during memory dump operation.
10	Condition for data collection	Except for the notes described later, LPAR manager dump is always enabled.

❑ How to use the LPAR manager dump collection command

For the basic usage of HVM management commands that are essential when using the LPAR manager dump collection command, see the *HVM Management Command (HvmSh) User's Guid*e. For how to use the LPAR manager dump collection command, see "Collecting LPAR manager dump data" in "LPAR manager Interface Individual Specifications" in the *HVM Management Command (HvmSh) User's Guide*.

❑ Notes

Consider the following when using the LPAR manager dump collection command.

- While LPAR manager dump is performed by the LPAR manager dump collection command, any other LP dump operation on the LPAR manager screen is disabled.
- While LPAR manager dump is performed by the operation on the LPAR manager screen, LPAR manager dump by the LPAR manager dump collection command is disabled.
- If an unrecoverable error occurs during the LPAR manager dump in the LPAR manager machine that performs the LPAR manager dump, the LP dump operation is cancelled. When this state occurs, contact the maintenance personnel.
- If a communication error occurs in the network between the LPAR manager machine and external FTP server during LPAR manager dump, the LP dump operation is cancelled. When this state occurs, check the network configuration between LPAR manager machine and external FTP server. If the problem is still not solved, check whether the FTP software of the external FTP server is running correctly. If the problem still remains, contact the reseller from which you purchased this equipment or consult maintenance personnel.

HVM Management Command

The HVM management command, HvmSh command, can execute the LPAR manager operation from the Windows command line that is executed on the LPAR manager screen. With this command, you can obtain the LPAR manager system information from the remote system, or set the LPAR configuration from programs such as script.

For details, see the *HVM Management Command (HvmSh) Operation Guide*.

Command for obtaining an overview of system operation

❑ Outline of the command for obtaining an overview of system operation

The command for obtaining an overview of system operation, HvmGetPerf, obtains statistics collected by the LPAR manager. Statistics information includes the LPAR manager execution time, busy ratio, LPAR execution time and service ratio, which can be referenced on the LPAR Usage screen. This command allows a remote system to obtain the operating status of the LPAR manager system or LPAR or scripting or other program to obtain that information.

The HvmGetPerf command can obtain the following performance statistics:

(1) Service ratio and service time for each LPAR

(2) Execution time and busy ratio for each LPAR

(3) Number of dedicated and shared processors for each LPAR

(4) Logical processor usage time for each LPAR

(5) Physical processor usage ratio

(6) Execution time and busy ratio for the LPAR manager system

The HvmGetPerf command obtains the latest values of performance statistics collected in a second.

It supports a summary output format for higher legibility and a text format that is easy for other programs to handle.

❑ Installing the HvmGetPerf command

The HvmGetPerf command is provided as an executable command on the command prompt of Windows Server 2003, Windows server 2008, Windows XP, and Windows VISTA. The HvmGetPerf command can be used from a management server to which BSM1 to 4 IP Address or LP CLI1 to 8 IP Address is set on the System Configuration screen.

The HvmGetPerf command is stored in the Compute Blade 2000 HVM Utility CD. To use the command, copy the HvmGetPerf command to the directory where the HvmGetPerf command execution path of the management server is set.

The command cannot be used from a management server to which BSM address or CLI IP address is not set. Set the IP address to the management server with BSM command of SVP command mode or System Configuration screen.

SC/BSM needs to operate on the management server to which the BSM IP Address is set .

❑ Using the HvmGetPerf command

The HvmGetPerf command obtains an overview of system operation from the specified LPAR manager and outputs the results to the specified destination. It can also output information for a specific LPAR only.

If it cannot connect to the specified LPAR manager, it terminates by time-out.

Execute the HvmGetPerf command as follows: (Δ indicates a space.)

HvmGetPerfΔ-host=*Ip-address*[Δ–type=*item-to-be-obtained*]
[Δ–lpar=*LPAR-number*] [Δ–filename=*output-destination-file-name*]
[Δ-timeout=*timeout-time*] [Δ-srcip=*IP address*]:

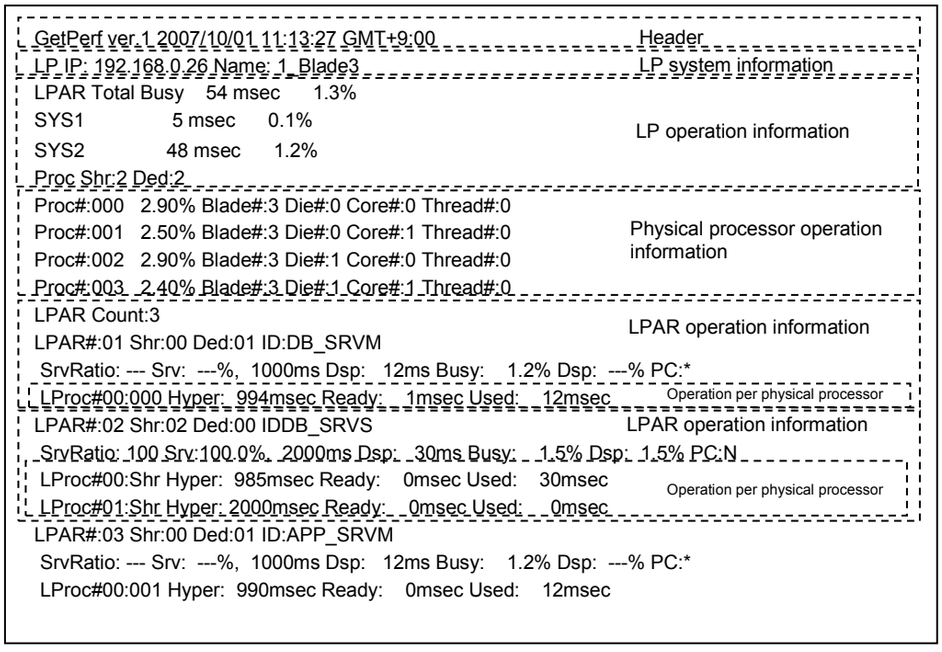
The following table describes options for the HvmGetPerf command.

Option	Description
-host=IP-address	Specify the IP address of the LPAR manager to obtain an overview of operation. Specify an address in dot-delimited decimal format (“.”). This parameter is required. Example: 192.168.0.20
-type=item-to-be-obtained	Specify the item to obtain an overview of operation. The following values can be specified. all Obtains all operation overview items. host Obtains an operation overview for the LPAR manager system. pcpu Obtains an operation overview for the physical CPU. lpar Obtains an operation overview for the LPAR. If this option is omitted, the command obtains all operation overview items.
-lpar=LPAR-number	Specify the LPAR to obtain an overview of operation using an integer value. If this option is omitted, the command outputs information for all LPARs.
-filename=output-destination-file-name	The command outputs an overview of operation in text format to the specified file. If the specified file exists, the contents of the file are erased and overwritten with the operation outline information. If a minus sign (-) is specified as the destination, the command outputs an overview of operation to the standard output. If the -filename parameter is omitted, the command outputs operation overview information in summary format to the standard output.
-timeout=timeou-ttime	Specify the time the command times out if it cannot connect to the LPAR manager, in the range from 1 to 3600 seconds. If this option is omitted, the command will time out in three seconds. If 0 is specified, the HvmGetPerf command never times out and infinitely waits for a response from the LPAR manager.
-srcip=IP address	Specify the IP address on the management server, a source address, which is used for communication with LPAR manager. This setting is required for fixing an IP address for HvmGetPerf command when the management server uses the IP address in the network configuration, where the server is connected to multiple segments. HvmGetPerf: 1.5 or later versions

❑ Output in summary format

If the filename option is omitted, the HvmGetPerf command outputs a system operation overview in summary format. The following figure shows an example output in summary format.

This section uses the output example of the IPF version LPAR manager.



The table below describes the information items output in summary format.

Output item	Description	Type option
Header	Outputs the command version and the time the operation overview was output.	Always
LPAR manager system information	Outputs the IP address and identifier of the target LPAR manager.	all host
LPAR manager system operation information	Indicates the operating status of the LPAR manager system. It shows execution times and busy ratios for all LPARs and LPAR manager system as well as the numbers of shared and dedicated CPUs assigned.	all host
Physical processor operation information	Indicates the operating status of the physical processors mounted in the LPAR manager system. It shows the busy ratio and the mounting location of each processor.	all pcpu

Output item	Description	Type option
LPAR operation information	Indicates the number of LPARs defined and the settings and operating status for each defined LPAR. The LPAR Count line at the top displays the number of LPARs defined. As definition information for each LPAR, the LPAR number, number of shared CPUs (Shr), number of dedicated CPUs (Ded) and LPAR name (ID) are output. As operation information for each LPAR, the same information as that shown in the LPAR Usage screen is displayed for SrvRatio, Srv(%), Dsp(ms), Busy(%), Dsp(%) and PC. Logical processor information defined for each LPAR is output. It includes the logical CPU number, whether it is dedicated or shared (Shr or the number of a dedicated physical processor), LPAR manager execution time (Hyper), running wait time (Ready) and LPAR execution time (Used). If the -lpar option specifies LPAR, the command outputs information only for the specified LPAR. If the -lpar option is omitted, the command outputs information for all LPARs defined. For inactive LPARs, the corresponding information field shows "---" and does not show information for each logical CPU.	all lpar

The summary format output shows information equivalent to that shown in the LPAR Usage screen. For details of data, see description in LPAR usage.

❑ Output in text format

The following figure shows an example of output in text format.

```
LP_192168020 192.168.0.20 55 1.3 12 0.3 48 1.2 2 2          LP system information
0 3.60 3 0 0 0
1 2.60 3 0 1 0                                              Physical processor information
2 3.00 3 1 0 0
3 2.30 3 1 1 0
4 * 0 0 0 0
5 * 0 0 0 0
(Omitted in the middle.)

1 DB_SRVM 0 1 * * 1000 12 1.2 * 2                           LPAR information
2 DB_SRVS 2 0 100 100.0 2000 31 1.5 21 1
3 APP_SRVM 0 1 * * 1000 12 1.2 * 2
4 * 0 0 0 0.0 0 0 0.0 0 0
(Omitted in the middle.)

1 0 0 1002 4 12
1 1 * 0 0 0                                                 LPAR1
(Omitted in the middle.)                                    Logical processor information
2 0 * 992 0 31
2 1 * 1000 0 0                                              LPAR2
(Omitted in the middle.)                                    Logical processor information
3 0 1 994 1 12
3 1 * 0 0 0
(The rest is omitted.)
```

The following table describes the information items output in text format.

Output item	Description	Type option
LPAR manager system information	Indicates the operating status of the entire LPAR manager. It shows the identifier of the target LPAR manager, LP IP address, total execution time for all LPARs, total busy ratio for all LPARs, execution time for LPAR manager System1, busy ratio for LPAR manager System1, execution time for LPAR manager System2, busy ratio for LPAR manager System2, number of shared CPUs and number of dedicated CPUs, in the stated order. Execution times are displayed in millisecond units.	all host
Physical CPU information	For each physical CPU mounted on the LPAR manager system, outputs the physical CPU number, busy ratio, blade number, socket number, core number and thread number, in the stated order. Information for the maximum number of installable CPUs is displayed, regardless of the number of installed CPUs. For CPUs not mounted, the busy ratio is shown as "*" and other items shown as 0.	all pcpu
LPAR information	Indicates the operating status for each LPAR. It shows the LPAR number, LPAR name, number of shared CPUs, number of dedicated CPUs, SrvRatio, Srv(%), Srv(ms), Dsp(ms), Busy(%), Dsp(%) and PC (processor capping) in the stated order. For details of each value, see description in LPAR usage. For PC, a value of 0 indicates a shared CPU with processor capping, 1 indicates a shared CPU without processor capping and 2 indicates a dedicated CPU. Information for 16 LPARs is displayed regardless of whether the LPARs are defined. For LPARs not defined, the LPAR name is shown as "*" and other items shown as 0. If the -lpar option specifies an LPAR number, the command outputs information only for the specified LPAR.	all lpar
Logical CPU information for each LPAR	Indicates the operating status of the logical CPU assigned to the LPAR. It shows the LPAR number, logical CPU number, dedicated/shared, system execution time, running wait time and LPAR execution time, in the stated order. Time values are displayed in milliseconds. The dedicated/shared item displays the physical CPU number for a dedicated CPU or "*" for a shared CPU. Information for the maximum number of logical CPUs for which the LPAR can be set is displayed, regardless of whether or not the LPAR is defined and of the number of logical CPUs defined in the LPAR. For logical CPUs that were not running when information was obtained, the dedicated/shared item is shown as "*" and other items shown as 0. A CPU that is "not running" refers to a logical CPU for an undefined or inactive LPAR or a logical CPU that is not defined for an active LPAR. To determine whether each LPAR is defined or how many logical CPUs are defined, see the LPAR name, the number of shared CPUs, and the number of dedicated CPUs in LPAR information. If the -lpar option specifies an LPAR number, the command outputs information only for logical CPUs for the specified LPAR.	all lpar

❑ Example

The HvmGetPerf command obtains a system operation overview only once per execution. To obtain an overview of system operation for a long period of time, it is necessary to use a batch file or other program that executes the HvmGetPerf command periodically. The table below shows an example of a batch file.

```
@echo off
:logging
date /t >>log.txt
time /t >>log.txt
HvmGetPerf -host=192.168.0.26 -filename=- >> log.txt
ping localhost -n 5 > nul
goto logging
```

Save the above text file as a batch file (with an extension of .bat). When executed, the batch file executes the HvmGetPerf command at intervals of about five seconds and logs the command outputs in the log.txt file. In this example, the date and time of command execution precede the results of the HvmGetPerf command.

❑ Error message

If an error occurs during command execution, the following message is output to the standard error.

```
IPMIClient: [Client/LP/Server] Time: 2007/05/01 12:12:12 Return: 0xXXXXXXXX Message

[Client/LP/Server]            Indicates the error location.
                                        Client:     Error detected in command.
                                        LP, Server: Error detected in LP.
Time: 2007/05/01 12:12:12    Indicates the time the error occurred.
0xXXXXXXXX                      Indicates the command termination code.
Message                          Describes the error.
```

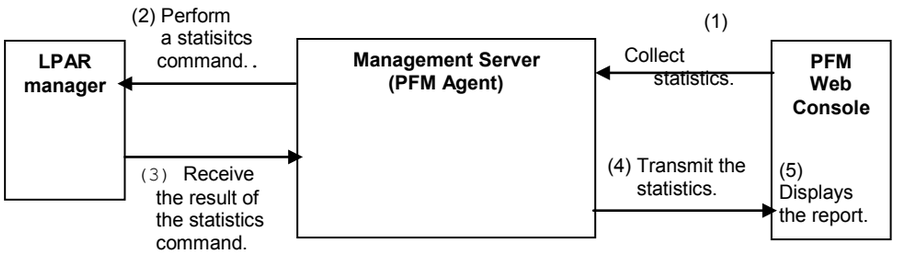
If an error occurs, the command process terminates with the termination code described in the message. In a Windows batch file, you can obtain the termination code by referencing the ERRORLEVEL environment variable immediately after executing the HvmGetPerf command.

The following table lists the errors contained in messages output by the command and the corresponding termination codes.

Error message and termination code	Description	Action
Invalid Option. 0x01010000	An invalid option is specified.	Check the command options.
Target Host Unreachable. 0x01020000	The specified host is not found.	Check that the specified address is correct and that the specified target host is operating normally.
Response Timeout. 0x01020001	The specified host has not responded.	Check that the specified address is correct and that the specified target host is operating normally.
Unknown Data Received. 0x01030000, 0x000000ce, 0x000000cc	Unexpected data has been received.	Check that the specified target host is operating normally.
failed to bind. 0x01030001	Network bind operation has failed.	Check the communication configuration. Alternatively, wait for a while and retry.
failed to activate session. 0x01030002	Failed to establish a communication session.	Check the number of SC/BSM devices concurrently connecting to the LPAR manager and whether other machines are executing the HvmGetPerf command simultaneously.
Cannot Write File or Given Too Long File Name. 0x01040000	Failed to write data to a file.	Check that the specified file is write-enabled. Alternatively, shorten the length of the filename.
Target LPAR is undefined. 0x04000000	The specified LPAR is not defined.	When using the lpar option, specify only a defined LPAR.
Unexpected Exception was raised. 0xffffffff	An internal error has occurred.	Check the command options, network conditions, and the operating status of the specified LPAR manager.
Invalid Command Received. 0x000000c1	The target host failed to accept the HvmGetPerf command.	Check whether the LP IP address is specified.

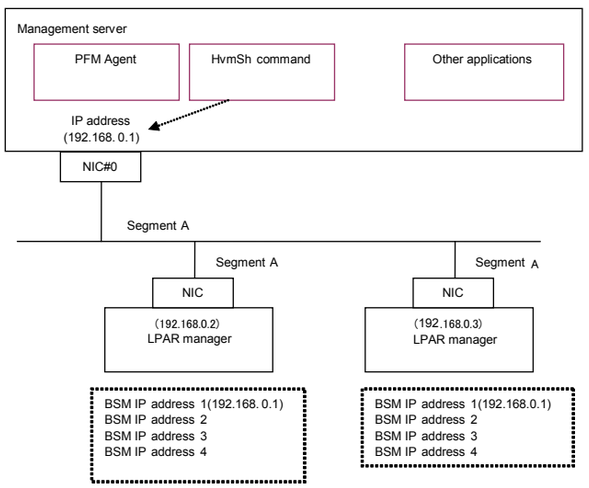
❑ Cooperation with PFM

Performing the HvmSh command from PFM allows you to collect LPAR manager statistics information and to show it as a report in a graphic form with Performance Management (PFM).

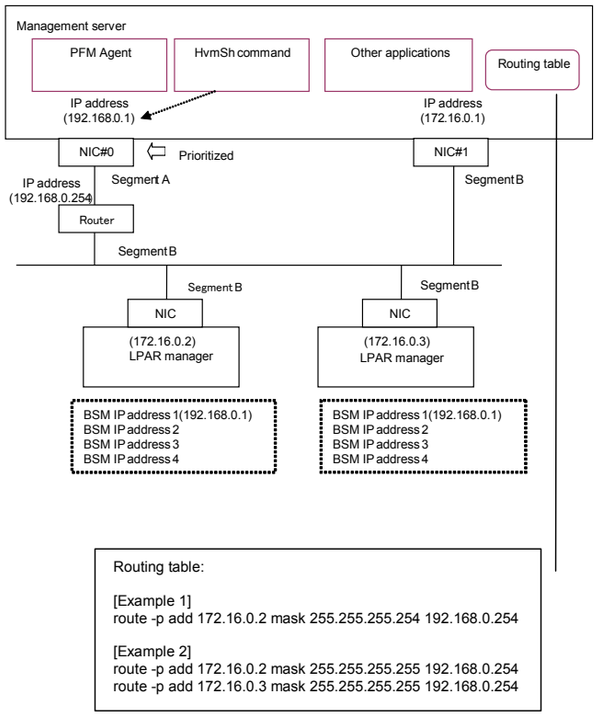


❑ Cooperation with HvmSh command

The HvmSh command is available from the management server, which is set to IP addresses of BSM1 to 4 or LP CLI1 to 8 on the system configuration screen. Set the IP address of the management server to the IP address of BSM1 to 4 or LP CLI1 to 8. The HvmSh command from a management server, which is set to neither BSM nor LP CLI IP address, will be ignored by LPAR manager. The management server needs to have PFM agent in operation.



In the network where the management server is connected to multiple segments, give priority to the NIC port on the management server that is used for the HvmSh command, and register the route on the routing table. Then, the registered route is used for all communication from the management server to LPAR manager.



To execute HvmSh command on PFM with the HvmSh command, copy the HvmSh command stored in the HVM Navigator CD into the specified PFM folder. GUI operation from PFM can display statistics information in a graph or table in the Web browser.

See the PFM manual for further details.

The following versions are required for executing HvmSh command on PFM.

PFM	HvmSh command	LPAR manager
09-10 or later versions	4.0 or later versions	57-30 or later versions

Tip

- With LPAR manager not supporting LP CLI IP Address, set the IP address of the management server to BSM IP Address.
- With LPAR manager supporting LP CLI IP Address, set the IP address of the management server to LP CLI IP Address. Setting the management server IP address to BSM IP Address.

HCSM

Hitachi Compute Systems Manager (HCSM) is software for operating large-scale systems. A system administrator can manage hardware resources and power supply, monitor operation status, and operate N+M cold standby and hardware.

See the *Compute Systems Manager Software User's Guide* for details.

HVM Navigator

HVM Navigator is a navigator tool for LPAR manager platforms, which provides user-friendly GUIs for a series of tasks, such as planning server integration, building environment, operation, and monitoring.

For this utility, consult your reseller.

Monitoring

❑ Monitoring overview

Monitoring is to monitor operation status in the LPAR manager environment, which is used for diagnosing the resource shortage per LPAR. It allows you to total the operation status to multiple LPAR managers on the network, and to view the monitored history picked up from various viewpoints.

For details, see the *HVM Navigator User's Guide Monitoring Functions*.

Configuration viewer

❑ Overview of the configuration viewer

The configuration viewer is a function to display the LPAR manager system configuration list and LPAR manager system block diagram.

For details, see the *HVM Navigator User's Guide Viewer Functions*.

LPAR migration

❑ Overview of LPAR migration

LPAR migration means that an LPAR migrates from a server blade, which is currently running, to another server blade. See the *HVM Navigator User's Guide - Migration* for details.

LP model updating

LP model is user-updatable.

See *LP Model up Procedure* for details.

LPAR manager version upgrade

LPAR manager version is user-upgradable.

See the *Compute Blade 2000 LPAR Manager Version Upgrade Guide/LPAR Manager Revision Update Guide* for details.

Migration between basic environment and LPAR manager environment

❑ Migration from basic environment to LPAR manager environment

The following table describes the setting and checking items when migrating from the basic environment to an LPAR manager environment.

Item	Setting and Checking	
	Before migration	After migration
OS	Delete the IP Address. (only for Windows)	Set an IP Address. (only for Windows)
	Set the SVGA resolution to 800x600; 256 colors.	-
	-	Install the NIC driver.
Server blade	Set EFI. *1	-
	Set the LP mode. *2	-
SAN security	-	Change the setting of WWPN/WWNN

*1 See EFI setting for the details.

*2 See LP mode setting for the details.

❑ Migration from LPAR manager environment to basic environment

The following table describes setting and checking items when migrating from LPAR manager environment to the Basic environment.

Item	Setting and Checking	
	Before migration	After migration
OS	Delete the IP Address. (only for Windows)	Set an IP Address. (only for Windows)
		Install the NIC driver.
Server blade	Set EFI. *1	-
	Set the Basic mode. *2	-
SAN security	-	Change the setting of WWPN/WWNN

*1 See EFI setting for details.

*2 See LP mode setting for details.



- LPAR manager environment using the virtual NIC and Basic environment have different NIC type and MAC address. Therefore, install the NIC driver at the first migration. Also change the middleware settings to identify MAC address.
  If migrating between the Basic environment and LPAR manager environment with NIC to which the fixed IP address is set, the IP address remains set to the old MAC address. As a result, resetting the IP address causes the overlap error. Therefore, delete the IP address before migration.
  See “MAC Address for Virtual NIC” for the NIC MAC address. For setting middleware, see the middleware manual.
- Change the setting of SAN security on the storage side because the LPAR manager environment and Basic environment WWPN/WWWNN are different. For WWPN/WWNN for the shared FC, see “FC Shared WWPN/WWNN”. For the setting change of SAN security, see the manual of your storage device.
- When you install OS in the Basic environment, change the resolution, and migrate to the LPAR manager environment, the screen might not be displayed via the remote console. Therefore, change the SVGA resolution to 800x600; 256 colors in Basic environment before migrating to the LPAR manager environment.

LPAR manager Security

You can improve LPAR manager security using Transport Layer Security (TLS) and certificates. Certificates play the following two roles.

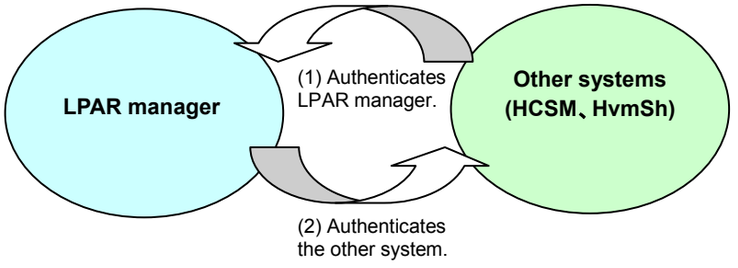
- Authenticating certificate ownership
- Encrypting communication

You can set LPAR manager security using the HvmSh command. Copy HvmSh to the directory where the execution path is set to the management server that executes HvmSh.

See the *HVM Management Command (HvmSh) Operation Guide* for details about the command.

Certificates in LPAR manager

LPAR manager can create and use a server certificate to certify its identity and authenticate other systems using the certificate of a system connected to LPAR manager (hereinafter referred to as the other system).



❑ LPAR manager certificate

When the other system tries to connect to LPAR manager over TLS, the LPAR manager certificate is sent to the other system. The other system can authenticate the LPAR manager by verifying the server certificate.

- LPAR manager server certificate

  LPAR manager can use self-signed certificates or certificates signed by a certificate authority (CA) as the LPAR manager server certificate.

  When the other system authenticates LPAR manager by verifying the LPAR manager server certificate, register the server certificate to the other system. See the other system's user's guide for registration.

  It may take about 30 seconds before a registered certificate is enabled, while connection to LPAR manager may be unavailable for that period.

- Systems for LPAR manager server certificate

  The following systems can use LPAR manager server certificates.

  - HCSM (Hitachi Compute Systems Manager)
  - HvmSh

- Server certificate parameters

  The following table describes parameters of LPAR manager server certificates.

Item	Description
Public key algorithm, bit- length	RSA (2048 bits)
Importable certificate format	PEM/DER
Certificate format in downloading	DER
Executable CSR format	PEM/DER
Subject information usable in a certificate and CSR	Common name (CN): Up to 60 characters (*1, *2)
	Country (C): Up to 2 characters (*3)
	State or province (ST): Up to 60 characters (*4)
	Locality (L): Up to 60 characters (*4)
	Organization name: Up to 60 characters (*4)
	Organization unit (OU): Up to 60 characters (*4)
	Mail address: Up to 60 characters (*5)
	Domain name (DN) qualifier: Up to 60 characters (*4)
	Surname: Up to 60 characters (*4)
	Given name: Up to 60 characters (*4)
	Initials: Up to 30 characters (*4)
	Unstructured name: Up to 60 characters (*4, *6)
	Challenge password: Up to 30 characters (*4, *6)

*1 Required item.

*2 Alphanumerical characters, hyphones (-) and period (.) can be used for this item.

*3 Uppercase alphabetic characters can be used.

*4 Alphanumerical characters, hyphones (-), periods (.), pluses (+), single quotations (‘), commas (,), left parentheses ((), right parentheses ()), slashes (/), colons (:), equals (=), question marks (?), and spaces can be used for this item.

*5 Printable ASCII characters can be used.

*6 This can be filled in when CSR is created.

- Creating LPAR manager server certificate

  To create a self-signed certificate:

  A self-signed certificate is automatically created at the LPAR manager first boot. When re-creating one, use the “opr HvmServerCertificate” command.

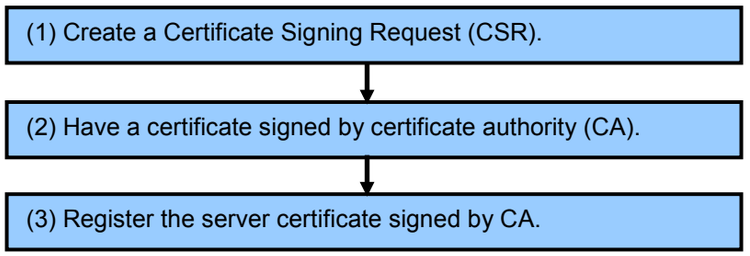
  Make sure that a unique common name (CN) is set in the subject information for a self-signed certificate per LPAR manager.

  To obtain a created self-signed certificate, use the “get HvmServerCertificate” command.

  Use the “opr HvmSecureCmmConfigSave” command to save the LPAR manager configuration information before shutting down or rebooting the LPAR manager after creating a self-signed certificate.

To register certificates signed by CA:

The following flow-chart shows the process of registering by using a certificate signed by CA.



(1) Create a Certificate Signing Request (CSR).

Use the “opr HvmCSR” command to create a CSR.

Make sure that a unique common name (CN) is set in the subject information for a self-signed certificate per LPAR manager.

A private key corresponding to the CSR is generated in LPAR manager. The same private key cannot be generated.

The private key and server certificate you have created will be used in step (3) to register the signed server certificate. Before the server certificate is registered, the previous private key and server certificate are used.

Use the “opr HvmSecureCmmConfigSave” command to save the LPAR manager configuration information before shutting down or rebooting LPAR manager.

(2) Have a certificate signed by certificate authority (CA)

Send the created CSR to the CA to obtain the signed certificate.

(3) Register the server certificate signed by CA.

Use the “opr HvmCACertificateRegist” command to register the signed server certificate to the LPAR manager. The certificate can be registered only in the LPAR manager for which the CSR is created.

Use the “opr HvmSecureCmmConfigSave” command to save the LPAR manager configuration information and back up that before shutting down or rebooting the LPAR manager.

❑ Authentication of the other system

When LPAR manager tries to connects to the other system using TLS, it can authenticate the other system by verifying the other system’s certificate. For authentication, register a certificate of the other system or a certificate of CA that has signed the certificate of the other system in the LPAR manager, and enable the certificate verification.

Use the “opr HvmClientCertificateRegist” command to register a certificate and “opr HvmIfSecureVerify” command to enable the certificate verification.

- System available for LPAR manager authentication

  The following system can be authenticated by LPAR manager.

  - HCSM (alert)

Management Interface Security

This subsection describes the security of LPAR manager management interfaces.

❑ Security strength

You can strengthen the LPAR manager security in the LPAR manager management interface. Security strength has two setting values, “Default” and “High”. “Default” is the default value at the factory.

Changing the value: “Default” to “High” to strengthen the security of LPAR manager management interface, which includes the following.

- Communication in plaintext is not allowed.
- In encrypted communication, only high security algorithm can be used.

❑ Security strength and LPAR manager management interfaces

For LPAR manager, you can change security strength of management interfaces shown in the following table. When the security strength is changed, LPAR manager interfaces will use the following protocol and encryption methods shown in the table below. See Encryption algorithm supported by LPAR manager for the setting.

Management interface	Security strength	Set in Default		Set in High	
		plaintext	encryption	plaintext	encryption
HvmSh	“Default” or “High”	UDP/TCP	TLS v1.0-v1.2	-	TLS v1.2
HCSM	“Default” or “High”	-	SSL v3.0, TLS v1.0-v1.2	-	TLS v1.2
SC/BSM	“Default” or “High”	TCP	-	-	-

(-): Communication is not available.



When using HVM Navigator, set the security strength of HvmSh and HCSM to “Default”.

❑ Changing security strength

You can set the security strength of LPAR manager management interfaces using HvmSh. See the *HVM Management Command (HvmSh) Operation Guide* for details about the command.

It may take about 30 seconds before the new security value is enabled, while connection to LPAR manager may be unavailable for that period.

❑ Encryption algorithm supported by LPAR manager

The following tables show encryption algorithm supported by LPAR manager.

- SSL/TLS

Cipher suites	Security strength	
	Default	High
TLS_RSA_WITH_AES_128_CBC_SHA	√	-
TLS_RSA_WITH_AES_128_CBC_SHA256	√	√
TLS_RSA_WITH_AES_256_CBC_SHA256	√	√
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	√	-
TLS_RSA_WITH_3DES_EDE_CBC_SHA	√	-

Server certificate (Public-key algorithm)	Security strength	
	Default	High
Verify RSA2048	√	√
Create RSA2048	√	√

Server certificate (Signature algorithm)	Security strength	
	Default	High
Verify SHA256	√	√
Create SHA256	√	√

(√): Supported
(-): Not supported

Cautions

This section describes the cautions when using LPAR manager. For those interested in system equipment, see Chapter 13: System Operation and Management.

Emulex 10 Gb NIC-1 Gb Switch Module

Emulex 10 Gb NIC-1 Gb Switch Module is supported under the following conditions.

When updating Emulex 10 Gb NIC driver to 4.2.390.6 or later for Windows or 4.2.456.0 or later for Linux, update Emulex 10 Gb NIC firmware to 4.2.433.604 or later.

When updating LPAR manager firmware to 59-4X/79-4X or later, update Emulex 10 Gb NIC firmware to 4.2.433.604 or later. See the following table.

		Emulex 10 Gb NIC driver version				LPAR manager firmware version	
		Windows		Linux			
		4.1.334.25 or lower	4.2.390.6 or later	4.1.334.18 or lower	4.2.456.0 or later	59-3X/79-3X or lower	59-4X/79-4X or later
Emulex 10Gb NIC firmware version	4.1.334.2801 or lower	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
	4.2.433.604 or later	Not supported	Supported	Not supported	Supported	Not supported	Supported

Emulex 10 Gb NIC-10 Gb Switch Module

Emulex 10 Gb NIC-10 Gb Switch Module is supported under the following conditions.

When updating Emulex 10 Gb NIC driver to 4.2.390.6 or later for Windows or 4.2.456.0 or later for Linux, update Emulex 10 Gb NIC firmware to 4.2.433.604 or later.

When updating LPAR manager firmware to 59-4X/79-4X or later, update Emulex 10 Gb NIC firmware to 4.2.433.604 or later.

		Emulex 10 Gb NIC driver version				LPAR manager firmware version	
		Windows		Linux			
		4.1.334.25 or lower	4.2.390.6 or later	4.1.334.18 or lower	4.2.456.0 or later	59-3X/79-3X or lower	59-4X/79-4X or later
Emulex 10Gb NIC firmware version	4.1.334.2801 or lower	Supported	Not supported	Supported	Not supported	Supported	Not supported
	4.2.433.604 or later	Supported	Supported	Supported	Supported	Supported	Supported

Setting FC switch

- FC switch ports, which will be connected to 4 Gbps Fibre-channel adapters in shared mode, should have NPIV enabled.

  With the “portcfgshow” command, you can determine whether or not NPIV is enabled.

  If NPIV is disabled, enable the NPIV using the “portcfgnpivport” command of the FC switch.

  See the manual attached to the FC switch for how to set and confirm NPIV.

- When the transfer rate of the FC port in an FC switch is the default value, auto-negotiation, the logical unit (LU) in storage might not be viewed because of the discrepancy between the transfer rate of the FC port and that of the Fibre-channel card.

  In this case, change the transfer rate of the FC port to the same rate of your Fibre-channel card using the “portcfgspee” command.

Using shared FC

The following table shows whether or not a shared FC is available.

Connection configuration			Shared FC: available or not	
			4 Gbps fiber channel adapter	8 Gbps fiber channel adapter
Connected to storage via FC switch module	NPIV is supported by the FC switch module.	P to P	Available	Available
		Loop	Not available	Not available
	NPIV is Not supported by the FC switch module.	Loop	Not available	Not available
		P to P	Not available	Not Available
Connected direct to storage (only with 8 Gbps Fibre-channel adapter)		Loop	Not available	Not available
		P to P	Not available	Available

Connection type for shared FC port

- For connection via a FC switch, follow the conditions shown in the table below.

Type of FC adapter	Firmware version of FC adapter	Connection type
4Gbps adapter	2x-08-12 or later	Auto or Point to Point
	2x-08-10 or earlier	Point to Point
8Gbps adapter	All versions	Auto or Point to Point

- For connection directly to the storage (available only for 8 Gbps adapters), set the connection type to Loop.

Notes on SMP configuration

- When you boot LPAR manager with different LP models in a SMP configuration, the lower level LPAR manager is booted. The primary server blade is the one installed in a slot with the smallest number, the left-end slot viewed from the front.

LP model		LP model to boot
Primary	Non-primary	
Enterprise model	Enterprise model	Enterprise model
Enterprise model	Essential model	Essential model
Essential model	Enterprise model	Essential model
Essential model	Essential model	Essential model

- If LPAR manager firmware versions are different between the primary server blade and non-primary one, the firmware version on the primary server blade is used.
- In an SMP configuration, updating LPAR manager firmware updates that are on the primary server blade. Those on the non-primary server blades are not updated.
- LPAR manager configuration file of the primary server blade is used for SMP configuration. The following table shows the relation between the server blade configuration and LPAR manager configuration files.

Server blade configuration		LPAR manager configuration file used
SMP Configuration	Slot number	
2-blade SMP	0 to 1	LPAR manager configuration file 0
	1 to 2	LPAR manager configuration file 1
	2 to 3	LPAR manager configuration file 2
	4 to 5	LPAR manager configuration file 4
	5 to 6	LPAR manager configuration file 5
2-blade SMP	6 to 7	LPAR manager configuration file 6
4-blade SMP	0 to 3	LPAR manager configuration file 0
	4 to 7	LPAR manager configuration file 4

- Since the LPAR manager configuration file of the primary server blade is used for SMP configuration, this configuration is taken over. The non-primary server blade configuration, such as settings for NIC, FC, and processor group, returns to the default, not taken over. Then, you need to set them again.

- The following table shows sequences of devices recognized in SMP configuration. Each device is recognized by the number shown at the bottom of the table.

Primary					Non-Primary															
Server blade #0					Server blade #1					Server blade #2					Server blade #3					
Onboard LAN	PCIe slot #1	PCIe slot #0	Expansion card slot #0	Expansion card slot #1	Onboard LAN	PCIe slot #1	PCIe slot #0	Expansion card slot #0	Expansion card slot #1	Onboard LAN	PCIe slot #1	PCIe slot #0	Expansion card slot #0	Expansion card slot #1	Onboard LAN	PCIe slot #1	PCIe slot #0	Expansion card slot #0	Expansion card slot #1	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	

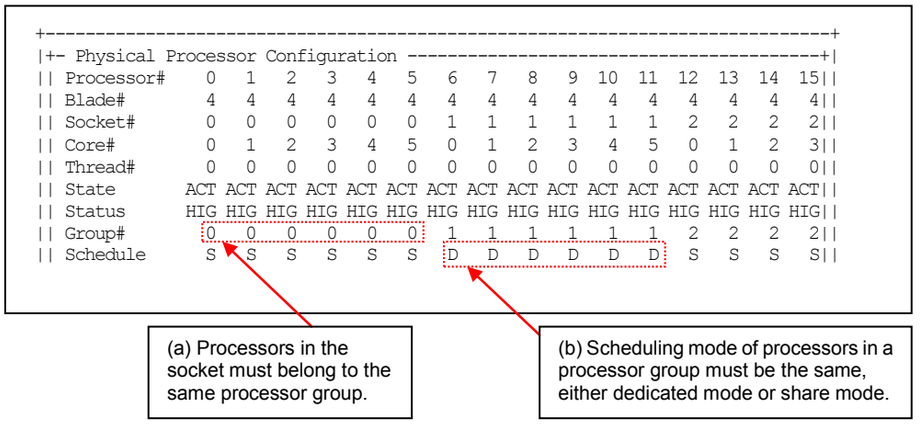
- With 4-blade SMP configuration, the following performance might be slower than that with 1 blade or 2-blade SMP.
  - Performance when more logical processors in shared mode than physical processors are assigned.
  - Virtual COM console
  - Time required for Windows bootup
- When the power capping is enabled with 4-blade SMP configuration, OS boot might take longer. If so, disable the power capping setting. See (6) How to change the power capping function (LPAR manager firmware version 58-7X/78-7X or later) for details.

■ When setting a processor group or scheduling mode with 4-blade SMP configuration, follow (a) and (b) below. If you do not follow those requirements for setting, performance between logical processors in the same LPAR might be extremely different, which might cause an OS on the LPAR to fail.

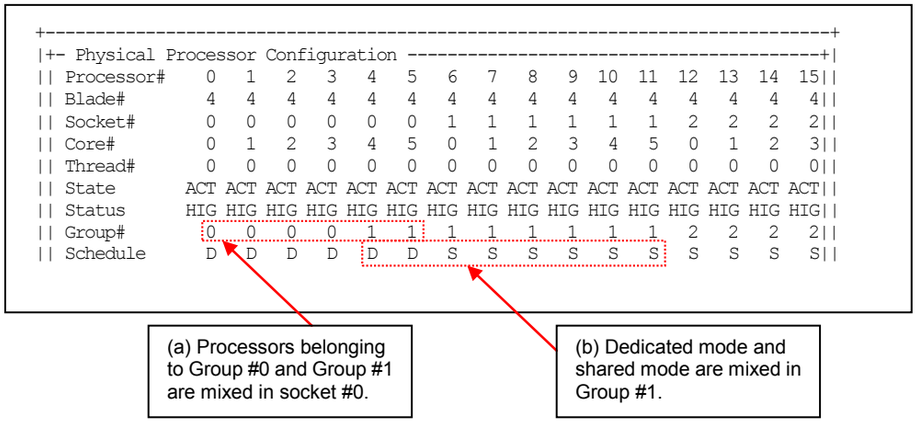
(a) Processors in the socket must belong to the same processor group.

(b) Scheduling mode of processors in a processor group must be the same, either dedicated mode or share mode.

◆ Example of recommended LPAR configuration with 4-blade SMP



◆ Example of not-recommended LPAR configuration with 4-blade SMP





When using LPAR migration function with 4-blade SMP configuration, configure both the source and destination satisfying requirements (a) and (b).

Restriction on X55R3/X55S3 with 2-core CPU

When a standard server blade X55R3/X55S3 model has a single 2-core CPU onboard, enable SMT (Simultaneous Multi-Threading). If it is disabled, an LPAR might fail unexpectedly.

Restriction on TPM (Trusted Platform Module)

LPAR manager does not support TPM (Trusted Platform Module). If with TPM installed, disable TPM SUPPORT in **EFI Setup Menu.** Click **Advanced > Trusted Computing**, and set **TPM SUPPORT** to **Disable**.

Notes on adding NIC

A network segment identifier (1a, 2a, 2b...) is changed automatically when changing to a shared NIC after adding NIC. You need to check LPAR network configuration or settings by the change when LPAR network configuration or setting is managed using a network segment identifier.

Restriction on Emulex 10 Gb NIC

When the following Emulex 10 Gb NICs are used, combinations of Emulex 10 Gb NIC firmware version and LPAR manager firmware version are restricted as shown in the table below.

- Emulex 10 Gb 2-port LAN adapter
- Emulex 10 Gb 4-port LAN adapter
- Emulex 10 Gb 2-port CNA adapter
- Emulex 10 Gb 4-port CNA adapter
- Emulex 10 Gb 2-port CNA board

Item		LPAR manager firmware version	
		59-3X/79-3X or lower	59-4X/79-4X or later
Emulex 10 Gb firmware version	4.1.334.2801 or lower	√ (- *)	-
	4.2.433.604 or later	√ (- *)	√
	4.6.348.0 or later	-	√

(√): Supported

(-): Not supported

(-*): Not supported when Emulex 10 Gb NIC and 1 Gb switch module are connected.

System requirements for LPAR manager and LPAR

The following table shows the requirements for using LPAR manager/LPAR. Without those requirements satisfied, LPAR manager and LPARs might not work correctly. Resources to be assigned to LPARs depend on your purpose and environment.

Item		System requirements
LPAR manager	Memory	1536 MB
LPAR	Processor	2 processors or more
	Memory	Windows Server 2003 R2: 256 MB (256 MB or greater)*1 Windows Server 2008: 512 MB (2048 MB or greater) Windows Server 2008 R2: 512 MB (2048 MB or greater) Windows Server 2012: 512 MB (2048 MB or greater) Windows Server 2012 R2: 512 MB (2048 MB or greater) Red Hat Enterprise Linux 5: 512 MB (1024 MB per logical processor) Red Hat Enterprise Linux 6: 1024 MB (1024 MB per logical processor)

*1: When memory is 256 MB, iup to 32 processors can be installed.
Figures in parentheses ( ) show the recommended value.

Setting LPAR manager system

Set a unique value to VNIC System number per LPAR manager including Compute Blade 1000, Compute Blade 2000, and Compute Blade 320. If a value overlaps with that of another LPAR manager, network communication is not available on LPAR because the MAC address of the virtual NIC to the LPAR overlaps.

Maximum resolution

The following table describes the maximum resolution when the remote desktop, remote console, or NETM/Remote Control is used.

Application	Maximum resolution	Prerequisite
Remote desktop	-	Up to the maximum resolution can be specified: 1280 x 1024 for example.
Remote console	1024 x 768	It is recommended that the resolution of a guest OS be 1024 x 768. If a guest OS resolution is more than 1024 x 768, the console terminal displays the area of 1024 x 768 out of the screen. But the screen can be scrolled by moving the scroll box.
NETM/Remote Console		

Setting guest OS display

When using the remote console, set the guest OS display. If the display is already set, skip this setting.

For how to set it, see Guest OS display setting.

Serial setting with guest screen in use

When using a guest screen, set the serial console. If it is already set, skip this setting.

For how to set the serial setting, see Serial setting when using the guest screen.

Using Linux

When you use Linux on LPAR manager, change the settings to those described in the *Hitachi Compute Blade Software Guide*.

Using Windows

When you use Windows on LPAR manager, change the settings to those described in the *Hitachi Compute Blade Software Guide*.

NETM/Remote control

When you use the remote control function, the screen display and mouse operation slow down due to SVGA emulation. If you do not need to assign USB, do not assign it.

With LPAR manager firmware version 58-7X/78-7X or later, the performance has been improved as long as the following requirements are satisfied.

Video mode	Resolution	USB device/Remote console LPAR status	
		Assigned	Not assigned
Text		Not targeted	Not targeted
Graphics	640 x 480	Not targeted	Not targeted
	800 x 600	Not targeted	Not targeted
	1024 x 768	Not targeted	Targeted
	1280 x 1024	Not targeted	Not targeted
	Other than above	-	-

Targeted: Targeted for performance improvement

Not targeted: Not targeted for performance improvement

-: Not supported

Notes on ServerConductor/Blade server manager

- VF NIC view and settings are not supported,
- Do not backup configuration information using SC/BSM while the configuration is being saved on the LPAR manager screen or HVM Navigator, or LPAR migration is being performed. If you do, the backed up configuration is incomplete. Discard the back-up obtained during the saving or migration mentioned earlier. Back up the configuration again after the save or the migration is complete.
- It is recommended that you use the following combination of the LPAR manager firmware version and SC/BSM firmware version.

LPAR manager firmware version	SC/BSM firmware version
58-30 or later: standard server blades	09-00 or later
78-30 or later: high-performance server blades	

If you use combinations other than those above, slot numbers are displayed differently on the LPAR manager screen and SC/BSM as shown below.

Example of the slot number for an expansion card

<[PCI device information] and [PCI device scheduling mode>

Item	LPAR manager screen	SC/BSM	Remarks to SC/BSM
Slot number	Ex0	E1x0	Extra “1” is added before “x”
	Ex1	E1x1	Extra “1” is added before “x”

x: Server blade number

<[FC information] and [LPAR configuration>

Item	LPAR manager screen	SC/BSM	Remarks to SC/BSM
Slot number	Ex0	1x0	Without “E”; Extra “1” is added before “x”
	Ex1	1x1	Without “E”; Extra “1” is added before “x”

x: Server blade number

Slot numbers for an I/O slot expansion unit

LPAR manager screen	SC/BSM
I000 - I015	20 - 35
I100 - I115	36 - 51
I200 - I215	52 - 67
I300 - I315	68 - 83
I400 - I415	84 - 99
I500 - I515	200 - 215
I600 - 615	216 - 231
I700 - I715	232 - 247

Tip

- A physical processor number for LPAR manager can be specified between 0 and 31. When you specify a number between 32 and 63, use the Logical Processor configuration screen.
- If you specify a physical processor number for LPAR manager between 32 and 63 from SC/BSM, use BSM 80-90 or a later version.

Notes on ServerConductor/Deployment Manager

For the latest specification of DPM, see *ServerConductor/Deployment Manager.*

- Not supported by VF NIC.
- Clearing partitions on the disk of LPAR manager including “OS clear install” is not supported.
- PXE boot (Network boot) of dedicated NIC is not supported.
- When using SC/DPM, make sure to configure the EFI driver by following the description to set PXE boot (network boot). See Setting the extensible firmware interface (EFI) driver, Creating Boot Options, and orders for the details.
  1. Boot function = Enabled
  2. Select Boot Device = Enabled
  3. WWPN/LUN # on the storage side port that is a target for the boot device list
- The MAC address to a parameter file for disk duplication of the DPM management server should be the same as the MAC address of a NIC registered at the top of the EFI Boot Order.
- LPAR reboots five times at the disk duplicate installation as Basic does. If executing one of the following before five reboots are completed, automatic reboots stops, and DPM will halt while still operating. Then follow the two instructions.
  1. Do not connect to the guest console from the LPAR manager screen.
  2. Do not connect via the remote desktop.
- The LPAR to be a master client and LPAR to be a target client should have the same number of ports for a Fibre-channel (FC), even if any LU is not assigned to the LPARs. If they are not the same, the installation might fail. FC assignment can be executed on the PCI Device Assignment screen.
  For other conditions including the LU size, see the manual *ServerConductor/Deployment Manager*.
- The progress status report displayed on the remote console might have disturbed characters. DPM will operate properly regardless of the symptom.

Notes on ServerConductor/Advanced Agent

If load is applied to an USB storage device, such as an USB memory, continuously on Linux using a benchmark measurement tool, watchdog timeout may occur when watchdog timer is set in SC/Advanced Agent.

Power capping

With the power capping function, too small values for the power capping reduces the CPU performance, which might cause the OS performance on the LPAR to slow down. Conduct tests adequately and then configure a proper value.

Processor capping

With LPAR manager firmware version 58-5X/78-5X or earlier, power consumption by an LPAR might not be controlled as the setting value regardless of that processor capping for the LPAR is shown as Enabled in the configuration information.

If it has occurred, reconfigure the processor capping to Enabled.

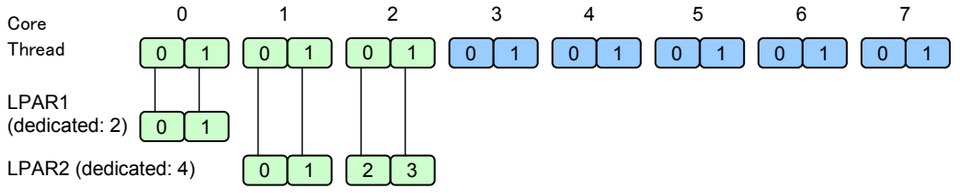
Assigning processors when SMT enabled

- When SMT is Enabled in the EFI setting, the entire system efficiency will be improved by up to 20%.
- To avoid interference between LPARs, which changes LPAR performance depending on the workload status of another LPAR, assign processors following the description below:
  - Assign an even number of processors to an LPAR.
  - Although you can select processors to use on the Logical Processor Configuration screen when assigning dedicated processors, do not assign any thread in the same core to different LPARs.

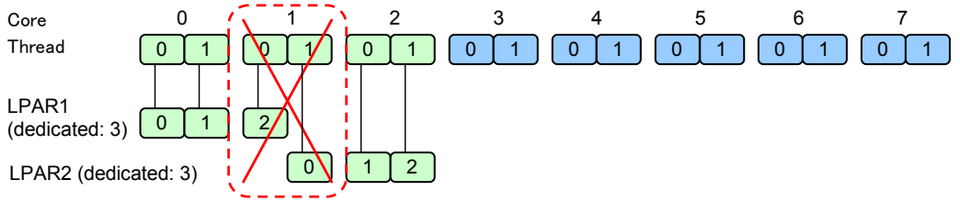
#	Thread0	Thread1	Interference	Recommended	Remarks
1	Dedicated	Dedicated (the same LPAR)	None	Dedicated	Automatically determined when an even number of processors are assigned.
2	Dedicated	Dedicated (different LPARs)	Interfered	Not recommended	Automatically determined when an odd number of processors are assigned.
3	Dedicated	Shared	Interfered	Not recommended	The status is “Shared”
4	Shared	Dedicated	Interfered	Not recommended	The status is “Shared”
5	Shared	Shared	Interfered	Shared	Assigning an even or odd number of processors is available.

Images of assigning processors are as follows:

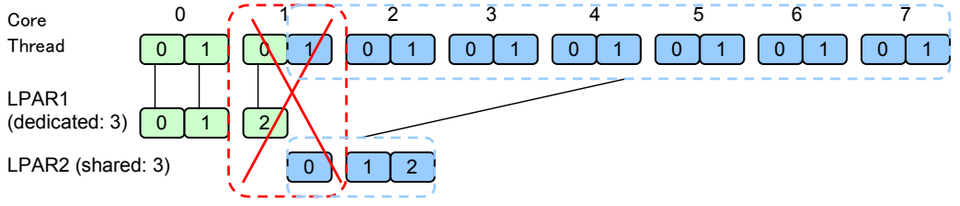
1. Assigning Dedicated processors to LPARs



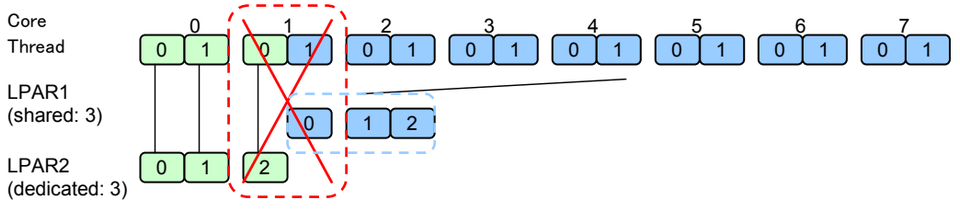
2. Assigning an odd number of Shared processors to LPARs: Not recommended.



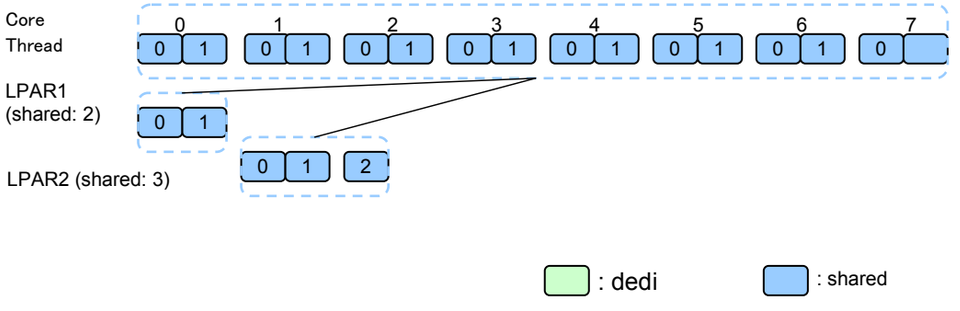
3. Assigning an odd number of Dedicated and Shared processors to LPARs: Not recommended.



4. Assigning an odd number of Shared and Dedicated processors to LPARs: Not recommended.



5. Assigning Shared processors to LPARs



Degeneration/Isolation of Processors, Memories, and PCI Devices

- When a processor, memory, or PCI device is degenerated or isolated, system event logs (SELs) of the system equipment are collected and alerts are sent to SC/BSM.
- When a processor, memory, or PCI device is degenerated or isolated, the device is not recognized at the next LPAR manager boot, and part of the related LPAR manager configuration information is deleted or reconfigured.
- When recovering the device from degeneration or isolation by replacing hardware, restore the backup file before booting the LPAR manager. If there is no backup file, check that the LPAR manager configuration is the same as before degeneration or isolation. If there is something wrong with it, reconfigure as necessary.
- When all processors are degenerated in a nonprimary server blade in SMP configuration, the server blade itself is degenerated including memories and PCI devices in it.

Degeneration of Processor Cores

- When the “State” of a processor core on the Physical Processor Configuration screen is Wrn, Warning: the number of recoverable failures is beyond the threshold, or Deg, Degenerate: degenerated due to proactive replacement or degeneration, the processor core will be degenerated and not be recognized at the next LPAR manager boot.
- When LPAR manager is rebooted while a processor core is degenerated, the LPAR manager cannot recognize the degenerated processor core, which causes the following.
  - Physical processor assignment to logical processors on all LPARs is initialized.
  - The processor group number of degenerated core is initialized.

Using USB device

- LPAR manager changes LPARs to use a USB device, connecting the newly assigned LPAR to the remote console for using the USB device.
- You need to assign a USB device to an LPAR before activating the LPAR. LPARs, to which the USB device is not assigned, cannot be selected as connection destination for the USB device.
- An LPAR to use a USB device must be activated. LPARs in deactivation or failure cannot be selected to use the USB device. When an LPAR using the USB device fails, another LPAR might not be assigned to the USB device.
- Make sure to satisfy the following conditions before detaching a USB device.
  - ◆ OS is not booting or rebooting.
  - ◆ The USB device has been detached from the OS by performing the steps for safely removing hardware for Windows, or unmounting the device for Linux after the USB device is recognized by the firmware or OS.
  - ◆ Remote console is displayed without keeping the Alt, Windows, Ctrl, and Shift keys pressed.

  If you detach the USB device without satisfying conditions above, the following events might occur.
  - ◆ Firmware or the OS behavior might become unstable, or the OS might hang up.
  - ◆ Data might be corrupted, or the display of the USB device might remain on the OS.
  - ◆ Keyboard operation might not be properly executed.

  If those events occur due to detaching the USB device, execute the following operation.
  - ◆ For instability in firmware or OS behavior or OS hangup, attach the USB device. If it does not recover the OS behavior, deactivate the LPAR and then activate it again.
  - ◆ For the USB device that remains displayed on the OS, attach the USB device and then detach it again.
  - ◆ For improper keyboard operation, any key might remain pressed on the OS. If so, execute the following operation.
    - For Windows, display the OS with the remote console, NETM/Remote Control, or remote desktop in full screen, simultaneously press Alt, Windows, Ctrl, and Shift keys.
    - For Linux, display the OS with the remote console, press all Alt, Ctrl, and Shift keys.
- When a USB device is attached to an LPAR, usually an OS running on the LPAR automatically recognizes the USB device. However, the USB device might not be automatically recognized due to the state of the OS or when the USB device might not have been completely detached. When the USB device cannot be recognized after a while, detach the USB device and then connect it again. If it does not work, unplug and then plug the USB cable, or uninstall the USB device driver from the OS and then install it again.
- With Linux, an error message appears when the USB device is detached. If the USB is not mounted, there is no problem for data on the USB device and OS behavior in the future.
- If you use a USB port that differs from the one used at boot option registration, the USB CD/DVD-ROM drive might not be recognized. If this happens, re-register the boot option.

- Do not use the device (such as a keyboard and mouse) not supported with LPAR manager. Otherwise, for example, a guest OS on the LPAR might fail to boot.
- When booting LPAR manager, do not connect a GUID partition table (GPT) disk to a front USB port. With a GPT disk connected to a front USB port, LPAR manager might fail to boot up. If this happens, remove the GPT disk from the front USB port, and then reboot the LPAR manager.

Memory size assigned to LPAR

Although the minimum memory allocation size to LPAR is 256 MB, the minimum memory size that the guest OS can work differs depending on the type and version of OS, the number of the logical processors, middleware or application.

1 TB or greater memory is supported only by the following OSs. Do not use that for other OSs. If you do, the OS might not work properly.

- Windows Server 2008 R2 (*)
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Red Hat Enterprise Linux 6

(*) When using memory more than 1 TB, execute the following steps.

1 Set memory to less than 1 TB, and then boot the OS.

2 Apply KB980598.

3 Shut down the OS.

4 Set memory to 1 TB or greater, and then boot the OS.

LPAR memory fragmentation

With LPAR manager firmware version 59-1X/79-1X or earlier, when you repeatedly activate and deactivate LPARs with different memory size, a message “Memory allocation failed (Fragmentation).” appears and an LPAR might fail to be activated even if the memory size is enough. This is called “LPAR memory fragmentation”, which occurs in activating an LPAR that requires discontinuous blank memories on physical memory. A typical example is shown below:

(1) Example of failure in LPAR activation due to LPAR memory fragmentation

When all blank memories including five or more discontinuous ones are allocated to LPARs, LPAR activation fails.

Memory allocation (Example)	
LPAR 1	3 GB
LPAR 2	1 GB
LPAR 3	1 GB
LPAR 4	1 GB
LPAR 5	1 GB
LPAR 6	1 GB
LPAR 7	1 GB
LPAR 8	1 GB
LPAR9	1 GB
LPAR 10	20 GB

1. Activates LPARs with an even number.

Memory allocation (Example)	
LPAR 1	3 GB
blank	1 GB
LPAR 3	1 GB
blank	1 GB
LPAR 5	1 GB
blank	1 GB
LPAR 7	1 GB
blank	1 GB
LPAR9	1 GB
blank	20 GB

2. Activates LPARs with 24 GB memory.



LPAR manager screen (Example)

```
+-------------------------------------------------+
|   Memory Allocation Display                     |
|    #  Mem Org Addr (Hex)    Mem Size   Name     |
|    1  00000000 00000000       768MB   SYS2     |
|    2  00000000 30000000      2304MB   LPAR1    |
|    3  00000000 c0000000       256MB   SYS1     |
|    4  00000001 00000000       768MB   LPAR1    |
|    5  00000001 30000000      1024MB   ******** |
|    6  00000001 70000000      1024MB   LPAR3    |
|    7  00000001 b0000000      1024MB   ******** |
|    8  00000001 f0000000      1024MB   LPAR5    |
|    9  00000002 30000000      1024MB   ******** |
|   10  00000002 70000000      1024MB   LPAR7    |
|   11  00000002 b0000000      1024MB   ******** |
|   12  00000002 f0000000      1024MB   LPAR9    |
|   13  00000003 30000000     19712MB   ******** |
|   14  00000008 00000000       512MB   ******** |
|  [PageUp]:Page Up / [PageDown]:Page Down        |
+-------------------------------------------------+
```

When this problem occurs, performing the following steps might activate the LPAR. You can locate the LPAR memory allocation on the physical memory in the memory allocation display in the logical partition (LPAR) configuration screen.

1. Change the memory size of an LPAR to activate to the size containing up to 4 blank memories.
2. Deactivate those activated LPARs that are using memories next to blank memories.
3. Define a dummy LPAR, specify smaller blank memories to the memory size of the dummy LPAR, and then perform activation.

   It is recommended that you should check blank memory allocation in the memory allocation display to keep the number of discontinuous blank memories up to 4 during operation.

(2) Example of failure in LPAR activation due to LPAR memory fragmentation

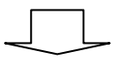
If there are 4 or more discontinuous blank memories beyond the memory size of address 0 to the top SYS1 (*1) displayed on the Memory Allocation Display and you allocate all those blank memories to LPARs, LPAR activation fails.

Memory allocation (Example)	
LPAR 1	3 GB
LPAR 2	4 GB
LPAR 3	1 GB
LPAR 4	4 GB
LPAR 5	1 GB
LPAR 6	4 GB
LPAR 7	1 GB
LPAR 8	4 GB
LPAR 9	20 GB

1. Activates LPARs with an even number.

Memory allocation (Example)	
LPAR 1	3 GB
blank	4 GB
LPAR 3	1 GB
blank	4 GB
LPAR 5	1 GB
blank	4 GB
LPAR 7	1 GB
blank	4 GB
LPAR9	20 GB

2. Activates LPARs with 16 GB memory.



LPAR manager screen (Example)

```
+-------------------------------------------------+
|    Memory Allocation Display                    |
|   #  Mem Org Addr (Hex)    Mem Size   Name      |
|   1  00000000 00000000       768MB   SYS2  (*1)|
|   2  00000000 30000000      2304MB   LPAR1     |
|   3  00000000 c0000000       256MB   SYS1      |
|   4  00000001 00000000       768MB   LPAR1     |
|   5  00000001 30000000      4096MB   ********  |
|   6  00000002 30000000      1024MB   LPAR3     |
|   7  00000002 70000000      4096MB   ********  |
|   8  00000003 70000000      1024MB   LPAR5     |
|   9  00000003  b0000000     4096MB   ********  |
|  10  00000004 b0000000      1024MB   LPAR7     |
|  11  00000004 f0000000      4096MB   ********  |
|  12  00000005 f0000000      2048MB   LPAR9     |
|  13  0000000a f0000000       256MB   SYS1      |
|                                                 |
+-------------------------------------------------+
```

If this occurs, the following operation might activate the LPAR. You can check the LPAR memory allocation on the physical memory in Memory Allocation Display on the Logical Partition (LPAR) Configuration screen.

1 Reduce the LPAR to activate: reduce one of the 4 blank memory sizes to below the size of address 0 to the top SYS1. For the figure above, reduce the LPAR to activate by 1024 MB.

2 Deactivate the activated LPARs using the memory next to the blank memory to reduce the number of discontinuous blank memories.

3 Define a new dummy LPAR, allocate the memory size described step 1 to the dummy LPAR, and activate the LPAR.

(3) Example of failure in LPAR activation due to LPAR memory fragmentation

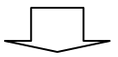
If there are 3 discontinuous blank memories beyond the memory size of address 0 to the top SYS1 displayed on the Memory Allocation Display (*1) and one 256 MB blank memory, and you allocate all those blank memories to LPARs, LPAR activation fails.

Memory allocation (Example)	
LPAR 1	3 GB
LPAR 2	4 GB
LPAR 3	1 GB
LPAR 4	4 GB
LPAR 5	1 GB
LPAR 6	256 GB
LPAR 7	1 GB
LPAR 8	4 GB
LPAR 9	2 GB

1. Activates LPARs with an even number.

Memory allocation (Example)	
LPAR 1	3 GB
blank	4 GB
LPAR 3	1 GB
blank	4 GB
LPAR 5	1 GB
blank	256 GB
LPAR 7	1 GB
blank	4 GB
LPAR9	2 GB

2. Activates LPARs with 12.25 GB memory.



LPAR manager screen (Example)

```
+-------------------------------------------------+
|    Memory Allocation Display                    |
|   #  Mem Org Addr (Hex)     Mem Size    Name    |
|   1  00000000 00000000        768MB   SYS2  (*1)|
|   2  00000000 30000000       2304MB   LPAR1     |
|   3  00000000 c0000000        256MB   SYS1      |
|   4  00000001 00000000        768MB   LPAR1     |
|   5  00000001 30000000       4096MB   ********  |
|   6  00000002 30000000       1024MB   LPAR3     |
|   7  00000002 70000000       4096MB   ********  |
|   8  00000003 70000000       1024MB   LPAR5     |
|   9  00000003 80000000        256MB   ********  |
|  10  00000003 c0000000       1024MB   LPAR7     |
|  11  00000004 c0000000       4096MB   ********  |
|  12  00000005 40000000       2048MB   LPAR9     |
|  13  00000005 50000000        256MB   SYS1      |
+-------------------------------------------------+
```

If this occurs, the following operation might activate the LPAR. You can check the LPAR memory allocation on the physical memory in Memory Allocation Display on the Logical Partition (LPAR) Configuration screen.

1. Reduce the LPAR to activate: reduce one of the 3 blank memory sizes to below the size of address 0 to the top SYS1. For the figure above, reduce the LPAR to activate by 1024 MB.
2. Deactivate the activated LPARs using the memory next to the blank memory to reduce the number of discontinuous blank memories.
3. Define a new dummy LPAR, allocate the memory size described step 1 to the dummy LPAR, and activate the LPAR.

Hardware memory dump

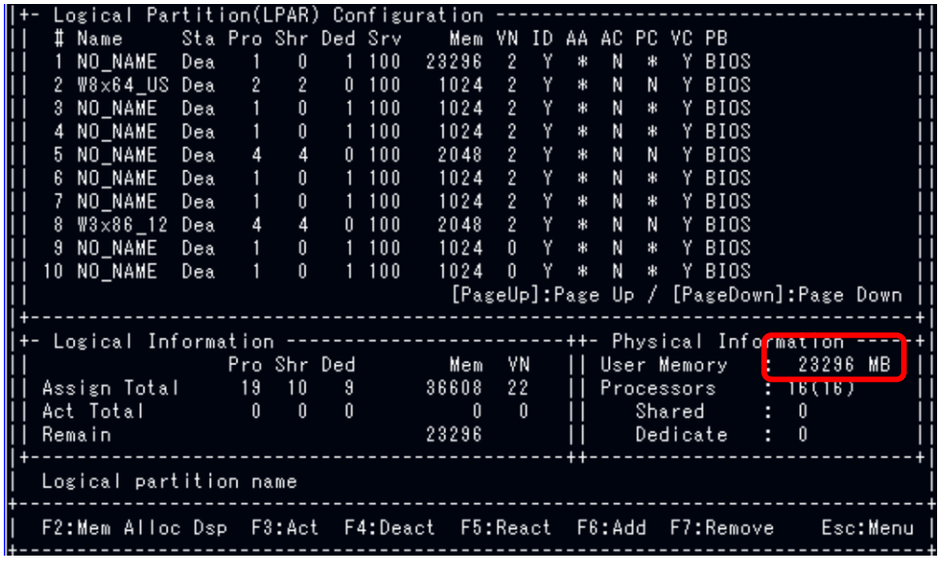
LP mode does not support hardware memory dump. When using LPAR manager, make sure to collect LP dump and guest memory dump instead of hardware memory dump.

When hardware memory dump is Enabled with LPAR manager firmware version 58-7X/78-7X or later, LPAR manager boot fails. Disable the hardware memory dump referring to Chapter 5: Server Blade Setup > EFI Setup Menu > Advanced > Hardware memory dump settings.

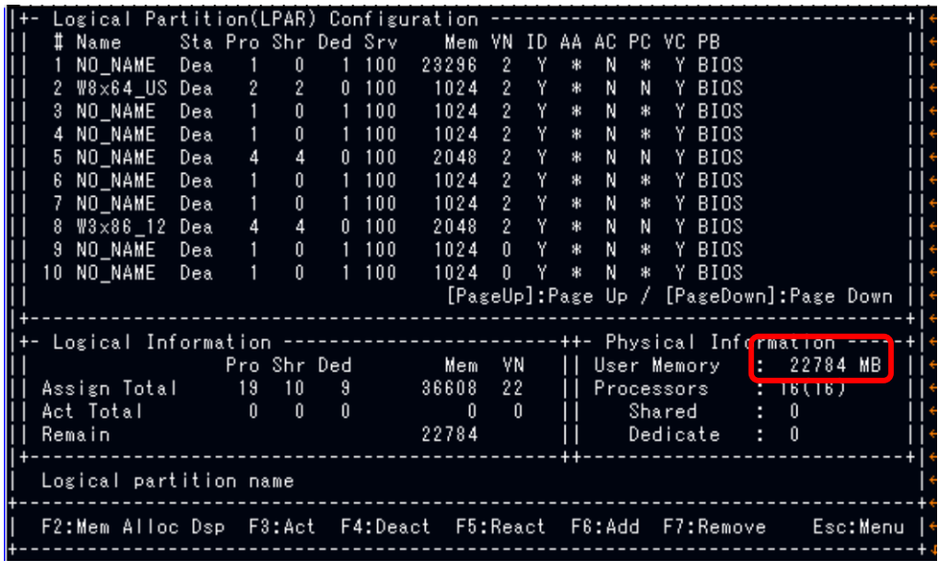
Memory space with hardware memory dump enabled

User Memory space with the hardware memory dump enabled is, at a maximum, 512 MB less than the space with the setting disabled.

For further details about hardware memory dump, see “Hardware Memory Dump” in Chapter 5.



Hardware Memory Dump: Disabled



Hardware Memory Dump: Enabled

Maximum number of NIC ports assigned to an LPAR on Linux

When Linux is used and Fusion-io Flash drive is assigned to an LPAR, the maximum number of NIC ports assigned to one LPAR is limited. If you assign NIC ports beyond the upper limit, loading the driver and Linux startup might fail.

❑ For Red Hat Enterprise Linux 5/6 x86_64

- Up to 32 ports can be assigned.
- Intel 10 Gb NIC uses 9 ports of resources per port. When assigning Intel 10 Gb NIC, 9-port resources are required for one port.
- Emulex 10 Gb NIC uses 3 ports of resources for a port. When assigning Emulex 10 Gb NIC, 3-port resources are required for one port.
- The following table shows the maximum number of ports to be assigned.

Number of ports to be assigned			Maximum number of ports
Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 9-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 3-port resources used for 1 port	
32	-	-	32
14	2	-	32
26	-	2	32
20	-	4	32

Maximum number of NIC ports assigned to an LPAR on Windows

On Windows OS, the maximum number of NIC ports assigned to one LPAR is limited. If you assign NIC ports beyond the upper limit, the following problems might occur.

- OS installation might fail, or might take extremely longer time.
- A temporary linkdown might occur when the OS is running.

❑ For Windows Server 2008/Windows Server 2008 R2 without SMP configuration

- The relation between the number of processors assigned to an LPAR and the maximum number of ports to be assigned to the LPAR is shown below.
  - SMT disabled: Maximum number of ports = the number of processors x 2 + 6
  - SMT enabled: Maximum number of ports = {(the number of processors + 1) / 2} x 2 + 6

- Intel 10 Gb NIC uses 3 ports of resources for a port. When assigning Intel 10 Gb NIC, 3-port resources are required for one port.
- Emulex 10 Gb NIC uses 4 ports of resources for a port. When assigning Emulex 10 Gb NIC, 4-port resources are required for one port.
- The following table shows examples of I/O assignment to the number of processors.

Number of processors/ LPAR		**Maximum number of ports**	**Example of I/O assignment combination**		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
1	1-2	8	8	0	0
			2	2	0
			0	0	2
2	3-4	10	10	0	0
			4	2	0
			2	0	2
3	5-6	12	12	0	0
			0	4	0
			4	0	2
4	7-8	14	14	0	0
			2	4	0
			6	0	2
5	9-10	16	16	0	0
			4	4	0
			0	0	4
6	11-12	18	18	0	0
			0	6	0
			2	0	4
7	13-14	20	20	0	0
			2	6	0
			4	0	4
8	15-16	22	22	0	0
			4	6	0
			6	0	4
9	17-18	24	24	0	0
			0	8	0
			8	0	4
10	19-20	26	26	0	0
			2	8	0
			10	0	4
11	21-22	28	28	0	0

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
			4	8	0
			12	0	4
12	23-24	30	30	0	0
			6	8	0
			14	0	4
13	25-26	32	32	0	0
			8	8	0
			16	0	4
14	27-28	34	32	0	0
			10	8	0
			18	0	4
15	29-30	36	32	0	0
			12	8	0
			20	0	4
16	31-32	38	32	0	0
			14	8	0
			22	0	4
17	33-34	40	32	0	0
			16	8	0
			24	0	4
18	35-36	42	32	0	0
			18	8	0
			26	0	4
19	37-38	44	32	0	0
			20	8	0
			28	0	4
20	39-40	46	32	0	0
			22	8	0
			30	0	4
21	41-42	48	32	0	0
			24	8	0
			32	0	4
22	43-44	50	32	0	0
			26	8	0
			32	0	4
23	45-46	52	32	0	0
			28	8	0

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
			32	0	4
24	47-48	54	32	0	0
			30	8	0
			32	0	4
25	49-	56	32	0	0
			32	8	0
			32	0	4

❑ For Windows Server 2008/Windows Server 2008 R2 with SMP configuration

- The relation between the number of processors assigned to an LPAR and the maximum number of ports to be assigned to the LPAR is shown below.
  - SMT disabled: Maximum number of ports = the number of processors x 2 + 4
  - SMT enabled: Maximum number of ports = {(the number of processors + 1) / 2} x 2 + 4
- Intel 10 Gb NIC uses 3 ports of resources for a port. When assigning Intel 10 Gb NIC, 3-port resources are required for one port.
- Emulex 10 Gb NIC uses 4 ports of resources for a port. When assigning Emulex 10 Gb NIC, 4-port resources are required for one port.
- The following table shows examples of I/O assignment to the number of processors.

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
1	1-2	6	6	0	0
			0	2	0
2	3-4	8	8	0	0
			2	2	0
			0	0	2
3	5-6	10	10	0	0
			4	2	0
			2	0	2

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
4	7-8	12	12	0	0
			0	4	0
			4	0	2
5	9-10	14	14	0	0
			2	4	0
			6	0	2
6	11-12	16	16	0	0
			4	4	0
			0	0	4
7	13-14	18	18	0	0
			0	6	0
			2	0	4
8	15-16	20	20	0	0
			2	6	0
			4	0	4
9	17-18	22	22	0	0
			4	6	0
			6	0	4
10	19-20	24	24	0	0
			0	8	0
			8	0	4
11	21-22	26	26	0	0
			2	8	0
			10	0	4
12	23-24	28	28	0	0
			4	8	0
			12	0	4
13	25-26	30	30	0	0
			6	8	0
			14	0	4
14	27-28	32	32	0	0
			8	8	0
			16	0	4
15	29-30	34	32	0	0
			10	8	0
			18	0	4
16	31-32	36	32	0	0

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination		
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 4-port resources used for 1 port
			12	8	0
			20	0	4
17	33-34	38	32	0	0
			14	8	0
			22	0	4
18	35-36	40	32	0	0
			16	8	0
			24	0	4
19	37-38	42	32	0	0
			18	8	0
			26	0	4
20	39-40	44	32	0	0
			20	8	0
			28	0	4
21	41-42	46	32	0	0
			22	8	0
			30	0	4
22	43-44	48	32	0	0
			24	8	0
			32	0	4
23	45-46	50	32	0	0
			26	8	0
			32	0	4
24	47-48	52	32	0	0
			28	8	0
			32	0	4
25	49-50	54	32	0	0
			30	8	0
			32	0	4
26 -	51-	56	32	0	0
			32	8	0
			32	0	4

❑ For Windows Server 2012/Windows Server 2012 R2 without SMP configuration

- The relation between the number of processors assigned to an LPAR and the maximum number of ports to be assigned to the LPAR is shown below.
  - ◆ SMT disabled: Maximum number of ports = the number of processors x 6
  - ◆ SMT enabled: Maximum number of ports = {(the number of processors + 1) / 2} x 6
- Up to 4 ports in Intel 10 Gb NIC can be assigned.
- Intel 10 Gb NIC uses 3 ports of resources for a port. When assigning Intel 10 Gb NIC, 3-port resources are required for one port.
- Emulex 10 Gb NIC uses 2 ports of resources for a port. When assigning Emulex 10 Gb NIC, 2-port resources are required for one port.
- FC uses one port of resources for 4 ports. When assigning FC, 1-port resource is required for four ports.
- The following table shows examples of I/O assignment to the number of processors.

Number of processors/ LPAR		**Maximum number of ports**	**Example of I/O assignment combination**			
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 2-port resources used for 1 port	FC (1 port resource is used for 4 ports)
1	1-2	6	5	0	0	4
			1	0	2	4
2	3-4	12	11	0	0	4
			5	2	0	4
			3	0	4	4
3	5-6	18	17	0	0	4
			5	4	0	4
			9	0	4	4
4	7-8	24	23	0	0	4
			11	4	0	4
			15	0	4	4
5	9-10	30	29	0	0	4
			17	4	0	4
			21	0	4	4
6	11-12	36	32	0	0	16
			23	4	0	4
			27	0	4	4
7	13-14	42	32	0	0	40
			29	4	0	4
			32	0	4	8

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination			
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 2-port resources used for 1 port	FC (1 port resource is used for 4 ports)
8	15-16	48	32	0	0	64
			32	4	0	16
			32	0	4	32
9	17-18	54	32	0	0	64
			32	4	0	40
			32	0	4	56
10-	19-	60	32	0	0	64
			32	4	0	64
			32	0	4	64

❑ For Windows Server 2012/Windows Server 2012 R2 with SMP configuration

- The relation between the number of processors assigned to an LPAR and the maximum number of ports to be assigned to the LPAR is shown below.
  - SMT disabled: Maximum number of ports = the number of processors x 6 -2
  - SMT enabled: Maximum number of ports = {(the number of processors + 1) / 2} x 6 -2
- Up to 4 ports in Intel 10 Gb NIC can be assigned.
- Intel 10 Gb NIC uses 3 ports of resources for a port. When assigning Intel 10 Gb NIC, 3-port resources are required for one port.
- Emulex 10 G 2-port resources are required for one port.
- FC uses one port of resources for 4 ports. When assigning FC, 1-port resource is required for 4 ports.
- The following table shows examples of I/O assignment to the number of processors.

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination			
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 2-port resources used for 1 port	FC (1 port resource is used for 4 ports)
1	1-2	4	3	0	0	4

Number of processors/ LPAR		Maximum number of ports	Example of I/O assignment combination			
SMT disabled	SMP enabled		Dedicated NIC (Intel 1 Gb; Broadcom 1 Gb) Shared NIC/ Virtual NIC (NIC2)	Dedicated NIC (Intel 10 Gb): 3-port resources used for 1 port	Dedicated NIC (Emulex 10 Gb): 2-port resources used for 1 port	FC (1 port resource is used for 4 ports)
2	3-4	10	9	0	0	4
			3	2	0	4
			1	0	0	4
3	5-6	16	15	0	4	4
			3	4	0	4
			7	0	0	4
4	7-8	22	21	0	4	4
			9	4	0	4
			13	0	0	4
5	9-10	28	27	0	0	4
			15	4	0	4
			19	0	4	4
6	11-12	34	32	0	0	4
			21	4	0	4
			25	0	4	32
7	13-14	40	32	0	0	4
			27	4	0	4
			31	0	4	56
8	15-16	50	32	0	0	8
			32	4	0	24
			32	0	4	64
9	17-18	52	32	0	0	32
			32	4	0	48
			32	0	4	64
10	19-	58	32	0	0	56
			32	4	0	64
			32	0	4	64
11-	19-	64	32	0	0	64
			32	4	0	64
			32	0	4	64

Notes on using SR-IOV

This section contains notes about using SR-IOV.

Item			Support specifications
Prerequisite configuration	Server blade		Standard server blades: X55R3/X55S3/X55R4 High-performance server blade: X57A2
	EFI firmware version		09-61/10-61 or later: Standard server blades (X55R3/X55S3) 11-46/12-46 or later: Standard server blades (X55R4) 07-68/08-68 or later: High-performance server blade (X57A2)
	BMC firmware version		07-14 or later: Standard server blades 08-09 or higher: High-performance server blade
	LPAR manager firmware version		59-70 or higher: Standard server blades (X55R3/X55S3) 59-72 or higher: Standard server blades (X55R4) 79-70 or higher: High-performance server blade (X57A2)
	Switch module		Connection only to10 Gb switch module is supported.
	NIC		Emulex 10 Gb NIC
	NIC firmware version		4.6.348.0: Standard server blades (X55R3/X55S3) 10.2.340.10: Standard server blades (X55R4) 4.6.348.0: High-performance server blade (X57A2)
	NIC driver version		When Emulex NIC firmware version is 4.6.x.x: 4.6.352.0 When Emulex NIC firmware version is 10.2.x.x: 10.2.340.7
	OS[1,2, 3, 4, 5]		Red Hat Enterprise Linux 6.4 Red Hat Enterprise Linux 6.5
Settings with SR-IOV	NIC SR-IOV settings[6]		Enabled
	LPAR manager operating mode[7]		LPAR manager expansion mode
	NIC scheduling mode		Shared mode
NIC functions	Performance (Recommendable)	Maximum throughput	about 7 Gbps
		Load on physical processors	Low
		Checksum	Send: on

Item			Support specifications
		offload	Receive: on
		TSO	on
		Maximum MTU size	9000
		RSS (Multi-queue)	Not supported.
		Flow control	Not limited.
		Interrupt interval control	Send/Receive: adaptive off Send/Receive: usecs=128 us
		Transmission bandwidth control	Only Send is supported. Unit: 100 Mbps Range: 100 Mbps to 10000 Mbps
	Virtual port (VF)	Number of Shared ports	16
		Multicast packet	Not limited.
		Broadcast packet	Not limited.
		Promiscuous mode	Not supported.
		ARP table	Not supported.
	Redundancy configuration (bonding)	Monitoring	ARP monitoring/MII monitoring
		Operating mode	balance-rr (mode 0): Not supported. active-backup (mode 1): Supported. balance-xor (mode 2): Not supported. broadcast(mode 3): Not supported. 802.3ad (mode 4): Not supported. balance-tlb (mode 5): Not supported. balance-alb (mode 6): Not supported.
		MAC failover	Supported.
	VLAN[8]	Undef	When Emulex NIC firmware version is 4.6.x.x: Supported When Emulex NIC firmware version is 10.2.x.x: Not supported.
		Port VLAN (Untagged)	Supported. (Only one VLAN can be set to one VF port.)
		Tagged VLAN	Supported. (Only [All] can be set.)
	Inter LPAR communication[9, 10]		Supported.
	Boot from VF	iSCSI FCoE	Not supported.

Item			Support specifications
		PXE	
	Wake On LAN (WOL)		Not supported.
LPAR manager functions	User interface	LPAR manager screen	Supported.
		HvmSh	Supported.
		HVM Navigator	Supported.
	LPAR migration	Shutdown	Supported.
		Concurrent maintenance	Not supported.
	MAC address specified by a user		Supported.
Middleware	HCSM		Not supported.
	SC/BSM		Not supported.
	SC/DPM		Not supported.
	Server installation and monitoring tool (SIMT) log monitor		Supported.
	Linux high reliability options	Linux Tough Dump	Supported.
		HA Network Driver for Linux	Not supported.
		HA Logger Kit for Linux	Supported.

Notes:

1. When you need to execute Force Recovery, shutdown the OS on the LPAR to be deactivated before the execution. If Force Recovery is executed while the LPAR is running, VF NIC will be unavailable on the OS on the LPAR. To recover VF NIC, reboot the OS on the LPAR after Force Recovery is completed.
2. When a VF NIC device is isolated, the following message appears in /var/log/messages. Immediately reboot the guest OS to which the VF NIC device is assigned to release the isolation.
   [/var/log/messages]

```
clocksource tsc unstable (delta = -8589944970 ns)
```

3. When a guest OS, to which VF NIC is assigned, is rebooted, the following messages may appear in /var/log/messages and in the system event log if SIMT log monitor is running. They do not affect the guest OS operation.
   [/var/log/messages]

```
be2net 0000:XX:XX.X: Could not use PCIe error reporting
```

   XX:XX.X: Bus: Dev. Func

   [System event log]

```
Timestamp           Module  Level   System event log                Message
------------------- ------ ------- ----------------------------
yyyy-mm-dd hh:mm:ss  PX       Info 007B D2 7400 32 37XX 39FFFFFF     An error was
detected in H/W agent.
```

   This appears only when 37XX 39FFFFFF (XX depends on the LPAR number) is output.

4. When a guest OS enables promiscuous mode to VF NIC, at tcpdump startup for example, the following messages may appear in /var/log/messages and in the system event log if SIMT log monitor is running. They do not affect the

guest OS operation.
[/var/log/messages]

```
be2net 0000:XX:XX.X: opcode 34-1 failed:status 3-8
```

XX:XX.X: Bus: Dev. Func

System event log

```
Timestamp           Module Level   System event log              Message
------------------- ------ ------- ----------------------------
yyyy-mm-dd hh:mm:ss PX    WARNING 007B D2 7400 32 37XX 34FFFFF  An error was detected
in H/W agent.
```

This appears only when 37XX 39FFFFFF (XX depends on the LPAR number) is output.

5. For RX-ERR RX-DRP RX-OVR and TX-ERR TX-DRP TX-OVR in output results of netstat –i command, a value of the physical port are displayed.
6. Emulex 10 Gb NIC has multiple ports per controller. Set the same value of SR-IOV to ports in the controller: Enable or Disable.
7. When LPAR manager mode is changed from expansion to standard, the definition of virtual NIC numbers: 8 to 15 and VF NIC is forcibly initialized to the not-assigned state.
8. When using path redundancy and VLAN, set the following values.

[When Emulex NIC firmware version is 4.6.x.x]

Item	VLAN mode for LPAR manager	fail_over_mac
ARP monitoring	Undef, Untagged	fail_over_mac=1
MII monitoring	Undef, Untagged	fail_over_mac=1
	Tagged (only [All])	fail_over_mac=0

[When Emulex NIC firmware version is 10.2.x.x]

Item	VLAN mode for LPAR manager	fail_over_mac
ARP monitoring	Untagged	fail_over_mac=1
MII monitoring	Untagged	fail_over_mac=1 (Recommended) fail_over_mac=0
	Tagged (only [All])	fail_over_mac=0

9. When using inter-LPAR communication with VF NIC, set “fail_over_mac=1” to the bonding option. If not, the inter-LPAR communication may not be availabale at switching bonding.
10. Inter-LPAR communication is not available between VF NIC and Shared NIC.

View of Shared NIC/Virtual NIC using the ethtool Command

The following table shows that Shared NIC and Virtual NIC are displayed using the Linux ethtool command, which is for both the onboard mezzanine card and PCI card.

Item	View	
	NIC1	NIC2
Supported ports	TP	FIBRE
Supported link modes	10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full (*)	1000baseT/Full

(*): Actually only 1000baseT/Full is available even though the view shows that 10baseT/100baseT are available.

Remote console

- With remote console connection, SVGA emulation slows down the screen display and mouse behavior of the remote console.
- When the OS of a server blade is in the LP mode, power operation through the remote console is disabled. Therefore, power-on, power-off, reset, and MNI using the remote console are not available.
- If you operate the mouse on the EFI screen or text screen during the guest OS installation, input from the keyboard might slow down. Do not use the mouse on those screens.
- In standard server blades with LPAR manager firmware version 58-1X or earlier, or high-performance server blades with LPAR manager firmware version 78-1X or earlier: When using a USB CD/ DVD-ROM drive or USB FD drive to transfer a large amount of data such as OS installation and LP model or version updating, assign the shared USB device to the target LPAR. Connect directly to the USB port on the front panel of the server blade. The remote DVD/remote FD functions are not available.

Detecting shared NIC linkdown

External devices might detect temporary linkdown of a shared NIC at LPAR manager boot, force recovery, or unexpected reboot.

Breakdown of Inter-LPAR communications

If all the following conditions are met, the inter-LPAR communication in the same LPAR manager using shared NICs, such as 1a and 1b, breaks down.

- With LPAR manager firmware version 57-30 or earlier
- With Linux
- With redundant network configuration, using shared NICs
- When switching networks occurs because some LPARs have detected a failure with redundant configuration using shared NICs

When Route monitoring or ARP monitoring is configured in the redundant network configuration (See Figure 1.), some LPARs may detect a failure. Switching networks occurs in some LPARs, which have detected a failure, not in all LPARs. Thus, each LPAR has different active VNIC, which causes inter-LPAR communication not to be available between the active and standby (See Figure 2).

When MI link monitoring is configured, this trouble does not occur because switching networks occurs in all LPARs at a failure. If switching back causes discrepancy, however this failure occurs.

When you configure a redundant network with virtual NICs, do not use those virtual NICs for inter-LPAR communication. If you need inter-LPAR communication, configure the other virtual NICs, such as Va, that has no redundant configuration.

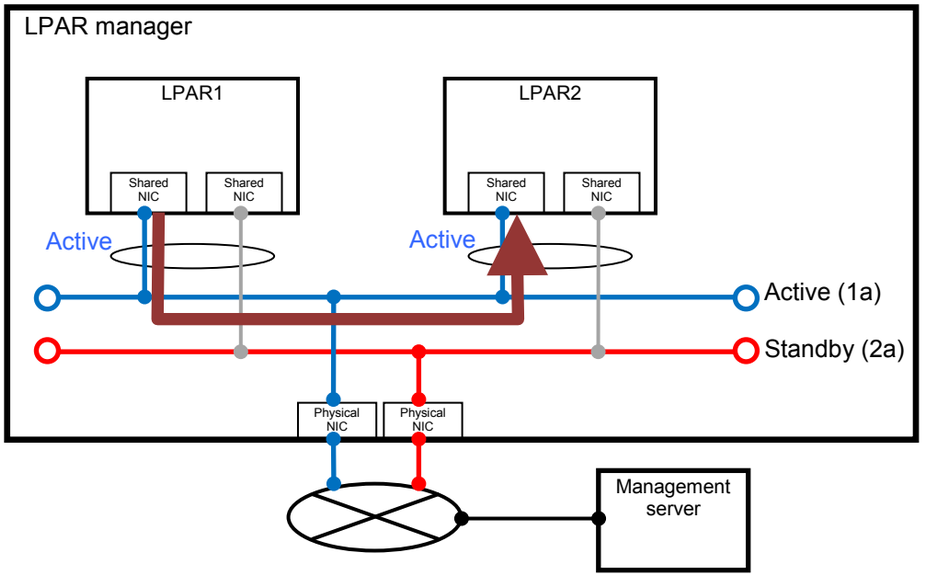


Figure 1: Redundant Network Configuration

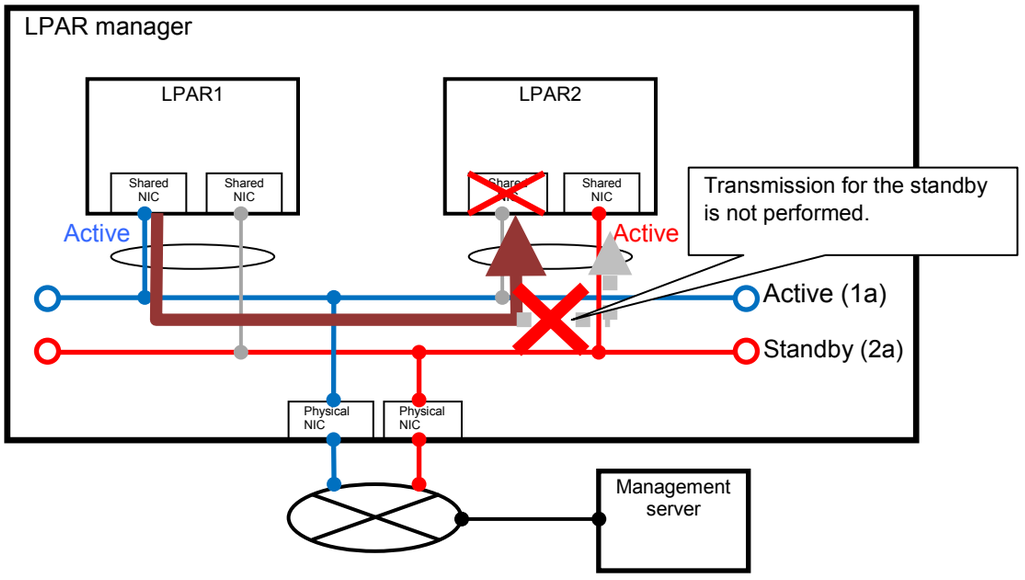
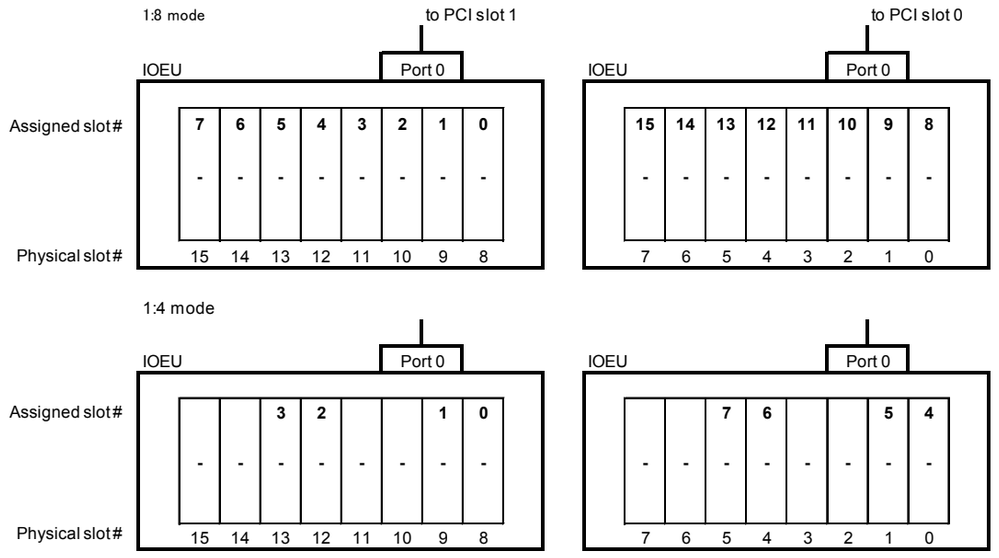


Figure 2: Discrepancy between LPARs

Impact on LPAR manager by I/O slot expansion unit modes

All 16 slots of an I/O slot expansion unit can be divided. The unit has two operating modes, 1:8 mode and 1:4 mode. The task of changing modes is performed only by maintenance personnel. Changing modes can affect LPAR manager as follows:



Impact

When I/O cards are installed in physical slots 4 and 5 (12 and 13) with 1:8 mode, changing modes will change the PCI Bus numbers of those cards as shown in the following table. This will cause the following conditions.

- Windows recognizes the I/O card in the same physical slot# as a new device. If no PCI bus value exists, the driver setting value is the default. If a PCI bus exists, the value that is set to the same assigned slot# before the mode change is applied.
- When I/O cards are installed in physical slots 2 and 3 with 1:4 mode and the mode is changed to 1:8 mode, their PCI Bus numbers will be changed: For Linux, the identifier such as ethx changes; for Windows, the number of Local Area connection changes.
- The number of VNIC segment changes. The segment number of a shared NIC automatically fluctuates as the number of NICs fluctuates.

1:8 mode				1:4 mode			
Physical slot#	Assigned slot#	PCI BUS#	Number of Bus in use	Physical slot#	Assigned slot#	PCI BUS#	Number of Bus in use
0	8	05h-08h	4	0	4	05h-08h	4
1	9	09h-0Ch	4	1	5	09h-0Ch	4
2	10	0Dh	1	2	-	-	-
3	11	0Eh	1	3	-	-	-
4	12	0Fh-12h	4	4	6	**0Dh-10h**	4
5	13	13h-16h	4	5	7	**11h-14h**	4
6	14	17h	1	6	-	-	-
7	15	18h	1	7	-	-	-

1:8 mode				1:4 mode			
Physical slot#	Assigned slot#	PCI BUS#	Number of Bus in use	Physical slot#	Assigned slot#	PCI BUS#	Number of Bus in use
-	-	-	-	-	-	-	-

Action to take

Recheck the device settings including driver functions and boot order, and connection destinations.

If you change modes, there is no impact on virtual NICs and shared NICs.

Timeout for saving configuration

The time-out period for configuration is 10 minutes for standard server blades and 17 minutes for high-performance server blades. With LPAR manager under heavy load conditions, timeout might occur when you are saving the configuration. Check the SYS2 value on the LPAR Usage screen to find how much load is on LPAR manager. When the SYS2 value, Dsp (ms), is 1800 ms or higher, a heavy load on LPAR manager might cause the timeout. If it occurs due to a temporary increase in load, save the configuration again after the load decreases.

Settings for WWN and MAC address

The following table describes whether or not to use Default Physical WWN/Optional Physical WWN and Default Physical MAC address/Optional Physical MAC address.

Item	Default Physical WWN	Optional Physical WWN
Dedicated FC	Available	Not available
Shared FC	Available	Not available

Item	Default Physical MAC	Optional Physical MAC
Dedicated NIC	Available*	Available
Shared NIC/Virtual NIC	Available	Not available

* : MAC address is not taken over at N+M failover.

N+M Cold Standby

- When using a non-standby partition as a standby partition, follow the steps below:
  1. Back up configuration information on a non-standby partition using the UBR command of SVP command mode.
  2. Configure the non-standby partition to a standby partition, and build N+M cold standby for operation.
- When using a standby partition as a non-standby partition, follow the steps below:
  1. Configure a standby partition to a non-standby partition to release the N+M cold standby.
  2. Configure the non-standby partition to the LP mode and start it.
  3. If some configuration is backed up, finish LPAR manager and restore the configuration using the UBR command of SVP command mode.



If you do not follow the steps above, more than one WWN or MAC address can exist and can cause serious problems. Make sure to use the steps above.

Time Setting in Switchover and Recovery with N+M Cold Standby

This subsection describes the time setting in switchover and recovery in N+M cold standby environment.

- Problem

  Time difference might occur when switchover or recovery occurs in the N+M cold standby environment due to the difference for BIOS time in specifications on the OS.

- This problem might occur if all the following three conditions are satisfied.

  (1) The Compute Blade System uses the N+M cold standby function.

  (2) The following OSs shown in (a) and (b) are mixed in the same N+M cold standby group.

  (a) OSs that recognize BIOS time as local time

  - Windows
  - Red Hat Enterprise Linux with Local time as a setting value

  (b) OSs that recognize BIOS time as UTC

  - Red Hat Enterprise Linux with UTC as a setting value

  (3) An active server blade with (a) running is switched to a standby server blade with BIOS time as UTC, or the former active server blade is switched back. Or an active server blade with (b) running is switched to a standby server blade with BIOS time as local time, or the former active server blade is switched back.

  (4) For standard server blade X55R4 model, RTC time synchronization is disabled. If N+M group includes LPAR manager, RTC time synchronization is not available. See “RTC time Synchronization at N+M Cold Standby Failover” in Chapter 13 for details.

■ Solutions

Configure the BIOS time setting using the following measures on the BIOS setup screen for standby server blades, or on the OS or virtual platform for server blades other than standby ones, and then reflect the setting value to BIOS time.

When powering on the standby server blade for checking or setting BIOS time, disable N+M cold standby. Then, enable N+M cold standby after checking or setting BIOS time. If you power on the standby server blade with N+M cold standby enabled, the state will turn to warning.

For standard server blade X55R4 model, enable RTC time synchronization without executing the following procedure. See “RTC time Synchronization at N+M Cold Standby Failover” in Chapter 13 for details.

- If all the OSs and virtual platforms in the same N+M standby group can be (2)-(a), BIOS time as local time

  When configuring the system

  Set your local time to all server blades including a standby server blade in the N+M standby group.

  When changing server blades

  Check that the local time is shown for BIOS time of the server blade before OS startup.

- If all the OSs and virtual platforms in the same N+M standby group can be (2)-(b), UTC time as local time,

  When configuring the system

  Set UTC to all server blades including a standby server blade in the same N+M standby group.

  When changing server blades

  Check UTC is shown for BIOS time of the server blade before OS startup.

Time difference at N+M cold standby

Time difference might occur in LPARs when partitions are switched under N+M cold standby environment. If it occurs, adjust the time on the guest OS.

When the failed partition is recovered, perform the following steps.

1. Start the active partition, and then set the system equipment time with the setup menu.
2. Restore configuration from the standby partition to the active partition.
3. Perform Adjust LPAR Time on the Date and Time screen.
4. Save the configuration with **F9: Save Configuration** on the LPAR manager Menu screen.
5. Activate the LPAR.

N+M cold standby with virtual NIC system number expansion

The following table shows whether N+M cold standby is supported due to expansion of the NIC system number. LPAR manager firmware version on the standby server blade is later than that on the active server blade.

Active		Standby	N+M cold standby Supported?
Expansion of virtual NIC system number	**Virtual NIC system number**	**Expansion of virtual NIC system number**	
Not supported	1 to 128	Not supported	Supported
		Supported	Supported *1
Supported	1 to 128	Not supported	Not supported
		Supported	Supported
	129 or greater	Not supported	Not supported
		Supported	Supported

*1: If you expand virtual NIC system numbers to 129 in the standby server blade, data cannot be restored from the standby server blade to the active server blade.

UPS (Uninterruptible Power Supply)

It takes about 30 seconds longer for server blades to shut down after a power failure than that in the basic environment. It might take more seconds depending on the number of activated LPARs.

Powering off LPAR manager

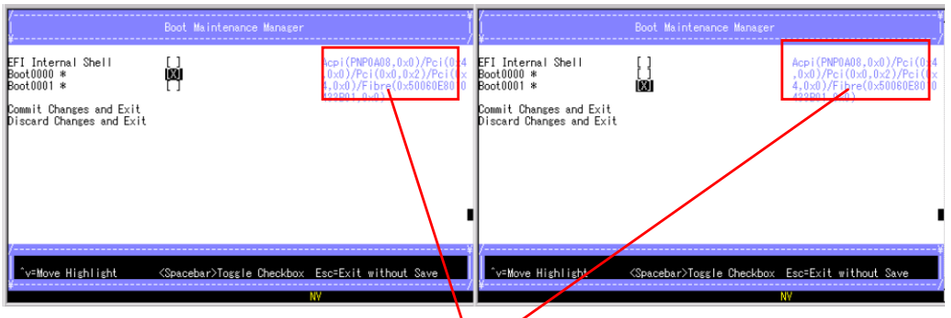
Do not power off LPAR manager using the server blade Web console or management module. If you do, LPAR manager might not boot properly.

Deactivate all LPARs, and then shut down LPAR manager using Alt + r keys in the LPAR manager screen. See Quit for further details.

Boot option settings

When the same device path is registered in different boot options, you might fail to install or boot the OS. This problem has occurred in Windows Server 2008 Enterprise and Windows Server 2008 Enterprise SP2 editions.

The following is an example where the same device path is registered in different boot options.



Screen with Boot0000 selected

Screen with Boot0001 selected

The same device path is registered in both Boot0000 and Boot0001.

The following steps will cause this problem.

1. Activate an LPAR, and then select “Continue” in the logical BIOS screen to enter EFI Shell.
2. Through EFI Shell, select “Boot Maintenance Manager” in the logical BIOS screen, and register a device path with Add Boot Option.

Performing Step 1 might cause the device path to be automatically registered in the boot option. If a device path is automatically registered, performing Step 2 allows the same device path to be registered.

If so, delete one boot option to which the device path is registered using Delete Boot Option, then install the OS, and then boot the OS.

Shared FC port status

It is highly recommended that you should set the shared FC port status to Available. When the shared port status is set to LinkDown, more time is required for booting LPAR manager and changing the scheduling mode of the PCI device depending on the number of LinkDown ports. The following table shows the relation between the number of installed ports and required time for execution.

All FC ports installed	Time required for LPAR manager boot (seconds)		Time required for changing scheduling mode of PCI device and for executing ForceRecovery (seconds)	
Port status	Available	LinkDown	Available	LinkDown
2	2’42”	4’4”	1’7”	1’48”
4	3’3”	4’22”	1’19”	3’45”
8	3’35”	6’23”	1’55”	5’33”
16	4’40’	10’3”	2’54”	9’21”
32	6’36”	16’51”	4’49”	16’29”
64	10’40”	31’55”	9’51”	30’47”

Notes on LPAR manager shutdown

There is no way to check when the LPAR manager configuration is saved. If the time is unknown, you need to save the LPAR manager configuration before shutting down LPAR manager. Press **F9 Save Configuration** on the LPAR manager Menu screen to save LPAR manager configuration. If you shut down or reboot LPAR manager before saving the configuration, newly changed values will be lost. See Save configuration changed on LPAR manager screen for information about how to save LPAR manager configuration.

Flash memory failure

- It is strongly recommended that you should regularly create backup files of LPAR manager configuration in case of flash memory failure.

LPAR manager firmware 58-5X/78-5X or later versions automatically recover from flash memory failure if it is not critical. A log “LPAR manager Loader detected the damage of flash memory and load configuration files from SVP.” is collected in the LP system log at automatic recovery. If this system log is collected every time you boot LPAR manager, contact your reseller or consult maintenance personnel.

Performance slowdown in management path

When the processor usage rate is significantly high in the LPAR manager network communication due to the heavy load on the shared NIC, performance in the LPAR manager management path can slow down and cause the following problems.

- It takes longer, six minutes or longer, to save LPAR manager configuration information.
- It takes longer, 30 minutes or longer for 1Gbps interface, to upload the firmware update in operation.
- It takes longer for HvmSh to respond to a command, or timeout occurs.
- Registering or updating LPAR manager with HVM navigator fails due to the communication error.
- Operation to LPAR manager from SC/BSM fails due to the timeout.
- LP Web system, logical VGA snapshot, is not displayed, or refreshing the display takes longer.
- It takes longer, five minutes or longer, to collect LPAR manager dumps.

You can find a value of the processor usage rate in the LPAR manager network communication as a value of SYS2 on the LPAR Usage screen. When a problem shown above occurs, check the SYS2 value on the LPAR Usage screen. If 1800 ms or larger is shown as Dsp (ms) in SYS2, the heavy load on the shared NIC is supposed to cause the problem.

When a heavy load on the shared NIC causes such a problem, reconfigure the network configuration of the shared NIC and the load on it.

When the heavy load is temporary, perform the failed operation again after the load is relieved.

Note on Oracle IPMI

Do not use Oracle IPMI, which might cause trouble such as guest OS hangup.

LPAR manager setting item

This section describes setting items when LPAR manager is introduced.

LPAR manager system setting

The following table shows LPAR manager system setting items.

Setting screen & Setting field	Description for setting field	Default
Server Blade Web console		
LPAR manager setting		
EFI	Set EFI.	-
OS mode	Basic or LP mode	LP mode
LPAR manager firmware bank number	Specify an LPAR manager FW bank number (#0/1)	0
LPAR manager screen		
System configuration		
LP IP address Subnet Mask Default Gateway	IP address needed for LPAR manager-SVP/BSM communication (IP address for the management segment; different from the SVP IP address)	-
VNIC System No	Set a unique value to each LPAR manager system, including Compute Blade 1000, Compute Blade 2000, and Compute Blade 320.	0
LP ID	LPAR manager identifier The default value created automatically from the LP IP address is recommended.	LPAR manager + IP address
Alert Language	Language used for alert notices	-
BSM IP address BSM Alert Port	Management server address setting, such as SC and BSM	-
Virtual Console Port	Port number used in the virtual COM console	20801
LPAR manager Operating Mode	LPAR manager operating modes	Standard
LP CLI IP Address	Management server address for commands such as HvmSh and HvmGetPerf.	0.0.0.0
Date and time		
System Time Zone	SEL time zone in LPAR	+ 0 hour
Display time	Time period for display on the screen	RTC
TimeSynch	Selection in settings for synchronizing time with NTP servers.	Disable
Options		
Pre-State Auto Activation	Restores an LPAR to a state before the restore if the LPAR is unexpectedly rebooted.	No

Setting screen & Setting field		Description for setting field	Default
	LP Auto Shutdown	LP system shutdown when all LPARs are deactivated.	No
	LP Error Watching	LPAR manager hang up detection	Yes
	PhyCPU C-State (>= C3)	Power capping	Enable
	USB Auto Allocation to LPAR	USB auto attachment	Enable
	Save Changed Config Format	Saves a changed configuration format.	Disable
	LP TimerCounter Base	Calculates a Timer Counter value.	TSC
	Save Time Config	Saves time configuration automatically.	Disable
	Activation	Confirmation of LPAR Activation operation	Yes
	Deactivation and Reactivation	Confirmation of LPAR Deactivation operation	Yes
	Screen Switching Character	Character for switching between the LPAR manager screen and guest serial screen	L(lowercase L)

LPAR manager partition setting

The following table shows LPAR manager partition setting items.

Setting screen & Setting field	Description for setting field	Default
LPAR manager screen		
Logical partition configuration		
LPAR creation	Creates LPAR (Logical PARtition).	No LPAR definition
LPAR name	8-character name is recommended. Up to 31 English characters or numbers can be used.	NO_NAME
CPU schedule (Shr/Ded or Scd))	Dedicated or Shared	Dedicated
CPU number (Pro)	Number of CPUs for LPAR	1
Processor group (Grp)	A processor group number	0
Memory size (Mem)	LPAR memory size (in 256 MB unit)	1024
Service rate (Srv)	LPAR service rate of a shared CPU	100
Memory node (MN)	Sets a memory node number to assign to LPAR only when NUMA is enabled.	A
Idle detection (ID)	Idle detection function of a guest CPU	Y
ProcessorCapping (PC)	Capping function for shared CPU service	* Not assigned.
AutoAct setting (AA)	Activates LPAR automatically when LPAR manager boots.	* Not assigned.
AutoClear setting (AC)	Automatically clears SEL for LPAR	N
Virtual COM console (VC)	Set “Y” or a VC number when using the virtual COM console.	N
Pre-boot setting (PB)	None but BIOS can be selected.	BIOS
Logical processor configuration		
Dedicated processor mapping	Relates a physical CPU to a logical CPU.	D *1
Physical processor configuration		
Processor group number setting	Sets the number of a processor group.	0
PCI device assignment		
PCI device schedule (Schd)	Dedicated (D) or Shared (S)	Dedicated
PCI device assignment (Type:U)	Assigns the front USB and remote console to LPAR.	A (Assign.)
PCI device assignment (Type:N)	Assigns the Network card to LPAR	- (Assign-ment not allowed)
PCI device assignment (Type:F)	Assigns HBA to LPAR.	- (Assign-ment not allowed.)
VNIC assignment		
VNIC device type	Sets the type of a VNIC device	NIC1

Setting screen & Setting field		Description for setting field	Default
	Shared NIC setting	Assigns shared NIC to LPAR.	* (Not assigned.)
	VF NIC setting	Assigns VF NIC to LPAR	* (Not assigned.)
	Virtual NIC setting	Assigns virtual NIC to LPAR	* (Not assigned).
	VLAN setting	Sets VLAN to shared NIC and virtual NIC	*(Not assigned.)
	Promiscuous mode setting	Sets promiscuous mode to shared NIC and virtual NIC.	- T for Shared NIC and virtual NIC - R for VF NIC
	Inter-LPAR packet filtering	Sets inter-LPAR packet filtering for shared NICs.	Disable
	Transmission bandwidth limitation	Sets transmission bandwidth limitation for LPAR.	10000 Mbps
Shared FC assignment			
	VfcID setting	Assigns shared FC to LPAR	* (Not assigned.)
Date and time			
	Logical SEL time mode	Time mode for logical SEL	Local
	Logical SEL time zone	Time zone for logical SEL (The time zone is set when adding LPARs.)	Same as the system

*1: Displays [A] with standard server blades with LPAR manager firmware 58-3X or later versions and high performance server blade with LPAR manager firmware 78-3X or later versions.

* (Not assigned): [*] is displayed in the default field, which shows “not assigned” by default but the assignment is available.

- (Not assigned): [-] is displayed in the default field, which shows “not assigned” by default and the assignment is not available.

HBA EFI driver setting

The following table shows LPAR manager EFI driver setting items.

Setting screen & Setting field		Description for setting field	Default
EFI shell			
drivers command: checks the driver handle.			
drvdfg command: checks the controller handle, and starts HBA option setting shell.			
HBA setting shell (HBA EFI driver)			
select command: Selects an adapter to set the option parameter.			
Basic option (set command)			
	Boot Function	Set “SAN boot” function to Enabled or Disabled per port. Make sure to set the FC port to Enabled.	Disabled
	Connection Type	Specify the connecting form of the FC interface: - When connected via FC switch, set “Auto” or “Point to Point” as a connection type. - When connected direct to the disk array device, set Loop as a connection type. (Only setting value reference is available in the FC shared mode.)	Auto
	Data Rate	Specify the data transmission rate for the FC interface: usually “Auto”. (Only setting value reference is available in the FC shared mode.)	Auto
	Spinup Delay	Set “Spinup Delay” to Enabled or Disabled and also wait time for a disk.	Disabled
	Login Delay Time	When login delay is necessary in configuration with multiple nodes connected to the FC-SW such, as cascade connection, specify the time to delay.	3 sec
	Persistent Bindings	Can specify whether or not the OS driver performs following the “Persistent Bindings” function in the Linux system.	Enabled.
	Force Default Parameter	When it is necessary for the OS driver (Windows or Linux) to boot with the default setting instead of the setting saved on the OS, set it to Enabled.	Disabled
	Select Boot Device	Set “Boot Device List” to Enabled or Disabled. - Enabled: Boot device search is limited to devices registered in the Boot Device List. - Disabled: Searches the device currently connected, ignoring the Boot Device List.	Disabled
	Boot Device List	Registers the Boot Device List used when Select Boot Device is set to “Enabled”. Only devices registered in the list are searched. If all devices cannot be detected, the currently connected device will not be searched.	(All Zero)

Setting screen & Setting field		Description for setting field	Default
		If exceeding Total number of LU, Number of LU per HBAFC Port, the entries remained in the list will be ignored.	

LPAR manager setting change and affected area

The following table shows LPAR manager items to change settings and areas to be affected by the change.

LPAR manager setting change	Affected area				
	LPAR (Target LPAR)	LPAR (Other LPAR)	LPAR manager (Service)	LPAR manager (System)	Remarks
System information update					
LP IP address	✓	✓	✓	-	Deactivate all LPARs. Reflecting the change makes NICs of all LPARs linkdown, which causes the network communication between servers running on LPARs to stop for several minutes. SC/BSM shows that the LPAR manager state is Deactivate, for which no error notification is performed.
Subnet Mask/ Default Gateway	✓	✓	✓	-	
Alert Language	✓	✓	✓	-	
VNIC System No	✓	✓	✓	-	
LP ID	✓	✓	✓	-	
Virtual console port	✓	✓	✓	-	
BSM IP address *3	✓	✓	✓	-	
BSM Alert Port *3	✓	✓	✓	-	
LP CLI IP Address	-	-	-	-	Deactivating the target LPAR is not required.
LPAR manager Operating Mode	✓	✓	✓	✓	Rebooting the server blade is required.
Change in LP option setting					
Pre-State Auto Activation	-	-	-	-	Deactivating target LPARs is not required.
LP Auto Shutdown	-	-	-	-	
LP Error Watching	-	-	-	-	
Confirmation Activation	-	-	-	-	
Confirmation Deactivation	-	-	-	-	
Screen Switching Character	-	-	-	-	
USB Auto Allocation to LPAR	-	-	-	-	
Save Changed Config Format	-	-	-	-	
Save Time Config	-	-	-	-	
PhyCPU C-State (>= C3)	✓	✓	-	-	Deactivating all LPARs is required.
LP TimerCounter Base	✓	✓	✓	✓	Rebooting the server blade is required.
Change in resource/function assigned to LPAR					
LPAR name change	✓	-	-	-	Deactivating target LPARs is required.
Change in CPU schedule *1	✓	-	-	-	
Change in the number of CPU	✓	-	-	-	
Change in processor group *2	✓	-	-	-	

LPAR manager setting change	Affected area				
	LPAR (Target LPAR)	LPAR (Other LPAR)	LPAR manager (Service)	LPAR manager (System)	Remarks
Memory size (Mem) change	✓	-	-	-	
Memory node number (MN) change	✓	-	-	-	
AutoAct (AA) setting change	✓	-	-	-	
AutoClear (AC) setting change	✓	-	-	-	
Service rate (Srv) change	✓	✓	-	-	Performance of the LPARs using a shared CPU changes between before and after the setting change.
Idle detection (ID) change	✓	-	-	-	Performance of the target LPARs changes between before and after the setting change.
ProcessorCapping (PC) setting change	✓	-	-	-	
Virtual COM console (VC) setting change	-	-	-	-	Deactivating the target LPARs is not required.
Change in device assignment to LPAR and setting					
USB device assignment	-	-	-	-	Assign a device to the LPAR deactivated, and attach the device to the LPAR activated.
NC/FC scheduling mode change	✓	✓	✓	-	Deactivate all LPARs..
VNIC Device Type setting	-	-	-	-	Deactivating the target LPARs is required. .
NIC assignment/ unassignment	✓	-	-	-	
MAC address change of NIC	✓	-	-	-	
FC assignment/ unassignment	✓	-	-	-	
FC vfcID change	✓	-	-	-	
VLAN setting to NIC	-	-	-	-	Deactivating the target LPARs is not required. To set VLAN to VF NIC, deactivating target LPARs is required.
Promiscuous setting to NIC	-	-	-	-	
Inter-LPAR packet filtering setting to NIC	-	-	-	-	
Addition and deletion of LPAR					
LPAR addition/deletion	✓	-	-	-	Deactivate an LPAR to delete.
LPAR activation	✓	-	-	-	
LPAR deactivation	✓	-	-	-	
LPAR manager firmware update					
LPAR manager firmware update	✓	✓	✓	✓	Make sure to reboot the server blade before execution with the updated firmware.
System transfer					
Transfer from LP mode to Basic mode	✓	✓	✓	✓	Make sure to reboot the server blade.

LPAR manager setting change	Affected area				
	LPAR (Target LPAR)	LPAR (Other LPAR)	LPAR manager (Service)	LPAR manager (System)	Remarks
Transfer OS from a LPAR manager environment to another LPAR manager environment *4	✓	-	-	-	Make sure to change the setting of the SAN boot environment, even if only the target LPAR is affected.
Transfer OS from Basic environment to LPAR manager environment	✓	-	-	-	
Transfer OS from LPAR manager environment to Basic environment	✓	-	-	-	

✓: affected, such as needing to deactivate LPAR.

- : not affected.

*1: Target LPARs need to be deactivated with standard server blades with LPAR manager firmware 58-3X or later versions or high-performance server blades with LPAR manager firmware 78-3X or later versions.

*2: Target LPARs need to be deactivated in the shared mode.

*3 Target LPARs need to be deactivated with standard server blades with LPAR manager firmware 58-4X or later versions or high-performance server blades with LPAR manager firmware 78-4X or later versions.

*4: For LPAR migration in concurrent maintenance mode, deactivating the target LPAR is not needed.

Port numbers used by LPAR manager

The following tables show port numbers used by LPAR manager.

Item	Protocol	Port number	Communication direction (LPAR manager - Management server)	Description	Remarks
HvmSh (HvmGetPerf)	UDP	623	←	Includes HvmSh Script, HVM Navigator, PFM, ITRM and HCSM.	RMCP
	TCP	23250, 20670	←		
LPAR migration	TCP	23401, 20671	←	LPAR migration	
Virtual COM console	TCP	20801 to 20816*1	←	Virtual COM console	
LP Web system	TCP	80, 443	←	LPAR manager firmware update, Logical VGA snapshot	HTTP, HTTPS
NTP	TCP	123	→	Time synchronization	NTP
Guest memory dump, LPAR manager dump collection command	TCP	21, 21	→	Dump collection	FTP
SC/BSM	TCP	20079	→	Transmission to the manager service	
	TCP	21001	←	Transmission from the manager service	

*1: the default port number

System configuration

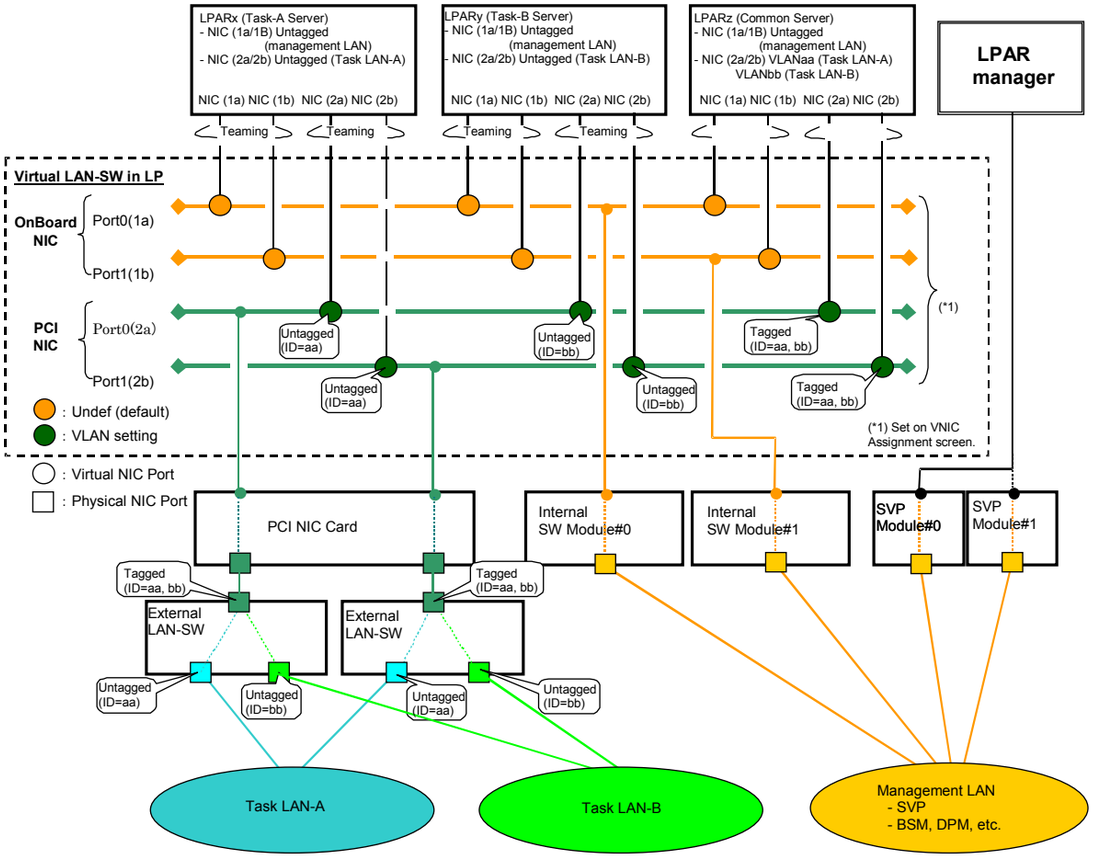
Example of system configuration (network)

The following is an example of system configuration in the LPAR manager environment.

This system configuration is described from the network setting view.

Set three LPAR (partitions) on LPAR manager, and configure a task-A server, task-B server, and common server for each LPAR.

- Set Untagged to the task-A server and task-B server with the LPAR manager virtual LAN-SW, not set VLAN on the OS, and each server communicate with task LAN-A and task LAN-B respectively. To communicate with the management LAN, the onboard dedicated NIC is used. VLAN is not set.
- Set VLAN to the common server on the OS, which allows it to communicate with task LAN-A and task LAN-B via LPAR manager virtual LAN-SW with Tagged setting. To communicate with the management LAN, the onboard dedicated NIC is used. VLAN is not set.
- LPAR manager uses the dedicated NIC, and connects to the management LAN. Using this path, LPAR manager communicate with SVP and the management server (SC/BSM) in the management LAN.


LPARx (Task-A Server)
- NIC (1a/1B) Untagged
(management LAN)
- NIC (2a/2b) Untagged (Task LAN-A)
NIC (1a) NIC (1b) NIC (2a) NIC (2b)
LPARy (Task-B Server)
- NIC (1a/1B) Untagged
(management LAN)
- NIC (2a/2b) Untagged (Task LAN-B)
NIC (1a) NIC (1b) NIC (2a) NIC (2b)
LPARz (Common Server)
- NIC (1a/1B) Untagged
(management LAN)
- NIC (2a/2b) VLANaa (Task LAN-A)
VLANbb (Task LAN-B)
NIC (1a) NIC (1b) NIC (2a) NIC (2b)
LPAR manager
Teaming
Teaming
Teaming
Teaming
Virtual LAN-SW in LP
OnBoard NIC
Port0(1a)
Port1(1b)
PCI NIC
Port0(2a)
Port1(2b)
Untagged (ID=aa)
Untagged (ID=bb)
Tagged (ID=aa, bb)
Untagged (ID=aa)
Untagged (ID=bb)
Tagged (ID=aa, bb)
(*1)
: Undef (default)
: VLAN setting
(*1) Set on VNIC Assignment screen.
: Virtual NIC Port
: Physical NIC Port
PCI NIC Card
Internal SW Module#0
Internal SW Module#1
SVP Module#0
SVP Module#1
Tagged (ID=aa, bb)
Tagged (ID=aa, bb)
External LAN-SW
External LAN-SW
Untagged (ID=aa)
Untagged (ID=bb)
Untagged (ID=aa)
Untagged (ID=bb)
Task LAN-A
Task LAN-B
Management LAN
- SVP
- BSM, DPM, etc.

Example of system configuration (connected to storage via FC switch)

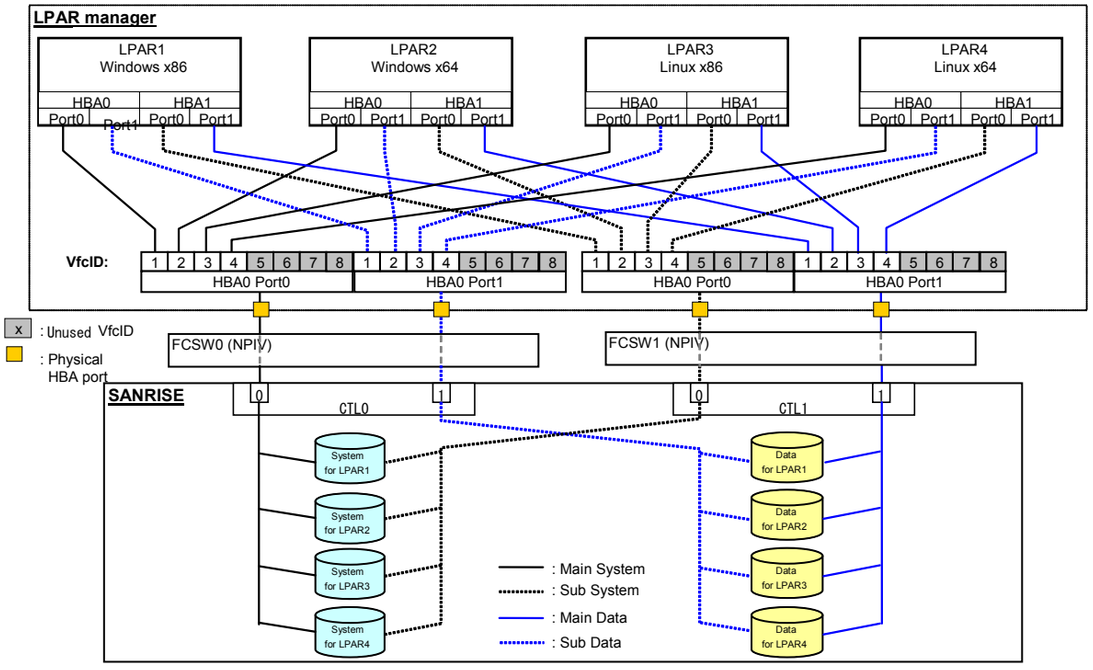
An example of connection to storage via FCSW with 4-Gbps Fibre-channel adapter is as follows:

This example is described in terms of storage.

Four partitions (LPARs) are configured in LPAR manager, each of which is allocated a system path and data path. They are implemented redundancy with redundancy software such as HiCommand Dynamic Link Manager (HDLM) and Hitachi Fibre Channel – Path Control Manager (HFC-PCM).

- The four ports share each HBA port using the FC sharing function.
- Make sure to connect the storage via FCSW to use the FC sharing function with 4 Gbps fiber channel adapter. Enable the N-Port ID Virtualization (NPIV)function of FCSW for using the NPIV function of FCSW.
- Multiple LPARs can share a single HBA port. To share a port, allocate the port to LPARs on the LPAR manager screen using the WWN identifier (vfcID). The following is an example for allocation with vfcID (1 to 8) in this configuration.

vfc ID	HBAO		HBA1	
	Port 0	Port 1	Port 0	Port 1
1	LPAR1 allocated	LPAR1 allocated	LPAR1 allocated	LPAR1 allocated
2	LPAR2 allocated	LPAR2 allocated	LPAR2 allocated	LPAR2 allocated
3	LPAR3 allocated	LPAR3 allocated	LPAR3 allocated	LPAR3 allocated
4	LPAR4 allocated	LPAR4 allocated	LPAR4 allocated	LPAR4 allocated
5	Unused	Unused	Unused	Unused
6	Unused	Unused	Unused	Unused
7	Unused	Unused	Unused	Unused
8	Unused	Unused	Unused	Unused


LPAR manager
LPAR1
Windows x86
LPAR2
Windows x64
LPAR3
Linux x86
LPAR4
Linux x64
HBA0
HBA1
Port0
Port1
VfcID:
1 2 3 4 5 6 7 8
HBA0 Port0
HBA0 Port1
x : Unused VfcID
: Physical HBA port
FCSW0 (NPIV)
FCSW1 (NPIV)
SANRISE
CTL0
CTL1
System for LPAR1
System for LPAR2
System for LPAR3
System for LPAR4
Data for LPAR1
Data for LPAR2
Data for LPAR3
Data for LPAR4
: Main System
: Sub System
: Main Data
: Sub Data

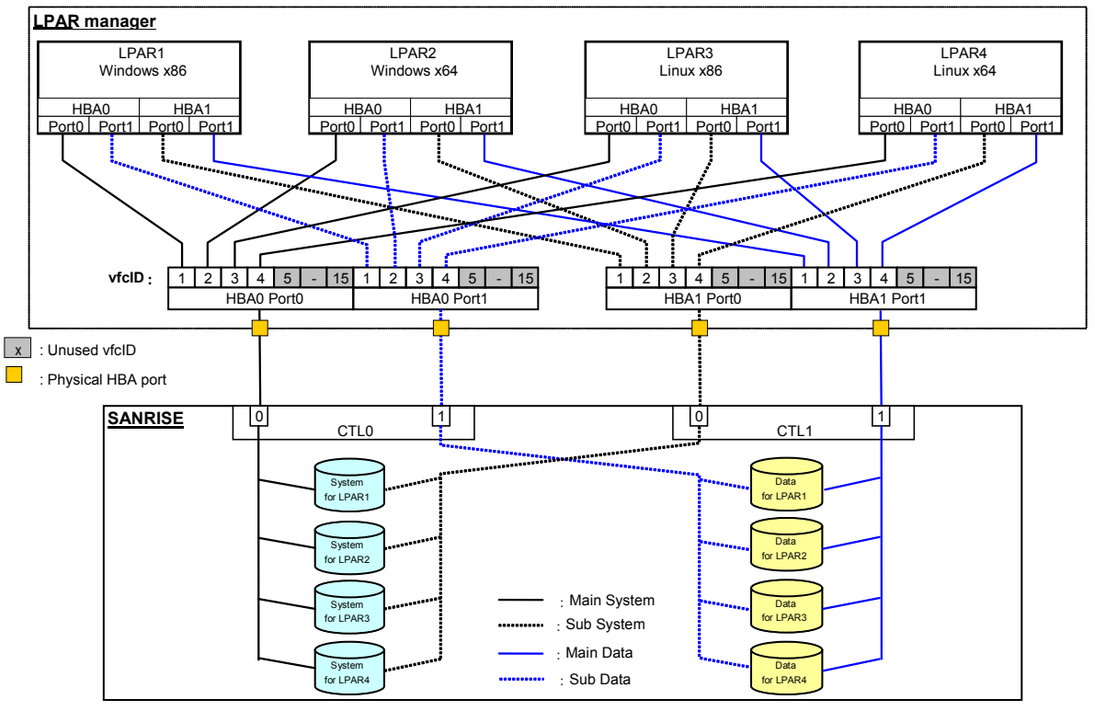
Example of system configuration (directly connected to storage)

An example of connection directly to storage with 8-Gbps Fibre-channel adapter is as follows:

Four partitions (LPARs) are configured in LPAR manager, each of which is allocated a system path and data path. They are implemented redundancy with redundancy software such as HDLM and HFC-PCM.

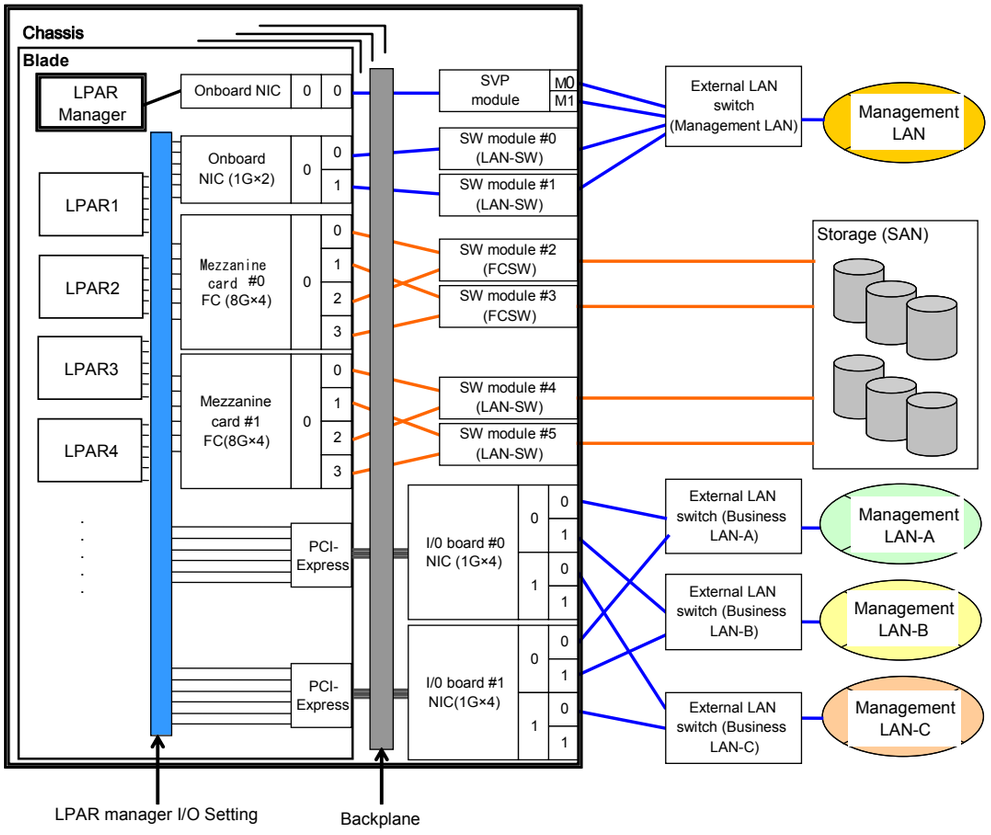
- The four ports share each HBA port using the FC sharing function.
- Make sure to connect the storage via Loop to use the FC sharing function with 8 Gbps Fibre-channel adapter. See How to use the shared FC function (II) with connection directly to storage for details.
- Multiple LPARs can share an HBA port. To share a port, allocate the port to LPARs on the LPAR manager screen using the WWN identifier (vfcID). The following is an example for allocation with vfcID (1 to 15) in this configuration.

vfc ID	HBAO		HBA1	
	Port 0	Port 1	Port 0	Port 1
1	LPAR1 allocated	LPAR1 allocated	LPAR1 allocated	LPAR1 allocated
2	LPAR2 allocated	LPAR2 allocated	LPAR2 allocated	LPAR2 allocated
3	LPAR3 allocated	LPAR3 allocated	LPAR3 allocated	LPAR3 allocated
4	LPAR4 allocated	LPAR4 allocated	LPAR4 allocated	LPAR4 allocated
5	Unused	Unused	Unused	Unused
|	Unused	Unused	Unused	Unused
15	Unused	Unused	Unused	Unused


LPAR manager
LPAR1
Windows x86
LPAR2
Windows x64
LPAR3
Linux x86
LPAR4
Linux x64
HBA0
HBA1
Port0
Port1
vfcID :
1 2 3 4 5 - 15 1 2 3 4 5 - 15
HBA0 Port0
HBA0 Port1
HBA1 Port0
HBA1 Port1
x : Unused vfcID
: Physical HBA port
SANRISE
0
1
CTL0
CTL1
System for LPAR1
System for LPAR2
System for LPAR3
System for LPAR4
Data for LPAR1
Data for LPAR2
Data for LPAR3
Data for LPAR4
: Main System
: Sub System
: Main Data
: Sub Data

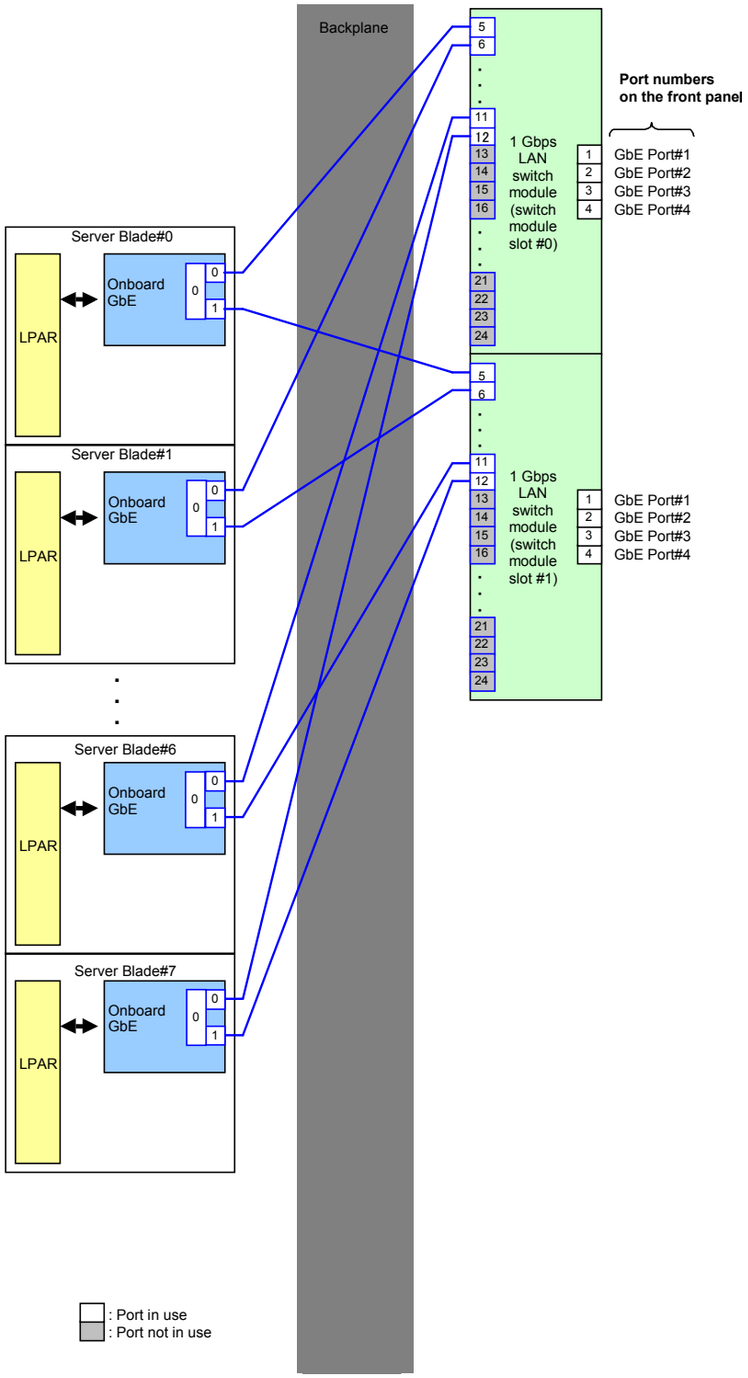
Example of system configuration (hardware configuration)

The following example shows configuration where two mezzanine cards (8 Gbps Fibre-channel x4) are installed in the expansion slots 0/1 and two PCI cards (1 Gbps Ethernet x4) are installed in the I/O board module slots 0/1.



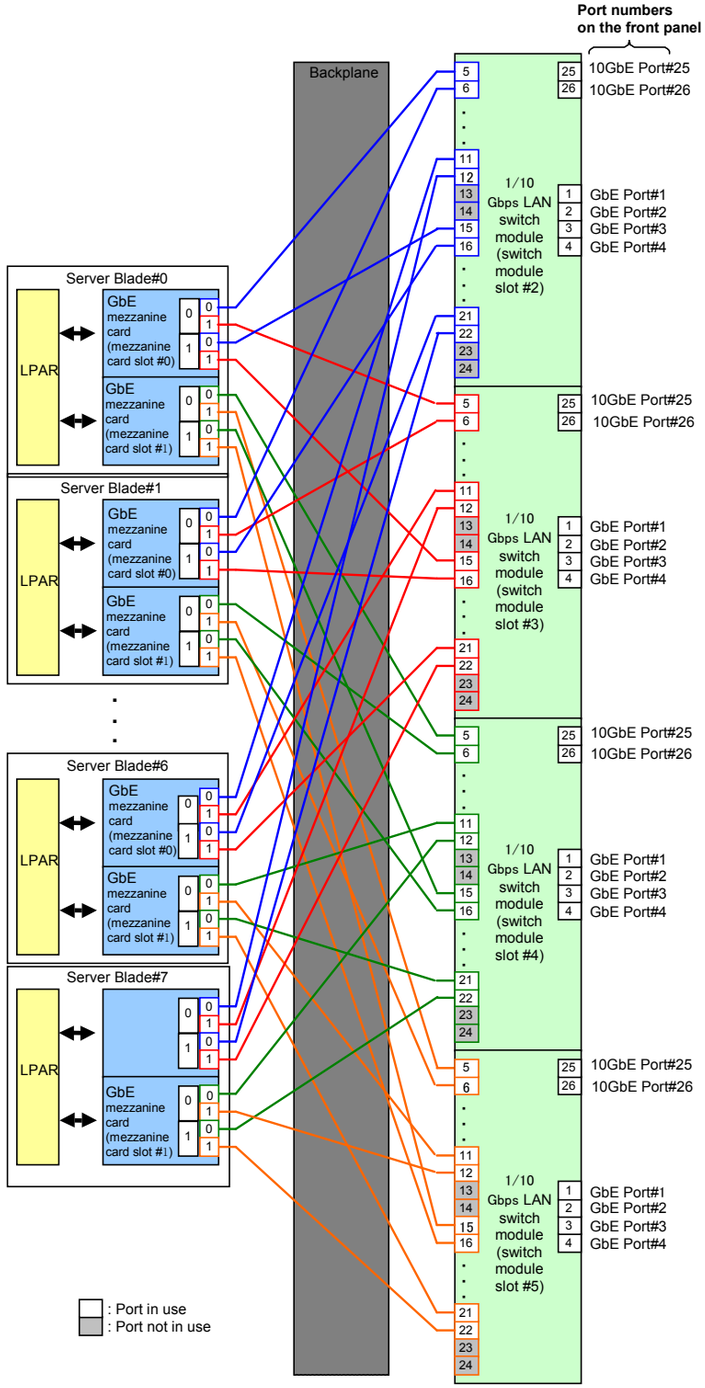
Connection to 1 Gbps LAN switch module

The following figure shows a connection between onboard GbEs and 1-Gbps LAN switch modules.



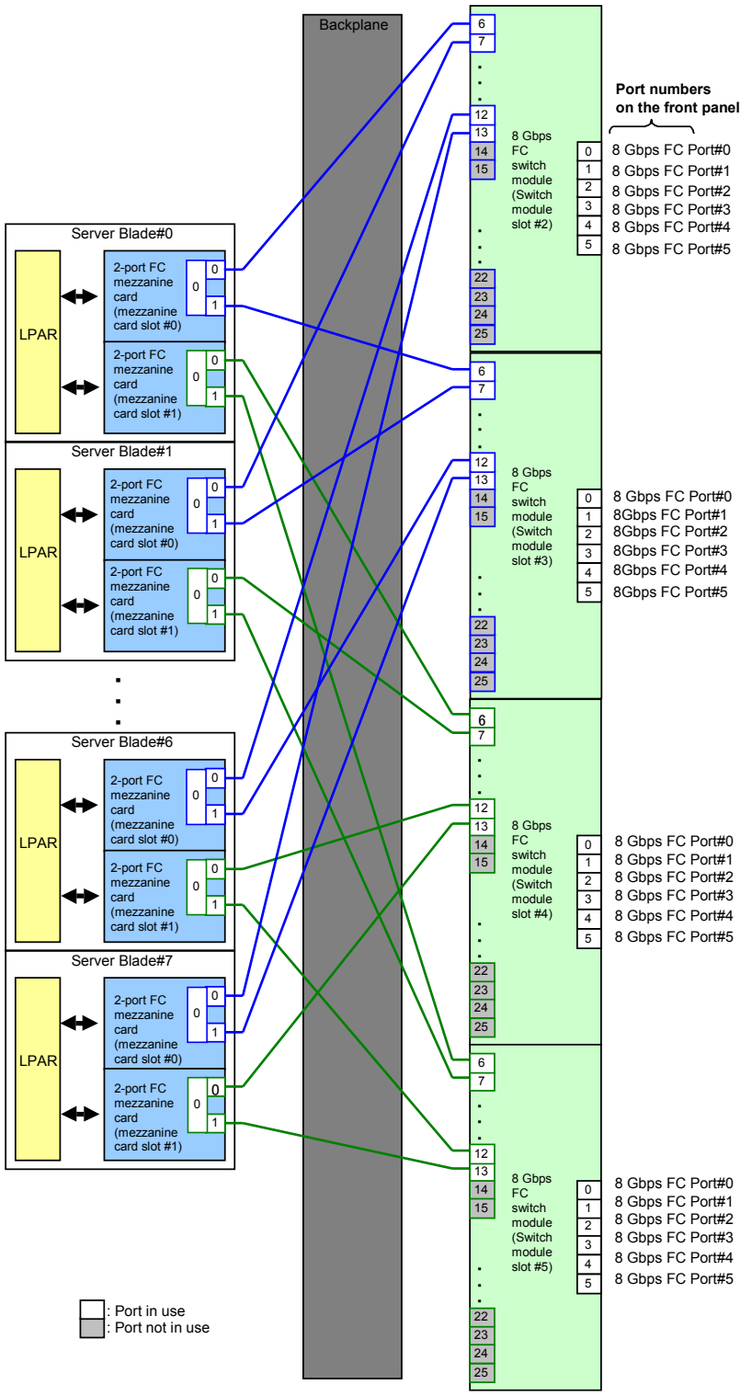
Connection to 1/10 Gbps LAN switch module

The following figure shows a connection between onboard mezzanine cards and 1/10 Gbps LAN switch modules.



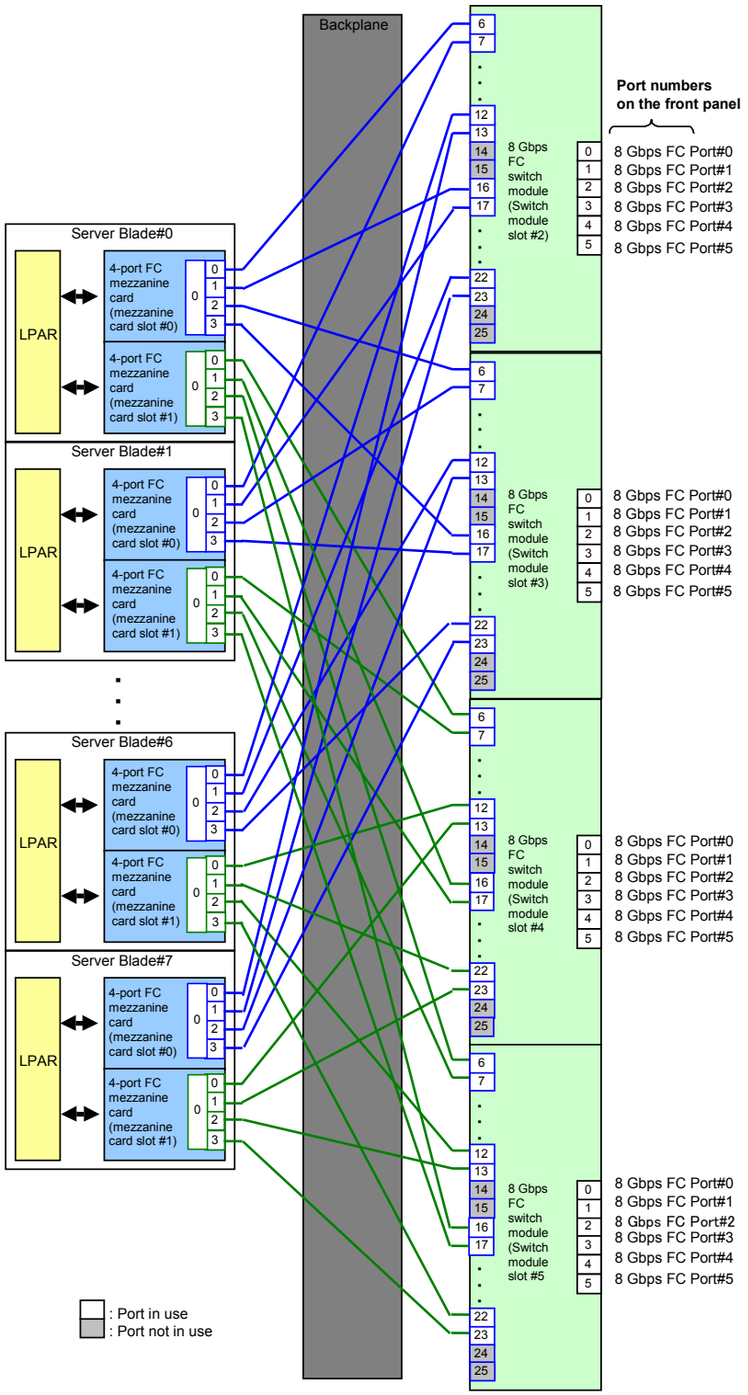
Connection between 8 Gbps FC switch modules and 2-port FC mezzanine cards

The following figure shows a connection between onboard 2-port Fibre-channel mezzanine cards and 8 Gbps Fibre-channel switch modules.



Connection between 8 Gbps FC switch modules and 4-port FC mezzanine cards

The following figure shows a connection between onboard 4-port Fibre-channel mezzanine cards and 8 Gbps Fibre-channel switch modules.



LPAR manager boot messages

Message content	Invalid LPAR manager configuration files exist in the SVP. Please restore valid LPAR manager configuration files.
Explanation	LPAR manager configuration file cannot be restored from the management module due to the invalid LPAR manager configuration file in the management module. Restore the correct LPAR manager configuration file.
What to do	Restore the correct LPAR manager configuration file.

Message content	Invalid SMT setting. (SMT is enabled. (01)) Please Power Off Partition.
Explanation	LPAR manager cannot boot due to the Enabled SMT setting.
What to do	Set Disable in SMT using the server blade Web console.

Message content	LPAR manager Loader detected enable H/W Memory Dump setting in this system. [INFO:XX] Please set H/W Memory Dump setting to disable.
Explanation	LPAR manager cannot boot due to the Enabled hardware memory dump setting.
What to do	Set Disabled in the EFI setup menu: [Advanced] > [hardware memory dump Settings] > [hardware memory dump].

Message content	LPAR manager Loader detected flash memory access error and load configuration from SVP.
Explanation	Automatic recovery was performed due to failure in the flash memory. Since the copy to the flash memory failed, however, configuration was loaded from the management module.
What to do	If this LP system log is collected at every LPAR manager boot, contact your reseller or consult maintenance personnel.

Message content	LPAR manager Loader detected invalid configuration files.[version is unmatch] (ErrorCode:XXXXXXXXXXXXXXXX AdditionalCode:XXXXXXXXXXXXXXXX) Please Power Off Partition.
Explanation	LPAR manager cannot boot due to the file with incorrect configuration.
What to do	Restore a file with a correct configuration.

Message content	LPAR manager loader detected the damage of flash memory and recovered.
Explanation	LPAR manager detected flash memory failure and recovered automatically.
What to do	None.

Message content	**LPAR manager loader detected invalid Intel(R) VT-d setting in this system.** **Please set Intel(R) VT-d setting to enable.**
Explanation	LPAR manager cannot boot due to the Disabled Intel(R) VT-d setting.
What to do	Set Enabled in Intel(R) VT-d using the EFI setup menu: [Chipset] > [North Bridge] > [Tylersburg IOH Configuration] >[Intel(R) VT for Directed I/O Configuration] > [Intel(R) VT-d].

Message content	**LPAR manager loader detected invalid Virtualization Technology setting in this system.** **MSR INFO [0xXXXXXXXXXXXXXXXX]** **Please set Virtualization Technology setting to enable.**
Explanation	LPAR manager cannot boot due to the Disabled Virtualization Technology setting.
What to do	Set Enable in Intel Virtualization Technology using the EFI setup menu: [Advanced] > [CPU Configuration].

Message content	**LPAR manager Loader detected x2APIC Mode setting to enable.** **x2APIC Mode is unsupported in LPAR manager system.** **Please change APIC Mode to xAPIC Mode.**
Explanation	LPAR manager cannot boot because APIC Mode is not set to xAPIC.
What to do	Set APIC Mode to xAPIC using the server blade Web console.

Message content	**LPAR manager-Loader detected Emulex Multi Channel mode (Bus:0xXX, Dev:0xXX, Fnc:0xXX), which is not supported. Please disable Emulex Multi Channel mode.**
Explanation	LPAR manager cannot boot because the Emulex NIC multi-channel mode is Enabled.
What to do	Disable the NIC multi-channel mode using Emulex PXESelect Utility. See the *Hitachi Compute Blade Emulex Adapter User's Guide for Hardware* for details.

Message content	**This LPAR manager F/W is not supported for this blade(BladeSymphony XXXXXX).** **Please install another LPAR manager F/W supported for this blade.** **XXXX: server blade model name**
Explanation	This LPAR manager firmware is not supported by this server blade.
What to do	Install LPAR manager firmware supported by this server blade.

If any message other than described above, contact the reseller from which you purchased the product or consult maintenance personnel.

LPAR manager on-screen messages

Followings are the LPAR manager messages that appear on the console screen when the processing for a screen operation has not concluded normally.

Message content	Active LPAR Exist
Explanation	The LPAR for which you tried to make a setting is active, so you cannot make any settings now.
LPAR manager operation	Aborts the specified process.
What to do	Make the setting again after the LPAR has been deactivated

Message content	All groups are already added.
Explanation	No group can be added.
LPAR manager operation	Aborts the specified process.
What to do	Review the specified process.

Message content	All LPARs are already defined.
Explanation	There is no LPAR left to be defined.
LPAR manager operation	Aborts the specified process.
What to do	Review the process.

Message content	Auto activation for LPARx results in error.
Explanation	Auto activation for LPARx failed.
LPAR manager operation	Aborts the specified process.
What to do	Follow the instructions in subsequent messages.

Message content	Cannot change LPAR manager System Time due to NTP enabled.
Explanation	LPAR manager system time cannot be changed due to NTP enabled.
LPAR manager operation	Aborts the specified process.
What to do	Disable the NTP before changing the LPAR manager system time.

Message content	Cannot change timezone of LPAR manager System Time due to NTP enabled.
Explanation	LPAR manager system time zone cannot be changed due to NTP enabled.
LPAR manager operation	Aborts the specified process.
What to do	Disable the NTP before changing the LPAR manager system time zone.

Message content	Change LP IP Address
Explanation	The LP IP Address needs to be changed (to something other than 0).
LPAR manager operation	Waits for the LP IP Address to be changed.
What to do	Change the LP IP Address.

Message content	Change VNIC System No
Explanation	The virtual NIC System Number needs to be changed (to something other than 0).
LPAR manager operation	Waits for the virtual NIC System Number to be changed.
What to do	Change the virtual NIC System Number.

Message content	Count Over Shared NIC Config.
Explanation	Due to beyond the upper limit of shared NIC, the scheduling mode cannot be changed to shared.
LPAR manager operation	Aborts the specified process.
What to do	Reconsider the specified process.

Message content	Device Assign error
Explanation	Indicates that connecting or disconnecting the device has failed.
LPAR manager operation	If activating the LPAR, stops activation. If changing the device target, stops connecting or disconnecting the device.
What to do	Deactivate the relevant LPAR, reassign the device that has been assigned to the LPAR, and then reactivate the LPAR.

Message content	Device Schedule Mode is not Exclusive Shared.
Explanation	The schedule mode of the target PCI device is not exclusively shared.
LPAR manager operation	Aborts the specified process.
What to do	Select a PCI device with the exclusively shared mode (Schd:E).

Message content	Error Character
Explanation	An error in the characters you typed caused the setting process to fail.
LPAR manager operation	Aborts character setting.
What to do	Revise the entry restrictions.

Message content	Failed to save LPAR manager configuration
Explanation	The process of saving the LPAR manager configuration information failed.
LPAR manager operation	Aborts the specified process.
What to do	Check the management path network configuration and then execute it again.

Message content	Go to Shared FC Assign on Type=F & Schd=S.
Explanation	The device is a shared FC, so you need to change it on the PCI Device Assignment screen.
LPAR manager operation	Aborts the specified process.
What to do	Make the setting on the Shared FC Assignment screen.

Message content	Go to VNIC Assign on Type=T & Schd=S.
Explanation	The device is a shared NIC, so you need to change it on the PCI Device Assignment screen.
LPAR manager operation	Aborts the specified process.
What to do	Make the setting on the VNIC Assignment screen.

Message content	Guest operating system might not remove USB devices safely. Force to detach.
Explanation	Indicates that connecting or disconnecting the device might have failed.
LPAR manager operation	Only detaches the USB device, and stops changing the USB device assignment to other LPARs.
What to do	Assign the USB device to the LPAR again.

Message content	LPAR manager could not import Time Setting of SVP.
Explanation	Importing time from the management module failed.
LPAR manager operation	Aborts the specified process.
What to do	Check if the management module version supports the NTP linkage.

Message content	LPAR manager is busy with another LPAR(X) activation process.
Explanation	During LPAR Activation processing, activation failed except for the securing of resources.
LPAR manager operation	Aborts the specified process.
What to do	Wait a moment and then retry the specified process.

Message content	LPAR manager is executing LPAR Migration, Please try again after it is finished.
Explanation	Operation is not available due to LPAR migration in execution.
LPAR manager operation	Aborts the specified process.
What to do	Wait a while until LPAR migration is complete and then retry the specified process.

Message content	LPAR manager is executing LPAR Migration. LP System Shutdown was canceled.
Explanation	LPAR manager shutdown was canceled due to LPAR migration in execution.
LPAR manager operation	Aborts the specified process.
What to do	Wait a while until LPAR migration is complete and then retry the specified process.

Message content	LPAR manager is not executable condition for this request. Please wait.
Explanation	The LPAR manager system is not in the condition to execute the requested processing.
LPAR manager operation	Aborts the specified process.
What to do	Wait a moment and then retry the specified process.

Message content	LPAR manager is not ready for the operation
Explanation	LPAR manager configuration information could not be saved.
LPAR manager operation	Aborts the specified process.
What to do	Perform Force Recovery in the System Service State screen.

Message content	LPAR manager is recovering specified LPAR from failed-migration state. This operation prevents some operations from performing.
Explanation	Does not allow you to operate screens because the failed LPAR in LPAR migration is currently being recovered.
LPAR manager operation	The failed LPAR in LPAR migration is being recovered.
What to do	None.

Message content	Inhibit ICV request for the operation
Explanation	LPAR manager configuration information could not be saved.
LPAR manager operation	Aborts the specified process.
What to do	Wait a while and try again.

Message content	Insufficient Processor resource
Explanation	When you tried to set the number of dedicated logical processors, a sufficient number of physical processors could not be secured. When an LPAR is activated, the physical processors assigned to the LPAR cannot be secured.
LPAR manager operation	Aborts LPAR activation.
What to do	Reduce the number of processors allocated or try again to activate the LPAR after you have deactivated a currently active LPAR. Alternatively, check the Logical Processor Configuration screen.

Message content	Invalid hour data.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid minute data.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid month data.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid second data.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid separator.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid year data.
Explanation	The numeric value you specified for the LPAR manager System Date and Time change is invalid.
LPAR manager operation	Aborts the specified process.
What to do	Correct the value and retry.

Message content	Invalid input data.
Explanation	The new data you tried to set is invalid and cannot set.
LPAR manager operation	Aborts the setting process.
What to do	Set different data.

Message content	IP address of NTP server is needed.
Explanation	An IP address is required for setting the NTP server.
LPAR manager operation	Aborts the time acquisition.
What to do	Set an IP address to NTP Server 1 or NTP Server 2.

Message content	LPAR activation failed.
Explanation	The LPAR cannot be activated.
LPAR manager operation	Aborts LPAR activation.
What to do	Check if the LPAR manager system error log is collected. If you cannot solve the error, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR activation failed (Insufficient LPAR memory(System Used:xxMB)).
Explanation	Memory size for the LPAR, a value subtracted memory size used by the system from memory assigned to the LPAR, is not enough.
LPAR manager operation	Aborts LPAR activation.
What to do	Assign more memory to the LPAR and then activate the LPAR.

Message content	LPAR corrupted in a LPAR Migration exist, Please try again after recovering the LPAR.
Explanation	Operation is not available due to a failed LPAR by LPAR migration.
LPAR manager operation	Aborts LPAR deactivation.
What to do	Remove the failure, and then execute LPAR migration.

Message content	LPAR deactivation failed.
Explanation	The LPAR cannot be deactivated.
LPAR manager operation	Aborts LPAR deactivation.
What to do	Check if LPAR manager system error log is collected. If you cannot solve the error, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR start failed.
Explanation	The target LPAR failed to restart.
LPAR manager operation	Aborts the specified process.
What to do	Retry the process.

Message content	Memory allocation failed (Insufficient).
Explanation	When you activated an LPAR, the memory capacity you specified could not be secured.
LPAR manager operation	Aborts LPAR activation.
What to do	Reduce the memory allocation or try again to activate the LPAR after you have deactivated a currently active LPAR.

Message content	Memory allocation failed (Fragmentation).
Explanation	When you activated an LPAR, the memory capacity you specified could not be secured.
LPAR manager operation	Aborts LPAR activation.
What to do	The memory could not be secured due to fragmentation. Reduce the memory allocation or try again to activate the LPAR after you have deactivated a currently active LPAR.

Message content	Memory size is zero.
Explanation	Because the memory size is zero, the LPAR cannot be activated.
LPAR manager operation	Aborts LPAR activation.
What to do	Set a memory size and active the LPAR.

Message content	No groups can be removed.
Explanation	No group can be deleted.
LPAR manager operation	Aborts the specified process.
What to do	Review the specified process.

Message content	Not Changed!! Select Device is Management Path.
Explanation	When you tried to change the NIC schedule mode, it was not changed because the selected NIC was set as the management path.
LPAR manager operation	Aborts the specified process.
What to do	Reconsider the specified processing.

Message content	NTP server is not set.
Explanation	Any NTP server is not set.
LPAR manager operation	Aborts the time acquisition from an NTP server.
What to do	Set an IP address to NTP Server 1 or NTP Server 2.

Message content	Over Max VLAN ID count (16).
Explanation	The number of the specified VLANID exceeds 16.
LPAR manager operation	Either automatically modifies the specified VLANID to be less than 16, or keeps the message subscreen on the terminal display until the Esc key is pressed.
What to do	Change the VLANID to be less than 16, or cancel the VLANID setting operation by pressing the Esc key.

Message content	Over the maximum number of activated LPARs(X).
Explanation	The LPAR cannot be activated because it is beyond the max number (X) of LPARs to activate. (X) shows the number of LPARs.
LPAR manager operation	Aborts the LPAR activation.
What to do	Deactivate an LPAR currently activated, and then activate the LPAR again.

Message content	Press any key first. Then press the F10 key next.
Explanation	To make the changed setting effective, you need to press the F10 key.
LPAR manager operation	Waits for the F10 key to be pressed.
What to do	Press any key, wait for the output message to disappear, and then press the F10 key.

Message content	Resource lock failure.
Explanation	Locking resources failed when you updated configuration information. Locking resources failed when you performed a system or LPAR operation. Locking resources failed when you updated the RAR of a NIC.
LPAR manager operation	Aborts the specified process.
What to do	Retry the specified process.

Message content	Sampling time Error
Explanation	Sampling time setting failed in LPAR Usage screen.
LPAR manager operation	Aborts the sampling time setting.
What to do	Set a number between 1 and 60.

Message content	Save Configuration request (F9 Key) is already accepted. Please wait.
Explanation	The Save Configuration request has already been accepted. Wait a moment.
LPAR manager operation	Aborts the specified process.
What to do	Wait until the LPAR manager configuration information begins to be saved.

Message content	Select Device is Single Port NIC. Cannot change Management Path.
Explanation	The NIC you selected in the management path setting is 1 port.
LPAR manager operation	Aborts the specified process.
What to do	Reconsider the specified process.

Message content	Target LPAR is active.
Explanation	The LPAR for which you tried to make a setting is active, so you cannot make any settings now.
LPAR manager operation	Aborts the specified process.
What to do	Make the setting again after the LPAR has been deactivated.

Message content	Target LPAR must be shared mode.
Explanation	The LPAR for which you tried to make a setting is in dedicated, so you cannot make any settings now.
LPAR manager operation	Aborts the specified process.
What to do	Change the scheduling mode of the LPAR to shared mode before reset.

Message content	The LPAR Migration is in progress. This LPAR Migration prevents some operations such as activation, deactivation, and LPAR-reconfiguration from performing.
Explanation	Operation with screen is not allowed due to LPAR migration in progress.
LPAR manager operation	LPAR migration is being performed.
What to do	Wait for a while until the LPAR migration is completed.

Message content	The name is used for other group.
Explanation	When you try to name a group, the name is already used by another group.
LPAR manager operation	Aborts change in the group name.
What to do	Give another name to the group.

Message content	The specified LPAR has corrupted in a LPAR Migration, please try to recover the LPAR.
Explanation	Since the LPAR has failed due to LPAR migration, it cannot be operated.
LPAR manager operation	Does not allow operation due to the failed LPAR in LPAR migration.
What to do	Recover the LPAR for LPAR migration.

Message content	Service Ratio must be 1-999
Explanation	The service ratio you tried to set was not in the range from 1 to 999 so it could not be set.
LPAR manager operation	Aborts the service ratio setting.
What to do	Set a service ratio between 1 and 999.

Message content	Target LPAR is coming to foreground.
Explanation	Now switching to the LPAR guest screen.
LPAR manager operation	Continues the specified processing.
What to do	Wait for a while.

Message content	Target LPAR is deactive.
Explanation	The LPAR you tried to deactivate is already deactivated.
LPAR manager operation	Aborts the service ratio setting.
What to do	Try again after activating the LPAR.

Message content	Target LPAR is Executing Migration.
Explanation	The LPAR you tried to manipulate is not available due to LAPR migration in execution.
LPAR manager operation	Aborts the specified process.
What to do	Retry the specified process after LPAR migration is complete.

Message content	Target LPAR is Executing Rollback.
Explanation	The LPAR you tried to manipulate is not available due to rollback by LPAR migration.
LPAR manager operation	Aborts the specified process.
What to do	Retry the specified process after LPAR rollback is complete.

Message content	Target LPAR is undefined.
Explanation	The LPAR you tried to manipulate is undefined. When you tried to change the configuration information of a virtual NIC, you tried to change an undefined LPAR.
LPAR manager operation	Aborts the specified process.
What to do	Retry the specified process.

Message content	The name is used for other LPAR.
Explanation	An LPAR with the name you set already exists.
LPAR manager operation	Aborts LPAR name change process.
What to do	Change the name.

Message content	The VF is already assigned the maximum assignable times to LPARs.
Explanation	A device failed to be connected or disconnected.
LPAR manager operation	Aborts LPAR activation. Aborts connecting or disconnecting the device.
What to do	Re-assign the device to the target LPAR once more, and re-activate the LPAR.

Message content	Updating LPAR manager firmware, Please try again after it is finished.
Explanation	LPAR manager shutdown or the F10 key cannot be executed because LPAR manager firmware is updating.
LPAR manager operation	Cancels the specified process.
What to do	Execute the process again when LPAR manager firmware update is completed.

Message content	Updating LPAR manager firmware, Please wait until it is finished.
Explanation	LPAR manager shutdown is waiting for execution during updating LPAR manager firmware.
LPAR manager operation	Stops activating LPAR.
What to do	Wait for a while until LPAR manager firmware updating is completed.

Message content	VLAN ID is not set.
Explanation	No VLAN ID is set in the LPAR manager system. No information can be displayed.
LPAR manager operation	Aborts the specified process.
What to do	Verify the setting of the network segment identifier, which is specified to display.

When a message other than the above is displayed, contact your reseller or maintenance personnel.

LPAR manager system logs screen messages

The following lists the LP System Logs screen messages displayed on the LP System Logs screen:

Message content	An abnormal time difference was detected.
Level	Error
Explanation	Aborted the regular time synchronization with NTP due to abnormal time difference detected.
What to do	Disable the NTP on the Date and Time screen to check the NTP server state. If with no problem, enable it again. Check the logical RTC time of the LPAR on the LPAR manager screen as well to set the logical RTC time of the LPAR using the OS command or Adjust LPAR Time. Message “LPAR manager damage occurred.” Is also collected with this message.

Message content	CPU core swap is completed. (Auto).
Level	Information
Explanation	Replaced the core with an alternative one due to a sign of failure detected.
What to do	Save the LPAR manager system configuration because the configuration is updated.

Message content	Dmar Fault occurred.
Level	Error
Explanation	DMAR fault occurred.
What to do	Contact your reseller or maintenance personnel.

Message content	Dmar Fault occurred.
Level	Error
Explanation	Dmar fault occurred.
What to do	Contact your reseller or maintenance personnel.

Message content	Found the machine type mismatch LPAR manager initialized the configuration files.
Level	Information
Explanation	LPAR manager configuration information and server blade configuration do not match.
What to do	Check the LPAR manager configuration information and server blade configuration.

Message content	Guest dump completed.
Level	Information
Explanation	Guest memory dump was completed.
What to do	None.

Message content	Guest dump failed.
Level	Warning
Explanation	Guest memory dump failed.
What to do	To get the information on the failure and its factors, execute the command “Get guest memory dump progress” of HVM management command (HvmSh command). Work with the problem according to ” ”Status Codes and Messages” displayed by this command.

Message content	Guest dump started.
Level	Information
Explanation	Guest memory dump started by the start operation of guest memory dump.
What to do	None.

Message content	Guest dump was cancelled.
Level	Information
Explanation	Guest memory dump was cancelled by the canceling operation of guest memory dump.
What to do	None.

Message content	Guest, Double Fault (#DF) occurred.
Level	Information
Explanation	A guest double fault occurred.
What to do	Check the guest OS operation status.

Message content	Guest, INIT occurred.
Level	Information
Explanation	A guest INIT interrupt occurred.
What to do	Check the guest OS operation status.

Message content	Guest, NMI occurred.
Level	Information
Explanation	A guest NMI interrupt occurred.
What to do	Check the guest OS operation status.

Message content	Guest, Triple Fault occurred.
Level	Information
Explanation	A guest triple fault occurred.
What to do	Check the guest OS operation status.

Message content	Guest, Watchdog timer has expired.
Level	Error
Explanation	A guest watchdog timer timeout was detected.
What to do	Take action while referring to other fault-indicating LP system logs. If the action you take does not take effect, contact inquires listed in this manual.

Message content	H/W Corrected MCK cumulative count was logged.
Level	Information
Explanation	The cumulative number of times of corrected machine check event are registered.
What to do	None.

Message content	H/W Corrected MCK logging was suppressed.
Level	Error
Explanation	The number of times of corrected machine check event logging exceeded the threshold. The error logging was suppressed.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	H/W Corrected MCK occurred.
Level	Warning
Explanation	A corrected machine check event occurred.
What to do	None.

Message content	H/W Fatal MCK occurred.
Level	Error
Explanation	A fatal machine check event occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Hardware Component BMC access error occurred.
Level	Error
Explanation	A fault occurred in accessing the physical BMC.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Hardware Component BMC access error was recovered.
Level	Information
Explanation	A fault in accessing the physical BMC was removed.
What to do	None.

Message content	LPAR manager activates LPAR in auto activation process.
Level	Information
Explanation	LPAR was activated with Auto Activate.
What to do	None.

Message content	LPAR manager Assist damage occurred.
Level	Error
Explanation	An LPAR manager fault (LPAR manager Assist fault) occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager Assist damage occurred. (due to H/W error)
Level	Error
Explanation	An LPAR manager fault (LPAR manager fault) resulting from a hardware fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR Manager detected a failure of retrying the setting of TxRate configuration.
Level	Error
Explanation	Retry of the operation to configure TxRate failed.
What to do	A network failure might have occurred. Check the status of the network to which this device is connected. If you cannot find any network problem, a device failure might have occurred.

Message content	LPAR manager auto activation process is cancelled.
Level	Information
Explanation	The Auto Activate operation was cancelled.
What to do	None.

Message content	LPAR manager auto activation process is ended.
Level	Information
Explanation	The Auto Activate operation is complete.
What to do	None.

Message content	LPAR manager auto activation process is started.
Level	Information
Explanation	The Auto Activate operation is started.
What to do	None.

Message content	LPAR manager booted with copied configuration files.
Level	Information
Explanation	LPAR manager was started with LPAR manager configuration information subjected to cloning.
What to do	None.

Message content	LPAR manager could not import Time Setting of BMC.
Level	Warning
Explanation	Importing time setting from BMC failed.
What to do	Check the BMC time setting and correct it if needed; re-import the time setting from the BMC.

Message content	LPAR manager could not import Time Setting of SVP.
Level	Warning
Explanation	Importing time setting from the management module failed.
What to do	Check if the management module version supports the NTP linkage. Correct the management module time setting if needed, and re-import the time setting from the management module.

Message content	LPAR manager could not power off the PCI slot.
Level	Error
Explanation	Failed to power off the physical PCI slot.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager could not power on the PCI slot.
Level	Error
Explanation	Failed to power on the physical PCI slot.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager could not retrieve Time Setting from SVP.
Level	Warning
Explanation	Retrieving the time setting from the management module failed.
What to do	Check if the management module version supports the NTP linkage. Correct the management module time setting if needed.

Message content	LPAR manager flash memory access error occurred.
Level	Error
Explanation	A fault occurred in accessing the flash memory.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager damage occurred.
Level	Error
Explanation	An LPAR manager fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager damage occurred. (due to H/W error)
Level	Error
Explanation	An LPAR manager fault resulting from a hardware fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected a failure of retrying the setting of TxRate configuration.
Level	Error
Explanation	Retrying TxRate setting failed.
What to do	Check the network state connected the device, because the network failure may occur. If the network has no problem, the device may be out of order. Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected a lack of I/O interrupt vectors.
Level	Warning
Explanation	LPAR manager detected a lack of interrupt vectors.
What to do	Check the PCI device configuration. If a PCI device is not supported by the product, remove it from configuration. If standard server blade X55R3 or X55S3 model has a single 2-core CPU onboard, enable SMT (Simultaneous Multi-Threading) for operation. If this cannot solve the problem, contact the reseller or consult maintenance personnel.

Message content	LPAR manager detected Activation error for Shared NIC at expansion card.
Level	Error
Explanation	A failure in validating shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Activation error for Shared NIC at on-board.
Level	Error
Explanation	A failure in validating shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Activation error for Shared NIC.
Level	Error
Explanation	A failure in validating shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR Manager detected different version of firmware on the NIC device.
Level	Error
Explanation	A fault in the combination of the firmware versions of NIC devices was detected.
What to do	Check that all NIC firmware versions on the server blade are the same. If you cannot solve the problem, contact your reseller or maintenance personnel.

Message content	LPAR manager detected AP initialization timeout.
Level	Warning
Explanation	A timeout occurred in initializing the guest OS.
What to do	Review the service rate allocation to the LPAR.

Message content	LPAR manager detected different version of firmware on the NIC device.
Level	Error
Explanation	Combination failure for the firmware version of the NIC device is detected.
What to do	Check that versions of NIC firmware mounted on the server blade are all the same. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Driver request MCK for Shared FC.
Level	Information
Explanation	LPAR manager received the driver request for recovering a failure in the shared FC from the guest OS.
What to do	None.

Message content	LPAR manager detected Driver request Port-Isolation for Shared FC.
Level	Information
Explanation	LPAR manager received the driver request for isolating ports in the shared FC from the guest OS. This log can be collected when the FC fault threshold management is enabled in the guest OS.
What to do	None.

Message content	LPAR manager detected Driver Ver Error at Shared FC at expansion card.
Level	Warning
Explanation	The FC driver not supporting shared FC was detected.
What to do	Upgrade the driver to the version supporting shared FC.

Message content	LPAR manager detected Driver Ver Error at Shared FC.
Level	Warning
Explanation	The FC driver not supporting shared FC was detected.
What to do	Upgrade the driver to the version supporting shared FC.

Message content	LPAR manager detected error of network communication at management path.
Level	Error
Explanation	A fault in the management path was detected. Internal LAN segment overlaps with the management LAN segment.
What to do	Review the LP IP address setting.

Message content	**LPAR manager detected error of network communication for SVP access.**
Level	Error
Explanation	A communication fault occurred between LPAR manager and the switch and management module.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected failed SR-IOV device was assigned to LPAR.
Level	Warning
Explanation	Detected that the LPAR, to which the isolated PCI device is assigned, is activated.
What to do	The PCI device is not available on the LPAR due to the error. If the PCI device is not automatically recovered, execute Force Recovery to release the isolation. Then, reboot the guest OS to use the PCI device.

Message content	LPAR manager detected failed SR-IOV feature was recovered.
Level	Information
Explanation	Detected the isolated PCI device is recovered.
What to do	None. The PCI device has been recovered from the error state. The PCI device isolated on the LPAR will run properly after the guest OS reboot.

Message content	**LPAR manager detected Hardware error for Shared FC at expansion card.**
Level	Error
Explanation	A fatal fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	**LPAR manager detected Hardware error for Shared FC.**
Level	Error
Explanation	A fatal fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Initialization error for Shared NIC at expansion card.
Level	Error
Explanation	A failure in initializing shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Initialization error for Shared NIC at on-board.
Level	Error
Explanation	A failure in initializing shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Initialization error for Shared NIC.
Level	Error
Explanation	A failure in initializing shared NIC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected invalid I/O slot expansion unit number.
Level	Warning
Explanation	An invalid I/O slot expansion unit number was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Down error for Shared FC at expansion card.
Level	Error
Explanation	Shared FC link down was detected.
What to do	Check the connection to shared FC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Down error for Shared FC.
Level	Error
Explanation	Shared FC link down was detected.
What to do	Check the connection to shared FC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Down error for Shared NIC at expansion card.
Level	Error
Explanation	Shared NIC link down was detected.
What to do	Check the connection to shared NIC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Down error for Shared NIC at on-board.
Level	Error
Explanation	Shared NIC link down was detected.
What to do	Check the connection to shared NIC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Down error for Shared NIC.
Level	Error
Explanation	Shared NIC link down was detected.
What to do	Check the connection to shared NIC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected Link Up recovery at Shared NIC at expansion card.
Level	Information
Explanation	Shared NIC link up recovery was detected.
What to do	None.

Message content	LPAR manager detected Link Up recovery at Shared NIC at on-board.
Level	Information
Explanation	Shared NIC link up recovery was detected.
What to do	None.

Message content	LPAR manager detected Link Up recovery at Shared NIC.
Level	Information
Explanation	Shared NIC link up recovery was detected.
What to do	None.

Message content	LPAR manager detected MCK recovery for Shared FC at expansion card.
Level	Information
Explanation	A fault recovery occurred in shared FC.
What to do	None.

Message content	LPAR manager detected MCK recovery for Shared FC.
Level	Information
Explanation	A fault recovery occurred in shared FC.
What to do	None.

Message content	LPAR manager detected MCKINT for Shared FC at expansion card.
Level	Error
Explanation	A temporary fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected MCKINT for Shared FC.
Level	Error
Explanation	A temporary fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected network communication error at SC Manager access.
Level	Error
Explanation	A communication error occurred between LPAR manager and SC/BSM.
What to do	Check the connection between LPAR manager and SC/BSM. If you cannot remove this error, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected PCI bus error for Shared FC at expansion card.
Level	Error
Explanation	A PCI bus fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected PCI bus error for Shared FC.
Level	Warning
Explanation	A PCI bus fault in shared FC was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected PCI Configuration unmatch and recovered.
Level	Information
Explanation	Changed PCI device setting information due to the unmatched hardware configuration. So, the PCI device mode was changed to the shared mode.
What to do	Check the LPAR manager configuration information and hardware configuration.

Message content	LPAR manager detected PCI Configuration unmatch.
Level	Information
Explanation	LPAR manager configuration information and PCI device configuration do not match.
What to do	Check the LPAR manager configuration information and hardware configuration.

Message content	LPAR manager detected PCI dev assign error.
Level	Warning
Explanation	LPAR manager detected invalid PCI device allocation information.
What to do	Re-allocate the PCI device on the PCI Device Assign screen. If this LP system log is re-obtained, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected recovery Port-Isolation for Shared FC.
Level	Information
Explanation	Releasing the shared FC port isolation was completed properly.
What to do	None.

Message content	LPAR manager detected Shared FC Link is Available at expansion card.
Level	Information
Explanation	Shared FC Link is available.
What to do	None.

Message content	LPAR manager detected Shared FC Link is Available.
Level	Information
Explanation	Shared FC Link is available.
What to do	None.

Message content	LPAR Manager detected the success of retrying the setting of TxRate configuration.
Level	Information
Explanation	Retry of the operation to configure TxRate finished .
What to do	None.

Message content	LPAR manager detected the duplication of I/O slot expansion unit number.
Level	Warning
Explanation	Duplication of an I/O slot expansion unit number was detected.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager detected the success of retrying the setting of TxRate configuration.
Level	Information
Explanation	Retrying the setting of TxRate was successfully.
What to do	None.

Message content	LPAR manager detected too many physical CPUs, some CPUs are ignored.
Level	Warning
Explanation	Ignored some CPUs due to those CPUs installed beyond the maximum number of them that LPAR manager can recognize.
What to do	Contact your reseller or maintenance personnel.

Message content	LPAR manager detected uninitialized Shared device.
Level	Error
Explanation	Detected an uninitialized shared I/O device.
What to do	Contact your reseller or maintenance personnel.

Message content	LPAR manager detected unsupported version of firmware on a NIC device.
Level	Error
Explanation	Detected not-supported NIC firmware version.
What to do	Check if your NIC firmware version is supported by LPAR manager. When you cannot solve the problem, contact your reseller or maintenance personnel.

Message content	LPAR Manager failed to get the firmware version on a NIC device.
Level	Error
Explanation	An attempt to obtain the firmware version from the NIC device failed.
What to do	Restart LPAR Manager. If this LPAR Manager system log is collected even after you restart LPAR Manager, contact your reseller or maintenance personnel.

Message content	LPAR manager dump generation failed.
Level	Warning
Explanation	The LPAR manager dump failed to be obtained.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager dump generation succeeded.
Level	Information
Explanation	The LPAR manager dump was obtained successfully.
What to do	None.

Message content	LPAR manager dump is lost.
Level	Warning
Explanation	The LPAR manager dump was lost.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager dump transfer failed.
Level	Warning
Explanation	Transfer of the LPAR manager dump to the management module failed.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager dump transfer retry.
Level	Information
Explanation	The LPAR manager dump was re-transferred to the management module.
What to do	None.

Message content	LPAR manager dump transfer succeeded.
Level	Information
Explanation	The LPAR manager dump was transferred to the management module.
What to do	None.

Message content	LPAR manager failed in network time synchronization by NTP.
Level	Warning
Explanation	Synchronizing the LPAR manager system time with NTP failed.
What to do	Check the following: - The specified IP address is correct. - An NTP server is in operation. - The NTP server is connected to LAN. - The ping command can work between the NTP server and LP IP address.

Message content	LPAR Manager started retrying the setting of TxRate configuration.
Level	Warning
Explanation	Failed to configure TxRate. Try to configure TxRate again.
What to do	Wait a while for the retry to finish.

Message content	LPAR manager failed to get the firmware version on a NIC device.
Level	Error
Explanation	Getting firmware version from NIC device failed.
What to do	Restart the LPAR manager. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager failed to have SR-IOV device enabled.
Level	Error
Explanation	Detected that different SR-IOV settings exist among ports in the controller.
What to do	Check the SR-IOV setting values of the PCI devices. Alternatively, make sure that the Personality setting is set to NIC mode. For details about how to check this setting, see the manual Hitachi Compute Blade 2000 / 500 Emulex Adapter User's Guide for Hardware. Note, however, that you cannot change the setting in LP mode. To change the setting, change the mode to Basic mode.

Message content	LPAR manager firmware update failed.
Level	Warning
Explanation	LPAR manager firmware updating failed.
What to do	A screen, showing that LPAR manager firmware update failed, is displayed. Follow the procedure shown in the screen to handle the problem.

Message content	LPAR manager firmware update finished successfully.
Level	Information
Explanation	LPAR manager firmware was successfully updated.
What to do	None.

Message content	LPAR manager firmware update was started.
Level	Information
Explanation	LPAR manager firmware updating was started.
What to do	None.

Message content	LPAR manager has successfully imported Time Setting of BMC.
Level	Information
Explanation	BMC time setting has been successfully imported.
What to do	None.

Message content	LPAR manager has successfully imported Time Setting of SVP.
Level	Information
Explanation	SVP time setting has been successfully imported.
What to do	None.

Message content	LPAR manager has successfully retrieved Time Setting of SVP.
Level	Information
Explanation	SVP time setting has been successfully retrieved.
What to do	None.

Message content	LPAR manager has successfully synchronized RTC with NTP server.
Level	Information
Explanation	RTC has been synchronized with the NTP server.
What to do	None.

Message content	LPAR manager has successfully synchronized the time with RTC.
Level	Information
Explanation	RTC has been synchronized.
What to do	None.

Message content	LPAR manager Isolated physical memory (address) due to uncorrectable error.
Level	Error
Explanation	Physical memory was isolated due to uncorrectable error.
What to do	If the same message happens multiple times, contact your reseller or maintenance personnel.

Message content	LPAR manager Loader detected load error and recovered.
Level	Warning
Explanation	Configuration information failed to be read; however, this error was corrected.
What to do	If this LP system log is obtained each time LPAR manager starts, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR manager Loader detected flash memory access error and load configuration from SVP.
Level	Warning
Explanation	LPAR manager detected flash memory failure, automatically recovered, tried to copy it to the flash memory but failed, and then read the configuration files from the management module.
What to do	If this log is collected at every LPAR manager boot, contact your reseller or consult maintenance personnel.

Message content	LPAR manager Loader detected the damage of flash memory and recovered.
Level	Information
Explanation	LPAR manager detected flash memory failure, and automatically recovered.
What to do	None.

Message content	LPAR manager Loader initialized the configuration files.
Level	Information
Explanation	LPAR manager configuration files were initialized.
What to do	None.

Message content	LPAR manager Loader loaded the configuration files from SVP.
Level	Information
Explanation	LPAR manager configuration files were retrieved from SVP.
What to do	None.

Message content	LPAR manager logged the EFI-Driver log for Shared FC at expansion card.
Level	Information
Explanation	The shared FC driver transferred the log to LPAR manager.
What to do	None.

Message content	LPAR manager logged the EFI-Driver log for Shared FC.
Level	Information
Explanation	The shared FC driver transferred the log to LPAR manager.
What to do	None.

Message content	LPAR manager recovered from NTP error status.
Level	Information
Explanation	The error in synchronizing the LPAR manager system time with the NTP server was recovered.
What to do	None.

Message content	LPAR manager restarted a LPAR on the destination blade.
Level	Information
Explanation	Concurrent maintenance is executed and the LPAR is restarted on the destination blade.
What to do	None.

Message content	LPAR manager restarted a LPAR on the source blade.
Level	Information
Explanation	Concurrent maintenance is executed and the LPAR is restarted on the source blade.
What to do	None.

Message content	LPAR manager saved configuration.
Level	Information
Explanation	The configuration has been saved.
What to do	None.

Message content	LPAR manager Shutdown State Changed to InProgress.
Level	Information
Explanation	The shutdown status has changed to InProgress.
What to do	None.

Message content	LPAR manager Shutdown State Changed to Ready.
Level	Information
Explanation	The shutdown status has changed to Ready.
What to do	None.

Message content	LPAR manager skipped LPAR auto activation process.
Level	Information
Explanation	“Activate” LPAR was skipped with the auto activate operation.
What to do	None.

Message content	LPAR manager started retrying the setting of TxRate configuration.
Level	Warning
Explanation	Failed to the setting of TxRate configuration. Retry the setting of TxRate configuration.
What to do	Wait until retrying the setting of TxRate configuration is complete.

Message content	LP System Shutdown Failed.
Level	Warning
Explanation	Failed to shutdown the LPAR manager system.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LP System Shutdown Started.
Level	Information
Explanation	LP system shutdown has started.
What to do	None.

Message content	LP system time has successfully synchronized with NTP server.
Level	Information
Explanation	LP system time has successfully synchronized with NTP server.
What to do	None.

Message content	LP system took a checkpoint of the source LPAR.
Level	Information
Explanation	Concurrent maintenance is executed and the LPAR is stopped on the source blade.
What to do	None.

Message content	LPAR manager updated configuration format.
Level	Information
Explanation	LPAR manager configuration format has been updated.
What to do	If Save Changed Config Format is not set to Enable on the LP Options screen, save the configuration once more.

Message content	LPAR manager updated the configuration files.
Level	Information
Explanation	LPAR manager configuration with the previous version is updated to the new version.
What to do	None.

Message content	LP-LFW detected failure of getting boot device.
Level	Warning
Explanation	LPAR manager logical firmware detected a failure to get boot device.
What to do	Contact your reseller or maintenance personnel.

Message content	LP-LFW detected failure of setting boot order.
Level	Warning
Explanation	LPAR manager logical firmware detected a failure to set a boot order.
What to do	Check and fix the boot order setting file. if it does not work, contact your reseller or maintenance personnel.

Message content	LP-LFW detected internal error.
Warning	Warning
Explanation	LPAR manager logical firmware detected an internal error and the error is recovered.
What to do	If this LP system log is often collected, contact your reseller or maintenance personnel.

Message content	LP-LFW detected internal error.
Level	Error
Explanation	LPAR manager logical firmware detected an internal error.
What to do	Contact your reseller or maintenance personnel.

Message content	LP-LFW detected not enough memory to activate LPAR.(LPAR:X)
Level	Warning
Explanation	LPAR manager logical firmware detected that memory is not enough to activate the LPAR.
What to do	Assign more number of memories, and then activate the LPAR.

Message content	LP-LFW detected tftp error and recovered.
Level	Information
Explanation	LPAR manager logical firmware detected a network failure while the network is booting, and the failure was recovered.
What to do	None.

Message content	LP-LFW detected tftp error.
Level	Warning
Explanation	LPAR manager logical firmware detected a network failure while the network is booting.
What to do	Check loading on the network and correct it if needed, and reboot the network. If this LP system log is collected regardless of your rebooting the network, contact your reseller or consult your maintenance personnel.

Message content	I/O interrupt vector mode was changed.
Level	Information
Explanation	I/O interrupt vector mode was changed.
What to do	None.

Message content	Invalid State was recovered. (ptc.l)
Level	Information
Explanation	LPAR manager corrected the invalid status of the ptc.l instruction.
What to do	None.

Message content	Lock timeout was recovered.
Level	Warning
Explanation	A lock timeout occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Logical CPU performance returns to normal.
Level	Information
Explanation	Performance has been recovered from problems including too many LPARs or logical processors, which cause performance to slow down.
What to do	None.

Message content	Logical CPU slowdown due to too many logical CPUs.
Level	Warning
Explanation	The number of LPARs or logical processors beyond the threshold value was detected, which causes performance to slow down.
What to do	Check and adjust the number of LPARs and logical processors. This event might be put out by the OS shutdown or LPAR deactivation. However, there is no problem if “Logical CPU performance returns to normal.” is put out in a few minutes.

Message content	LPAR damage occurred.
Level	Error
Explanation	An LPAR manager fault (LPAR fault) occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR damage occurred. (due to H/W error)
Level	Error
Explanation	An LPAR manager fault (LPAR fault) resulting from a hardware fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	LPAR Migration event occurred.
Level	Information
Explanation	LPAR migration has started or finished.
What to do	None.

Message content	LPAR Migration failed.
Level	Warning
Explanation	LPAR migration has failed.
What to do	Follow the troubleshooting described in LPAR Migration, *HVM Navigator User’s Guide*.

Message content	Manual CPU core degeneration is completed.
Level	Information
Explanation	The CPU core with a sign of failure detected is cancelled.
What to do	None.

Message content	Network configuration error for Shared FC at expansion card.
Level	Error
Explanation	A shared FC interface fault occurred.
What to do	Check the connection to shared NIC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Network configuration error for Shared FC.
Level	Error
Explanation	A shared FC interface fault occurred.
What to do	Check the connection to shared NIC. If this action takes no effect, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Network Segment damage occurred.
Level	Error
Explanation	A fault occurred in the network segment used for shared NICs or virtual NICs.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	NTP server settings contain invalid characters.
Level	Warning
Explanation	Improper characters are contained in the NTP server settings.
What to do	Set an NTP server IP address to NTP Server 1 or NTP Server 2.

Message content	Number of active CPU cores decreased.
Level	Information
Explanation	The number of activated cores is decreased.
What to do	None.

Message content	Number of active CPU cores increased.
Level	Information
Explanation	The number of activated cores is increased.
What to do	None.

Message content	PCI device error was detected.
Level	Error
Explanation	Detected an error in the PCI device.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	PCI Express Error Isolation was detected.
Level	Error
Explanation	Detected PCI Express isolation.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Number of active CPU cores increased.
Level	Information
Explanation	The number of activated cores is increased.
What to do	None.

Message content	Please isolate specified CPU core manually.
Level	Information
Explanation	Although a sign of failure is detected in the CPU core, replacement is not available due to lack of alternative cores.
What to do	Cancel the specified core to use although the performance might slow down.

Message content	Physical Memory Isolation.
Level	Error
Explanation	Uncorrectable memory failure was detected and the physical memory was degraded.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Physical Processor Isolation.
Level	Error
Explanation	The physical CPU was degraded.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Physical SEL has been cleared.
Level	Information
Explanation	Physical SEL was cleared.
What to do	None.

Message content	RTC time synchronization has failed.
Level	Warning
Explanation	Synchronizing RTC with an NTP server failed.
What to do	Check the NTP setting.

Message content	Shadow Command is rejected.
Level	Error
Explanation	A request to LPAR manager Assist was discarded.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	RTC time was not successfully synchronized last time.
Level	Warning
Explanation	Synchronizing RTC with an NTP server failed due to some temporary factor.
What to do	When RTC time synchronization cannot succeed more than a day after this log message is collected, save the configuration and then synchronize RTC time. If RTC time synchronization system log is not collected even though you have saved the configuration, consult your reseller or call for maintenance personnel.

Message content	Shadow Command was retried.
Level	Information
Explanation	A request to LPAR manager Assist was retransmitted.
What to do	None.

Message content	Shared FC MCK Log was logged in LPAR at expansion card.
Level	Information
Explanation	Shared FC fault information was stored in the LPAR.
What to do	None.

Message content	Shared FC MCK Log was logged in LPAR.
Level	Information
Explanation	Shared FC fault information was stored in the LPAR.
What to do	None.

Message content	SR-IOV device of LPAR was damaged and isolated.
Level	Error
Explanation	Forcibly isolated the PCI device due to error.
What to do	Immediately shut down the guest OS to which the isolated PCI device is assigned. If the PCI device is not automatically recovered, execute Force Recovery to release the isolation. Then, reboot the guest OS to use the PCI device.

Message content	SVGA Initialization failed.
Level	Error
Explanation	Physical SVGA initialization failed.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	SVP access initialization failed.
Level	Warning
Explanation	Initializing the access to the management module failed.
What to do	Contact your reseller or maintenance personnel.

Message content	System Service request command failed.
Level	Error
Explanation	System service request failed.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	There are not enough H/W resources for SR-IOV feature.
Level	Error
Explanation	Detected hardware resource shortage for SR-IOV functions.
What to do	Check if all firmware combination supports SR-IOV. Refer to “Hitachi Compute Blade Emulex Adapter User's Guide for Hardware” for the correct combination.

Message content	Thermal error occurred.
Level	Warning
Explanation	A temperature rise warning event occurred.
What to do	Remove the dust from the air vent of the system device to improve ventilation. If this LPAR manager event log is collected although ventilation is improved, contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Thermal error was restored.
Level	Information
Explanation	A temperature rise warning was released.
What to do	None.

Message content	Uncorrectable memory error occurred (address).
Level	Error
Explanation	A memory error, which LPAR manager cannot correct, occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Unknown event occurred.
Level	Warning
Explanation	An unknown event was obtained.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	VNIC damage occurred.
Level	Error
Explanation	A virtual NIC fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	VNIC damage on LPAR manager Assist occurred.
Level	Error
Explanation	A virtual NIC (LPAR manager Assist) fault occurred.
What to do	Contact the reseller from which you purchased this equipment or consult maintenance personnel.

Message content	Your CPU core usage license expired.
Level	Information
Explanation	CPU core license is insufficient.
What to do	Purchase additional license or reduce the number of cores to use.

HCSM (Hitachi Compute Systems Manager) Alert Message

(1) Table headings of HCSM alert messages

ID: Message ID

Level: Level of the message: Information; Warning; Error

Message: Alert messages are shown. “X” and “Y” in a message stands for character strings.

(2) List of alert messages

ID	Level	Message
Description and Action		
0xFC71	Information	LPAR <>, Activating due to scheduled turn on request.
Description: Starts scheduled LPAR<X> activation. <X> is the LPAR number. Action: None.		
0xFC70	Information	LPAR <X>, Activation completed.
Description: LPAR <X> has been activated. <X> is the LPAR number. Action: None.		
0xFCA0	Warning	LPAR <X>, Failed to activate. (RC=<Y>)
Description: Failed to activate LPAR<X>. <X> is the LPAR number; <Y> is the error reason code. Action: Check if space for CPU and memory is enough for activating the LPAR.		
0xFC72	Information	LPAR <X>, Deactivation completed.
Description: Deactivated LPAR <X>. <X> is the LPAR number. Action: None.		
0xFCA1	Warning	LPAR <X>, Failed to deactivate. (RC=<Y>)
Description: Failed to deactivate LPAR <X>. <X> is the LPAR number; <Y> is the error reason code. Action: Contact your reseller or maintenance personnel.		
0xFC73	Information	LPAR <X>, Initiating shutdown due to scheduled turn off request.
Description: Starts scheduled LPAR<X> deactivation. <X> is the LPAR number. Action:		
0xFCA2	Warning	LPAR <X>, Watchdog timer has expired. (RC=<Y>)
Description: Watchdog timeout has been detected. <X> is the LPAR number; <Y> is the error reason code. Action: Contact your reseller or maintenance personnel.		
0xFC74	Information	Migration process started on the source LP. (SIP=<X>,DIP=<Y>)
Description: Starts LPAR migration on the source LP. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP. Action: None.		
0xFC75	Information	Migration process started on the destination LP. (SIP=<X>,DIP=<Y>)
Description: Starts LPAR migration on the destination LP. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP. Action: None.		
0xFC76	Information	Migration process completed on the source LP. (SIP=<X>,DIP=<Y>)

ID	Level	Message
Description and Action		
Description: LPAR migration process has been completed properly on the migration source. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP. Action: None.		
0xFC77	Information	Migration process completed on the destination LP. (SIP=<X>,DIP=<Y>)
Description: LPAR migration process has been completed properly on the migration destination. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP. Action: None.		
0xFCA3	Warning	Migration failed on the source LP. (SIP=<X>,DIP=<Y>,RC=<Z>)
Description: LPAR migration failed on the source LP. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP; <Z> is the error reason code. Action: Take actions following HCSM messages shown during LPAR migration task in operation.		
0xFCA4	Warning	Migration failed on the destination LP. (SIP=<X>,DIP=<Y>,RC=<Z>)
Description: LPAR migration failed on the destination LP. <X> is the IP address on the migration source LP; <Y> is the IP address on the migration destination LP; <Z> is the error reason code. Action: Take actions following HCSM messages shown during LPAR migration task in operation.		
0xFC78	Information	LPAR <X>, Sent information update alert.
Description: LPAR <X> information is updated. <X> is the LPAR number. Action: None.		
0xFC79	Information	LPAR <X>, Sent information update alert (add).
Description: LPAR <X> is added. <X> is the LPAR number. Action: None.		
0xFC7A	Information	LPAR <X>, Sent information update alert (remove).
Description: LPAR <X> is removed. <X> is the LPAR number. Action: None.		
0xFC03	Information	LP configuration format has been changed. (Previous Ver.=<X>,New Ver.=<Y>)
Description: LP configuration format has been changed. <X> is the configuration format version before change; <Y> is the configuration format version after change. Action: None.		
0xFC02	Information	LP configuration was saved. (RC=<X>)
Description: LP configuration was saved. <X> is the trigger for saving. Action: None.		
0xFC01	Information	LP started to shut down.
Description: LP started shutdown. Action: None.		
0xFC00	Information	LP boot has completed.
Description: LP boot has completed. Action: None.		

Software license

Information on software license

Software incorporated in LPAR manager consists of independent multiple pieces of software. Each of them is copyrighted by Hitachi, Ltd. or third parties.

The property rights and the intellectual property rights of software incorporated in LPAR manager, which Hitachi, Ltd. itself has developed or created, are owned by Hitachi, Ltd. The property rights and the intellectual property rights of documents related to the software are owned by Hitachi, Ltd. Those are protected by the copyright and other laws.

LPAR manager uses the following open source software in compliance with each software license agreement as well as software developed or created by Hitachi, Ltd. Visit those websites to read their software license agreement in English.

Software	License Agreement
Linux Kernel ser2net binutils	GNU General Public License version 2: Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
glibc	GNU Lesser General Public License 2.1: Visit the following URL. http://www.gnu.org/licenses/lgpl-2.1.html
bzip2	BSD License: Visit the following URL. http://www.opensource.org/licenses/bsd-license.php
tianocore EFI	BSD License/Eclipse License/FAT32 License/TianoCore.Org Contribution Agreement: Visit the following URL. http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=BSD_License_from_Intel http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=Eclipse http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=FAT32_License http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=How_To_Contribute
zlib	zlib license Visit the following URL. http://www.zlib.net/zlib_license.html
openssl	OpenSSL License Visit the following URL. http://www.openssl.org/source/license.html
shttpd	sHTTPd License "THE BEER-WARE LICENSE" (Revision 42): Sergey Lyubka wrote this software. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return.
Intel PRO/1000 Linux driver	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
Intel(R) Gigabit Ethernet	GNU General Public License version 2 Visit the following URL.

Software	License Agreement
Linux driver	http://www.gnu.org/licenses/gpl-2.0.html
Emulex Driver for Linux	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
Broadcom Tigon3 ethernet driver	GNU General Public License version 2 Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
Others: software contained in Redhat Enterprise Linux	GNU General Public License version2, and license agreement of each software Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html

12 Logical partitioning manager

13

System operation and management

This chapter provides information that can be useful when operating the system.

Server blade operation 1486
Operation of I/O slot expansion unit 1496
Network settings 1499
Setting management server information for ServerConductor/Blade Server Manager 1511
HCSM (Hitachi Compute Systems Manager) 1513
WWN in the Compute Blade 2000 1515
MAC address in the Compute Blade 2000 1517
Smart Configure 1518
N+M cold standby 1522
Digital certificates for the system web console 1543
E-mail notification 1555
SNMP function 1562
SNMP function for I/O slot expansion unit 1693
LDAP server linkage 1727
Power efficiency 1742
Dictionary updating 1748
Operation log 1752
Syslog Transfer 1766
Notes on Windows 1769
Useful settings for Red Hat Enterprise Linux 1771
Useful settings for VMware 1781
PCI error handling mode 1784
SMASH for server blades 1790
IPMI commands list 1800
Security of management interfaces 1802

Server blade operation

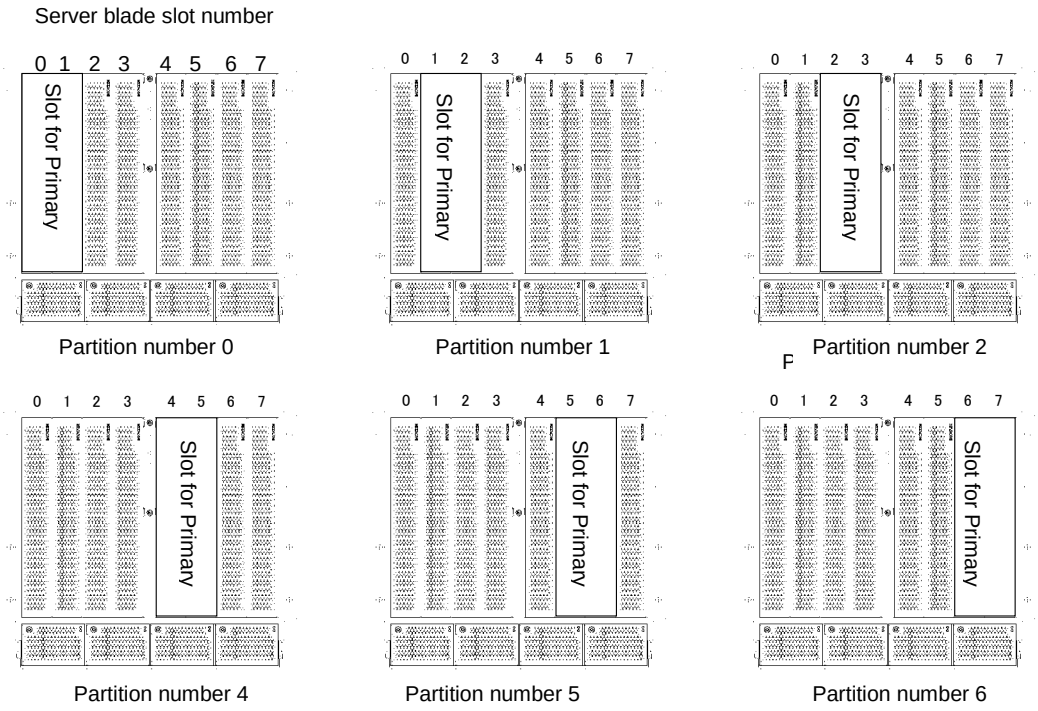
When running a server blade, you can perform operations remotely using the OS console and the remote console.

Symmetric multiprocessing (SMP) between server blades

With high-performance server blades, you can connect 2 server blades with the 2-blade SMP connection board or connect 4 server blades with the 4-blade SMP connection board to form SMP configuration with up to 8 central processing units (CPUs). See “PR Command” in Chapter 6 for how to change partitions for SMP configuration.

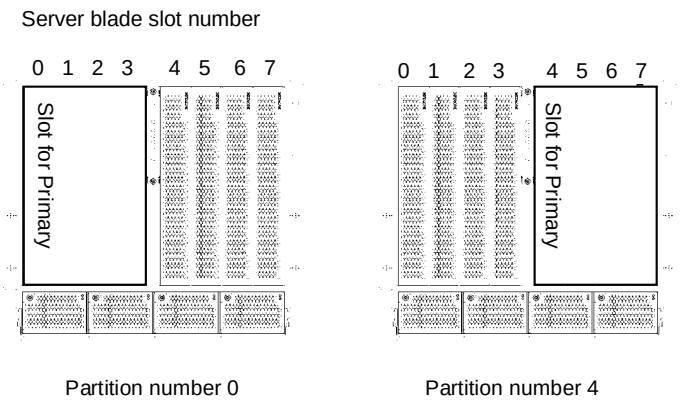
❑ Primary server blade and partition number

Between multiple server blades composing 2-blade or 4-blade SMP configuration, a server blade installed in a slot with a smaller number, located on the left viewed from the front, is called the primary server blade. The primary server blade can be installed in slot #0, 1, 2, 4, 5, 6 in the 2-blade SMP configuration. The slot to which the primary server blade is installed is the partition number.



Slot location for 2-blade SMP configuration

The primary server blade can be installed in slot 0 and slot 4 in the 4-blade SMP configuration. The slot to which the primary server blade is installed is the partition number.



Slot location for 4-blade SMP configuration

OS console (serial console redirection)

The OS console enables remote operation of the server blade's serial console, which transfers input/output data between the server blade's serial port and the console terminal.

The OS console can be accessed by connecting to the server blade via the management network, using Telnet or Secure Shell (SSH) client software installed on the console terminal.

The OS console does not support the operations described below.

1 Operation before OS Startup

The OS console functionality is not available until the OS starts. To control and do setup of the server blade, use the remote console.

2 OS Installation

You cannot use the OS console to install the OS. Use the remote console to install the OS.

For details about the remote console, see "Connect the System" in Chapter 3.

1. Preparation for using the OS console

1.1 Terminal software installation

Terminal software must be installed in the console terminal in advance.

(Note that some OSs of the console terminal includes terminal software and you may use it.)

The terminal software should provide the following functionality:

- Support for Telnet protocol
- Support for SSH version 2 protocol



Some input/output keys may not be supported, depending on the terminal software specifications.

Set up the terminal software to emulate the type of the terminal set up for the OS.

1.2 Checking the OS serial port settings

The OS console uses the server blade's COM1 port.

Sample setup with a server blade running Windows

Make sure the OS's COM1 port settings are as follows:

Port: COM1

Baud rate: 115200

Data bits: 8

Parity bits: None

Stop bits: 1

Flow control: None

Recommended terminal type: VT100



The OS console cannot be used as a Windows Special Administration Console (SAC).

Sample setup with a server blade running Linux 5

This example is for Red Hat Linux.

1 /boot/grub/grub.conf setting

At the end of each kernel line, enter the console parameters to be passed to the kernel.

console=tty0 console=ttyS0,115200

2 /etc/inittab setting

(1) To the last line, append "co:2345:respawn:/sbin/agetty 115200 ttyS0 vt100".

(2) Execute "init q(telinit -q)".

3 /etc/sysconfig /kudzu setting

Change to "SAFE=yes".

4 /etc/securetty setting

Add "ttyS0".

Sample Setup with a Server Blade Running Linux 6

This example is for Red Hat Linux.

1 /boot/grub/grub.conf setting

At the end of each kernel line, enter the console parameters to be passed to the kernel.

```
console=tty0 console=ttyS0,115200
```

When entering from the keyboard on OS console, set the following.

2 /etc/securetty setting

Add "ttyS0".

3 Create /etc/init/ttyS0.conf

```
# --------------------------
# ttyS0 – agetty
# This service maintains a agetty on ttyS0.

stop on runlevel [S016]
start on runlevel [23]
respawn
exec agetty -h -L -w /dev/ttyS0 115200 vt100
# --------------------------
```



Install Linux to use "Text mode" login.
If you installed Linux to use "Graphic mode" login, switch to "Text mode" login. For details about how to change the login mode, see your Linux manual.

2. Using the OS console

2.1 Starting the terminal software

Start the terminal software on the console terminal, and then connect to the server blade via Telnet or SSH.

For the server blade's IP address, see "LC Command" in Chapter 6.

2.2 Logging in to the server blade

You can log in to a server blade by entering the user name and password at Telnet or SSH prompt. For details about how to set the user name and password, see "Initial Settings with Server Blade Web Console" - "User Account Configuration" in Chapter 5.

If you use public key authentication of SSH, the public key should be registered to the server blade in advance to the SSH connections. See "Initial Settings with Server Blade Web Console" - "User Account Configuration"-" Edit User Accounts Screen" in Chapter 5.



You can create up to 1 session of OS console for a server blade. You cannot create multiple sessions of OS console simultaneously for the same server blade.

The following is a sample of SSH connection sequence using Linux terminal.

(1) Enter the command “ssh [-i public_key_file] -l <username > <Server Blade’s IP address>”

(2) The command tries the public key authentication, and then password authentication

If there is no public key registered to the server blade, you will be prompted to enter the password.



The username and the password are the same as the settings in "User Account Configuration" of Server Blade Web Console.

[-i public_key_file] in the SSH command line is optional.

Route to target: Advanced > USB Configuration > Legacy USB Support

2.3 OS console logging

The server blade provides the functionality for saving output from the OS console as a log. OS console logs can be downloaded using the server blade Web console. For details, see “Server Blade Web Console Function”-”Log Tab”-”Download Logs Screen” in Chapter 5.

3. Important tips

3.1 OS console operations

(1) The OS console is designed for input from the keyboard and does not support high-speed data input by file transfer or other such means. Always use the keyboard to communicate with the OS console.

(2) Recovery after Session Disconnection

Depending on your system environment, the screen display might slow down or the terminal software session may be disconnected. If this occurs, reconnect to the server blade over Telnet or SSH from the terminal software.

When an application produces a large amount of text data to be used with the OS console, performance may decline or a timeout may occur on the I/O device. It is recommended to evaluate the impact on the performance by suppressing text outputs. If required, try suppressing some text outputs to improve the performance.

(3) Text data input to the OS console with the cut-and-paste operation may not be transferred in its entirety if the data are more than 16 bytes.

3.2 Character codes and display colors

The terminal device may handle character codes and display colors differently from the server blade. If the following problem occurs, try one of the suggested actions.

Problem	Garbled display on the terminal device
Possible cause	(a) The serial port settings are set incorrectly. (b) An inappropriate character set is selected in the software on the terminal device side. (c) The software (Windows, Linux) on the sending side produces inappropriate character codes.
Action	(a) Check whether the settings in the software on the terminal device side are the same as those on the sending side. See "1.2 Checking the OS Serial Port Settings". (b) Select the appropriate character set in the software on the terminal device side. (c) See the documentation for the software on the sending side.

3.3 System request key in Red Hat Linux

To use the System Request Key functionality in the OS console, use the sequence described below.

Protocol Used	Sequence to Emulate System Request Key
Telnet protocol	Send an IAC (Interpreted As Command) break sequence as specified in the Telnet protocol or send [Ctrl] + [\]. The procedure for sending a break signal from terminal software differs according to terminal software. For details, see the documentation for your terminal software.
SSH protocol	Send [Ctrl] + [\].

The following are typical examples of break sequences:

- Microsoft Hyperterminal (Windows XP, Windows 2000, and Windows 98)

  > Press the **Ctrl** and **Break** keys simultaneously.

- Telnet client on UNIX variant

  > Press the **Ctrl** and "**]**" keys simultaneously to escape to Telnet command mode. Then type `send brk` and press **Enter**.

For details about the System Request Key, see the *Red Hat Enterprise Linux Reference Guide*". For security reasons, the System Request Key is disabled by default. See the *Reference Guide* for the setup procedure.



When performing OS operations from an OS console connected to the serial port on the front panel of the server blade, send the break signal of the RS232C interface from the terminal software.



The following is a sample of System Request Key.

[Ctrl]+[\], [X]: Display Help.

SysRq : HELP : loglevel0-8 reBoot
Crashdump tErm Full kIll saK showMem
Nice powerOff showPc unRaw Sync
showTasks Unmount shoWcpus

[Ctrl]+[\], [B]: Reboot the system.

Notes on the Wake On LAN (WOL) functionality

1 Enable the WOL functionality before you use power control via WOL in ServerConductor/Deployment Manager or ServerConductor/Blade Server Manager.



- WOL is supported only by the server blade's on-board local area network (LAN) controller. WOL is not supported by the server blade's expansion card or expansion adapter.
- If you are using the LAN driver (igb) included as standard in Red Hat Enterprise Linux 5.x, WOL using port 1 of the server blade's on-board LAN controller is not supported.

  By using the LAN driver (igb) provided by Hitachi, WOL can be used from port 1 of the on-board LAN controller, even in a Red Hat Enterprise Linux 5.x environment.

  By executing the following command, you can check whether the Hitachi LAN driver (igb) has been applied:

  # modinfo igb | grep version

  version: xx.xx.xx-hx

  If "-hx" (where x is a number) appears at the end of the "version:" value, the Hitachi LAN driver (igb) has been applied.
- When you use Windows Server 2012 R2 on a high-performance server blade, WOL function is not supported.

2 WOL is not enabled immediately after a server blade's AC power is turned on. To enable WOL on a server blade, enable the WOL setting on the OS supporting the advanced configuration and power interface (ACPI), and then shut down the OS. (WOL is enabled immediately after the OS shuts down.)

Note that WOL is disabled by the following:

(1) Turning off the AC power on the server chassis

(2) Inserting or removing a server blade

(3) A power outage

(4) Forcibly powering off the server blades and chassis (Power Button Override)

The server blade and chassis are forcibly powered off by holding down the power button for at least four seconds. WOL is also disabled by the following forced power-off methods: (1) the Management Module's "PC Command"; (2) remote power control provided through the server blade

Web console; (3) remote power control provided by a remote console application.

(5) Forced power-off from ServerConductor/Blade Server Manager

(6) Executing the Smart Configure function

For details about the Smart Configure functionality, see Smart Configure in N+M cold standby.

In cases (4) to (6) above, you can restore the WOL setting to the enabled status by shutting down the OS. Shut down the OS by powering off the blades using the front panel button, or by entering the Management Module's PC command.

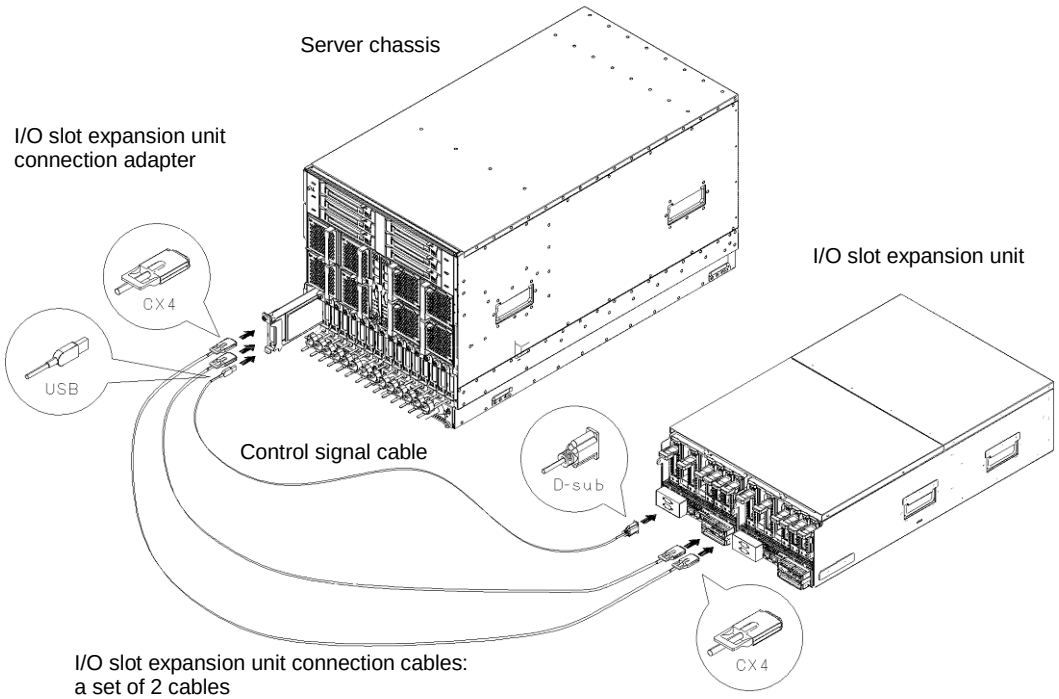


- In Windows Server 2003 and Windows Server 2008, OS setup is required to enable WOL. For the required settings, see "Using Wake-On-LAN (WOL) in LAN Devices" described in the *Compute Blade 2000 Software Guide*, and LAN Advanced Function Manual as appendixes included in *Compute Blade 2000 Software Guide*.
- In Red Hat Enterprise Linux 5.x, WOL is enabled by default.

Operation of I/O slot expansion unit

Overview of I/O slot expansion unit

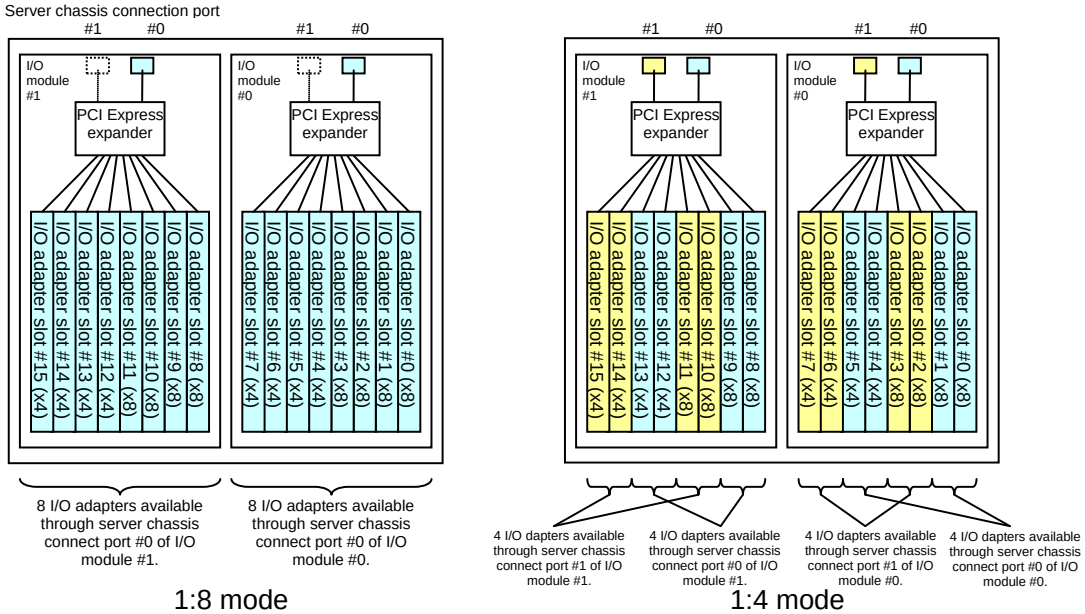
With Compute Blade 2000, I/O board slots can be expanded by the following procedure: install an I/O slot expansion connection adapter in the I/O slot expansion unit connect port, and connect it to the I/O slot expansion unit with the I/O slot expansion connection cable. Up to 16 slots per blade are available with the I/O slot expansion unit, and up to 8 I/O slot expansion units can be connected to a server chassis.

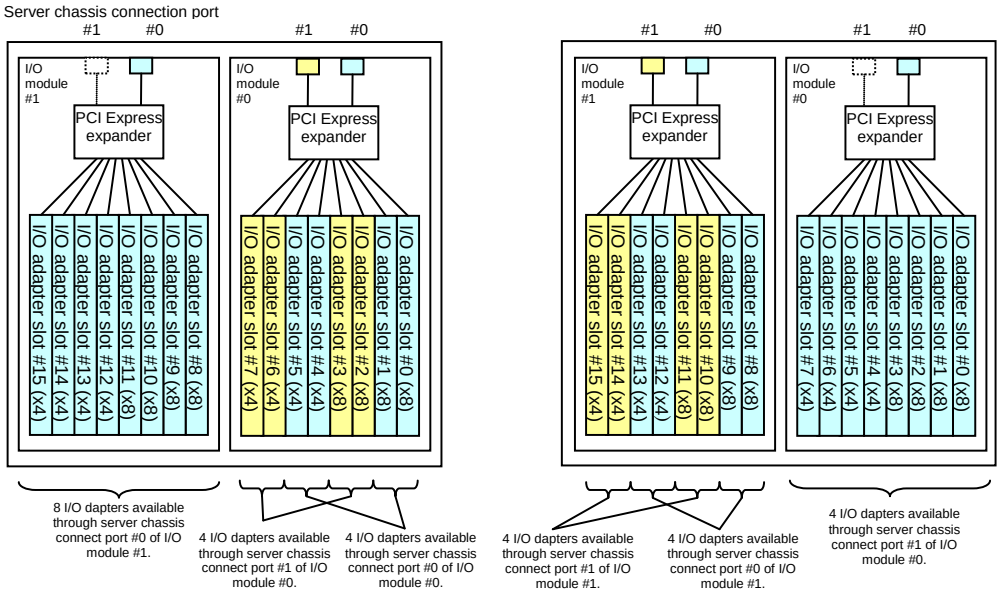


Connection between I/O slot expansion unit and server chassis

Operation mode of I/O slot expansion unit

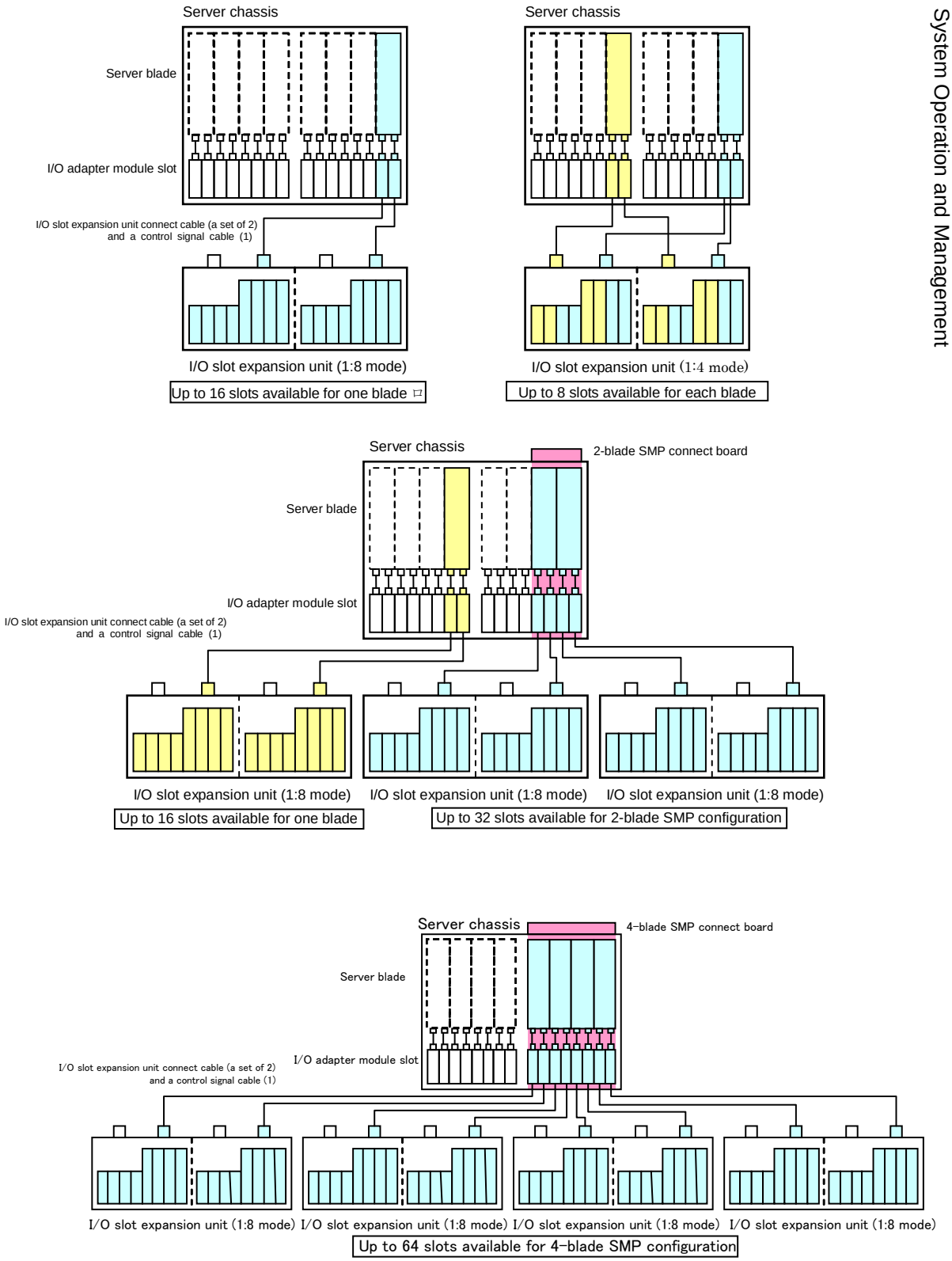
The I/O slot expansion unit has two I/O modules with eight I/O adapter slots. The I/O module has two operation modes, 1:8 mode and 1:4 mode. I/O adapter slots assigned to each module depend on the mode. Mode setting can be configured to two I/O modules in the unit respectively. Respective setting can be available for I/O modules connected to one physical partition. The following figure shows an example of operation modes and connection. Operation modes can be changed by maintenance personnel. Consult your reseller or maintenance personnel.





Mixed configuration with 1:8 mode/1:4 mode

Operation mode of I/O slot expansion unit



Examples of I/O slot expansion unit configuration

Network settings

List of module management interfaces

Each of the modules in the Compute Blade 2000 has a management interface. The table below lists the management interfaces and their purposes.

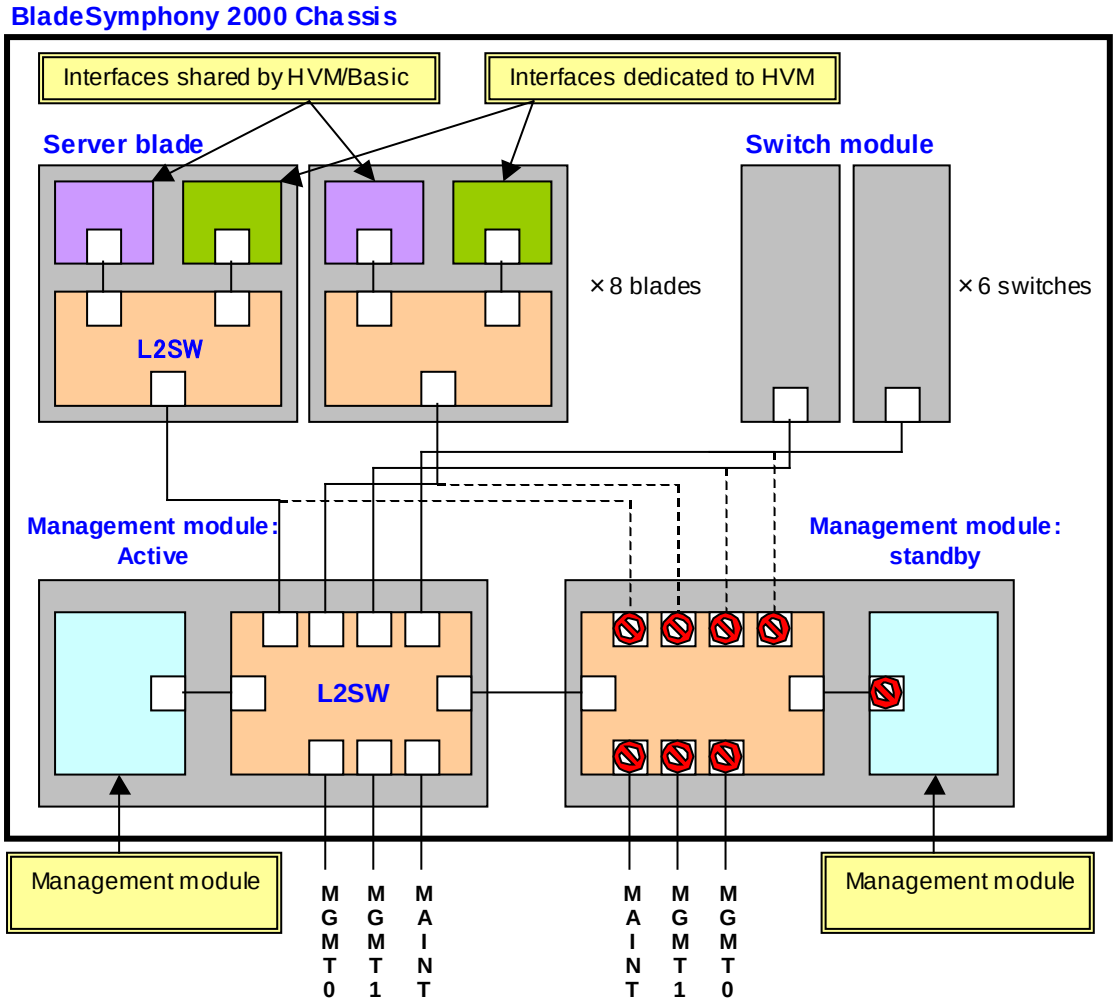
Module name	Interface name	Purpose	Remarks
Management module	Management module interface	▪ System Web console ▪ System console ▪ Communication with the ServerConductor (SC)/Blade Server Manager (BSM) management modules ▪ Simple Network Management Protocol (SNMP) ▪ E-mail notification	When management modules are configured redundantly, only the interface on the active side is enabled.
Server blade	Basic/logical partitioning (LPAR) manager shared interface	▪ Remote keyboard, video, mouse (KVM) ▪ Server blade Web console ▪ OS console ▪ intelligent platform management interface (IPMI) over LAN	For details, see "Initial Settings with Server Blade Web Console" in Chapter 5.
	LPAR manager Dedicated Interface	▪ LPAR manager console ▪ Communication between LPAR manager and SC/BSM	For details, see Chapter 12: Logical partitioning manager.
Switch module	Switch module interface	▪ Switch module console ▪ SNMP	For details, see Chapter 7, Configuring the LAN Switch Module and Chapter 10, Configuring the Fibre channel switch module”.

Management network

The Compute Blade 2000 Management Module and Server Blade have an L2SW built in, and the management interfaces of the modules are connected inside the Compute Blade 2000.

This network is connected outside the Compute Blade 2000 via the Management Module's external output ports (MGMT0 and MGMT1). By connecting cables to these ports, the management interfaces of each module can be accessed. Hereafter, this network is referred to as a management network.

A schematic diagram of the management network is shown below.





- The MAINT port is for maintenance purposes only and should not be used. Do not connect a cable to this port as it will hinder servicing.
- The ports on the standby management module are normally closed, and are opened only if the active management module fails or if the Link Fault Tolerance feature is enabled. For details, see Network configuration at management module failover and Link Fault Tolerance (LFT).

Internal network

In addition to the management network, the Compute Blade 2000 has an internal network built into the chassis.

The internal network is used for the following purposes:

- Control-related communication among the management modules
- Control-related communication between the management module and server blade.
- Communication for the OS console between the management module and server blade. See “CHCO command” in Chapter 6 for details.
- Connection to the Switch Module console (for details, see "Connection to the Setup Terminal" in Chapter 7.)
- Smart configuration (for details, see Smart Configure.)

For these purposes, the Compute Blade 2000 uses a class C (subnet mask 255.255.255.0) network address as its internal network. This IP address cannot be used on the Compute Blade 2000 management network or on the external network reached from the Compute Blade 2000 management network. The IP address is initially set as 192.168.253.0, and can be changed from the management module console. For the procedure to change the IP address, see "Command List" or "List of System Web Console Features" in Chapter 6.

NOTICE

- Errors could occur if an address identical to the network address on the internal network is used on Hitachi Compute Blade 2000 management network or the external network reached from Hitachi Compute Blade 2000 management network. Change the network address used on the internal network before connecting the cables.
- When you change the IP address used on the internal network, the management module restarts automatically.

Setting the connection method

The management interface for each module can be accessed via port MGMT0 or port MGMT1. You can choose from the connection methods in the following table. The connection method can be set separately for each module and can be changed from the management module console. For details about how to change the connection method, see "List of Commands" or "List of System Web Console Features" in Chapter 6.

Connection Method	User-Specifiable Per Module			Remarks
	Management Module	Server Blade	Switch Module	
Via MGMT0	Yes	Yes	Yes	
Via MGMT1	Yes	Yes	Yes	For details, see Port selection for management interface connection.
Using Tag-VLAN	Yes	Yes	Yes	For details, see Management interface connection using Tag-VLAN.
Management module exclusive	No	No	Yes	

Note 1 Yes: Can be selected; No: Cannot be selected.

Note 2 The same connection method is always used for the Basic/ LPAR manager shared Interface and LPAR manager Dedicated Interface for the same blade.

The management module exclusive method can only be selected for the switch module. This option behaves as follows:

- Connection to management interfaces from MGMT0 and MGMT1 is disabled.
- Connection from the Management Module to the Switch Module console is enabled.



- If you choose to connect to the switch module using the management module exclusive method, you must set an appropriate IP address. For the setting method, see "Setting the IP address"
- If you choose to connect to the switch module using the management module exclusive method, the management interfaces are invisible to devices outside the Compute Blade 2000. This means that SNMP and other functions that link with external nodes cannot be used.

The default connection methods at shipment are as follows:

Module	Connection Method	Remarks
Management Module	Via MGMT0	
Server Blade	Via MGMT0	The IP address is not preset. The server blade cannot be accessed until its IP address is set.
Switch Module	Management module exclusive	The IP address for connection using the management module exclusive method is preset in the switch module.

Setting the IP address

The IP address of each module's management interface can be set as follows:

Module		Connection Method	Remarks
Management Module		Management module's serial console or the system Web console	For details, see "Command List " or "List of System Web Console Features" in Chapter 6.
Server Blade	Basic/ LPAR manager Shared Interface	Management module's serial console or the system Web console	For details, see " Command List " or "List of System Web Console Features" in Chapter 6.
	LPAR manager Dedicated Interface	LPAR manager console	For details, see "Chapter 12: Logical partitioning manager".
Switch Module		Switch module console	For details, see your switch module manual.

If you choose to connect to the switch module using the management module exclusive method, you must set the switch module's IP addresses in advance, as listed in the following table. If the IP address differs from these values, the switch module console will not be accessible from the management module.

Switch module slot	IP address (*)	Subnet mask
Slot 0	192.168.253.35	255.255.255.240
Slot 1	192.168.253.36	255.255.255.240
Slot 2	192.168.253.37	255.255.255.240
Slot 3	192.168.253.38	255.255.255.240
Slot 4	192.168.253.39	255.255.255.240
Slot 5	192.168.253.40	255.255.255.240

(*) Value when the internal network setting is the factory default (192.168.253.0). If the internal network IP address has been changed, change the upper three bytes to the internal network setting.



The management module communicates with switch modules using IP address 192.168.253.33.

The default IP addresses at shipment are as follows:

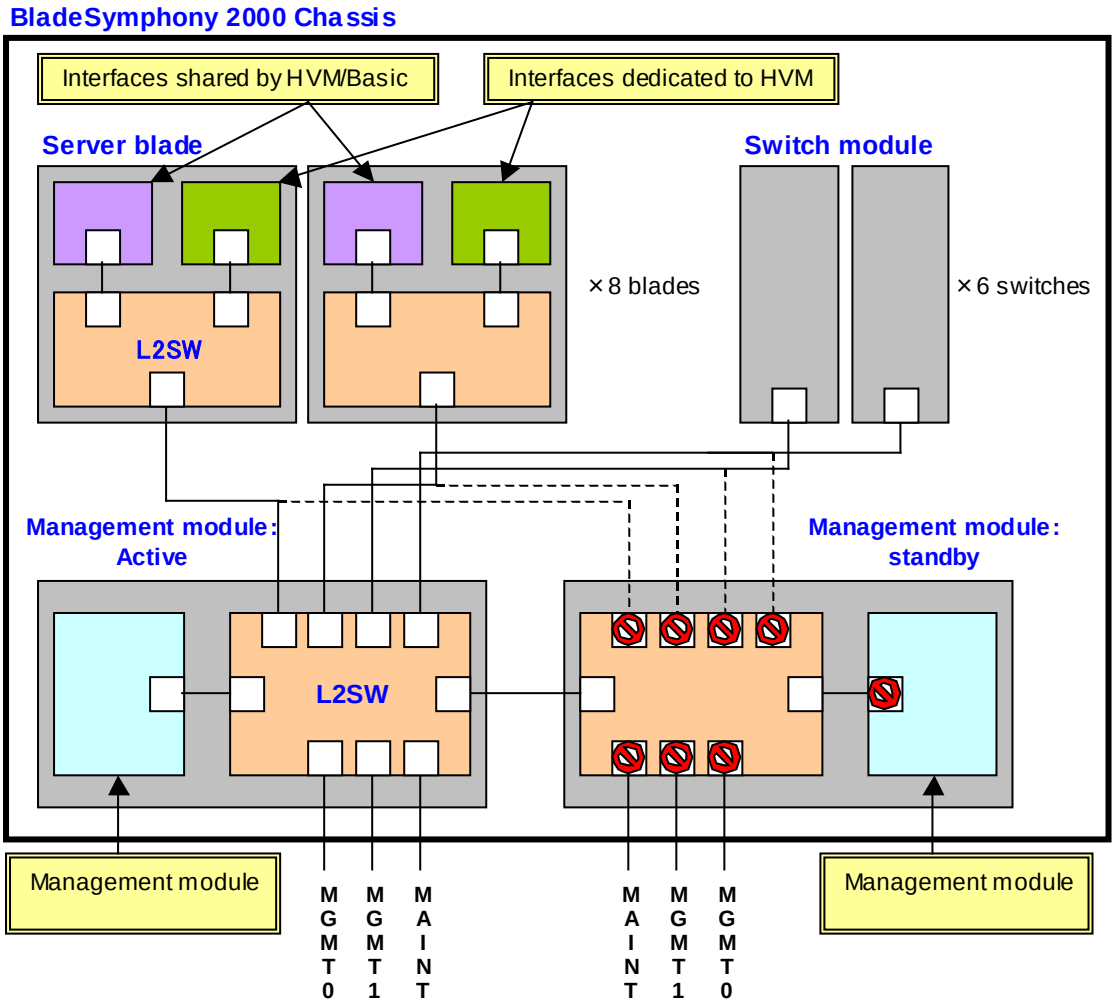
Module		IP address	Subnet mask	Remarks
Management Module		192.168.0.1	255.255.255.0	
Server Blade	Basic/ LPAR manager Common Interface	Not set.		
	LPAR manager Dedicated Interface	Not set.		
Switch Module	Slot 0	192.168.253.35	255.255.255.240	
	Slot 1	192.168.253.36	255.255.255.240	
	Slot 2	192.168.253.37	255.255.255.240	
	Slot 3	192.168.253.38	255.255.255.240	
	Slot 4	192.168.253.39	255.255.255.240	
	Slot 5	192.168.253.40	255.255.255.240	

Port selection for management interface connection

The Compute Blade 2000 is equipped with ports MGMT0 and MGMT1 for connecting to the management network. For each module, you can choose which of these two ports to use when connecting to the management interfaces. This allows the system to be configured for different purposes, as in these examples:

- Use MGMT0 to connect to the management module, and MGMT1 to connect to the server blade and switch module. This allows a clear separation of the network based on the management targets.
- Use MGMT0 to connect to server blades 0 to 3, and MGMT1 to connect to server blades 4 to 7, thereby distributing the network load.

You can change the port settings from the management module's serial console or from the system Web console. For the procedure, see "Command List" or "List of System Web Console Features" in Chapter 6.


BladeSymphony 2000 Chassis
Interfaces shared by HVM/Basic
Interfaces dedicated to HVM
Server blade
Switch module
×8 blades
×6 switches
L2SW
Management module: Active
Management module: standby
L2SW
Management module
Management module
MGMT0
MGMT1
MAINT
MAINT
MGMT1
MGMT0

Management interface connection using Tag-VLAN

Tag-VLAN (IEEE802.1Q) can be used between MGMT0 or MGMT1 and their associated switches for connecting to the management interfaces. This allows various configurations, such as the following:

- To enhance security, each server blade can be assigned to a different VLAN, so that the user of a server blade cannot connect physically to a different server blade.
- Each module can be assigned to a different virtual local area network (VLAN), so that the network is clearly segmented by the management target (when division between ports MGMT0 and MGMT1 is insufficient for this purpose).

A maximum of 19 VLANs can be created, with between 2 and 4000 VLAN IDs. Either one of ports MGMT0 and MGMT1 must be assigned to each VLAN; both ports cannot be assigned to the same VLAN.

The Tag-VLAN functionality can be used in conjunction with Port selection for management interface connection. This allows configurations such as the following:

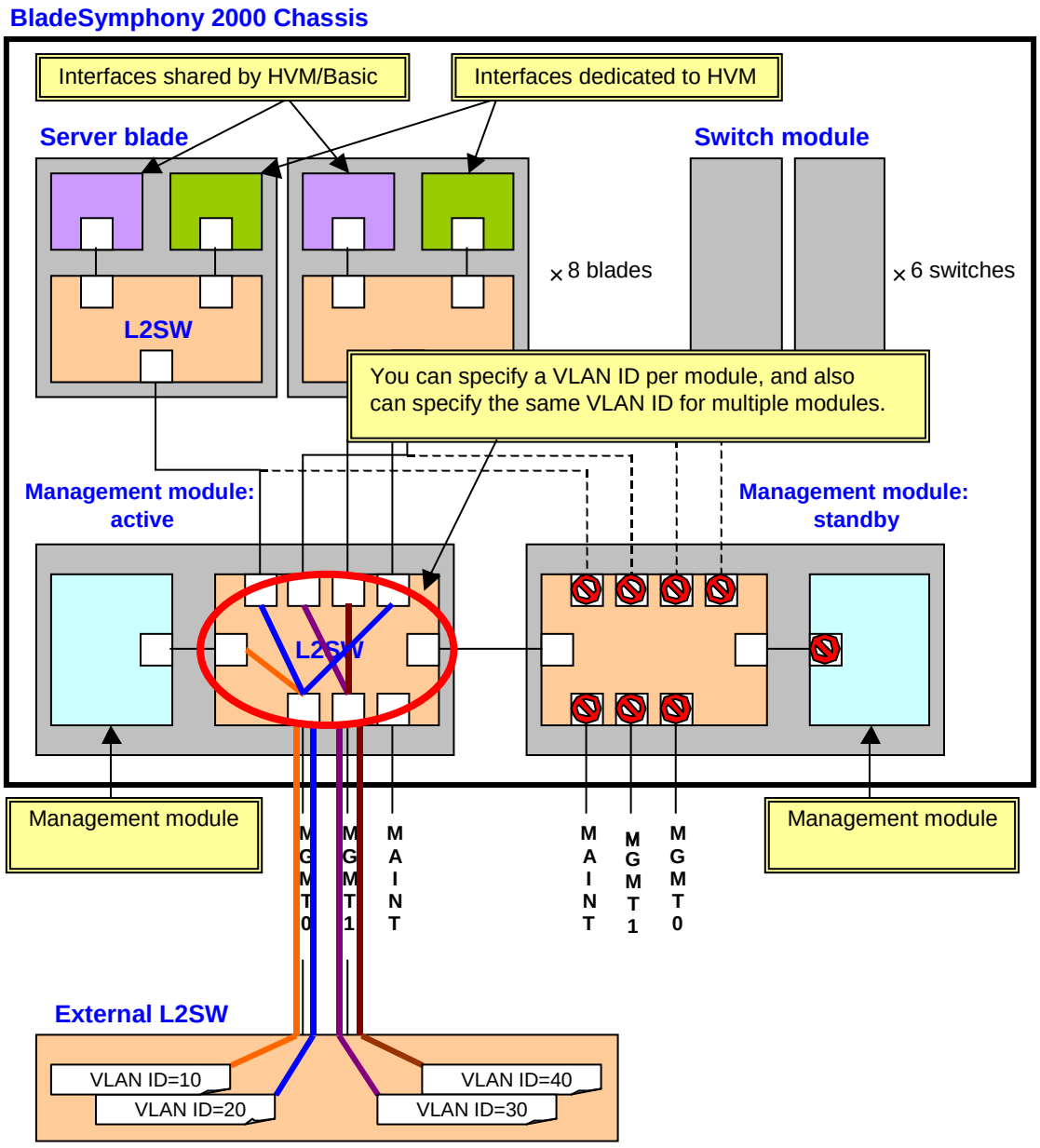
- Connect to the management module and switch module through MGMT0, not via a VLAN. Connect to server blades 0 to 3 through MGMT0 with VLAN IDs 10 to 13, and to server blades 4 to 7 through MGMT1 with VLAN IDs 20 to 23. This allows separation of the network for specific purposes and distributes the network load.



VLAN ID 1 and VLAN IDs 4001 to 4094 are used internally and cannot be used by the customer.



To use Tag-VLAN, the associated switches must also support IEEE802.1Q VLAN.


BladeSymphony 2000 Chassis
Interfaces shared by HVM/Basic
Interfaces dedicated to HVM
Server blade
Switch module
L2SW
×8 blades
×6 switches
You can specify a VLAN ID per module, and also
can specify the same VLAN ID for multiple modules.
Management module:
active
Management module:
standby
L2SW
Management module
Management module
MGMT0
MGMT1
MAINT
MAINT
MGMT1
MGMT0
External L2SW
VLAN ID=10
VLAN ID=20
VLAN ID=40
VLAN ID=30

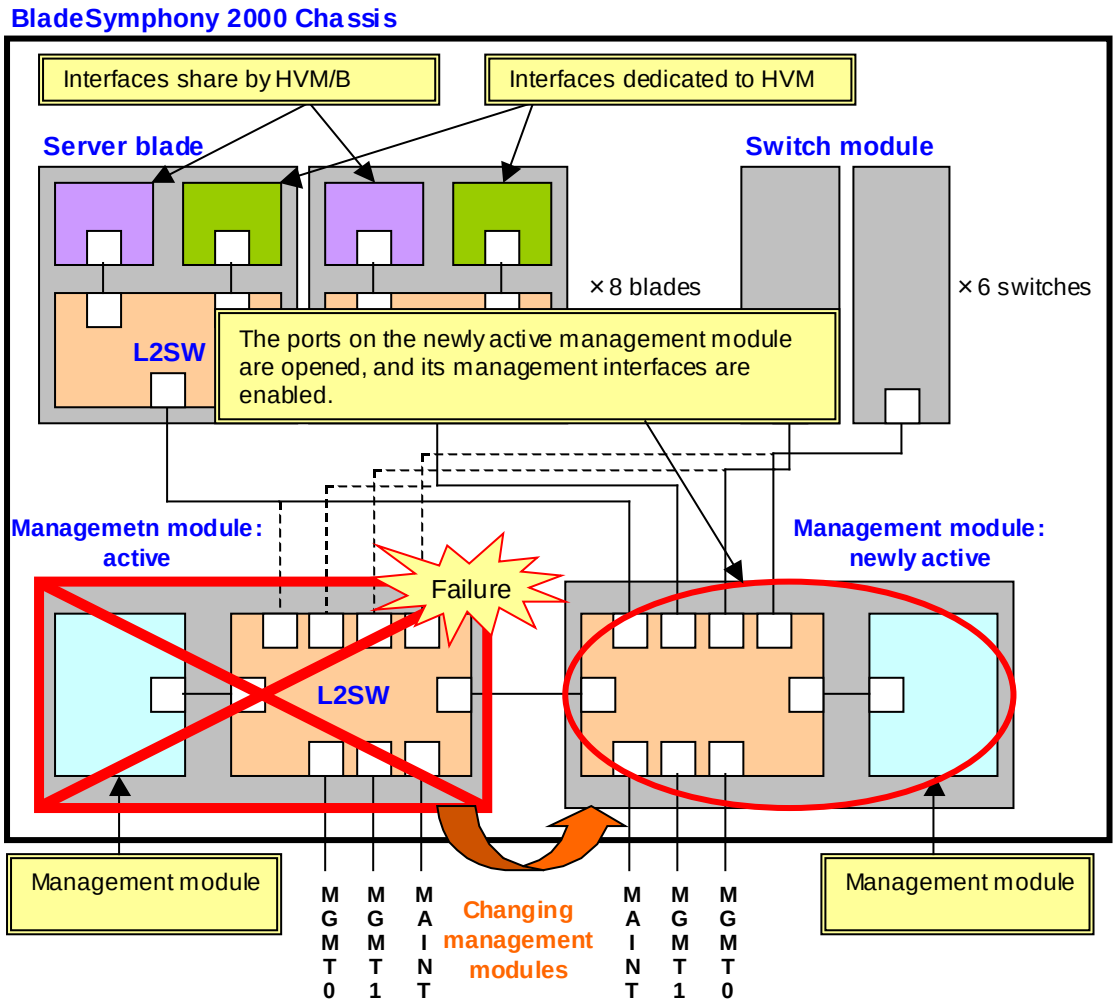
Network configuration at management module failover

In a redundantly configured management module, only the management interfaces on the active management module are enabled, and the ports on the standby management module are closed.

If a failure occurs on the active management module, the standby management module takes over and continues operation. The ports on the newly active management module are opened, and its management interfaces are enabled.

The newly active management module uses the same IP addresses for the management interfaces as did the failed-over management module.

When connecting to a management interface, you do not need to be aware of which management module is active.

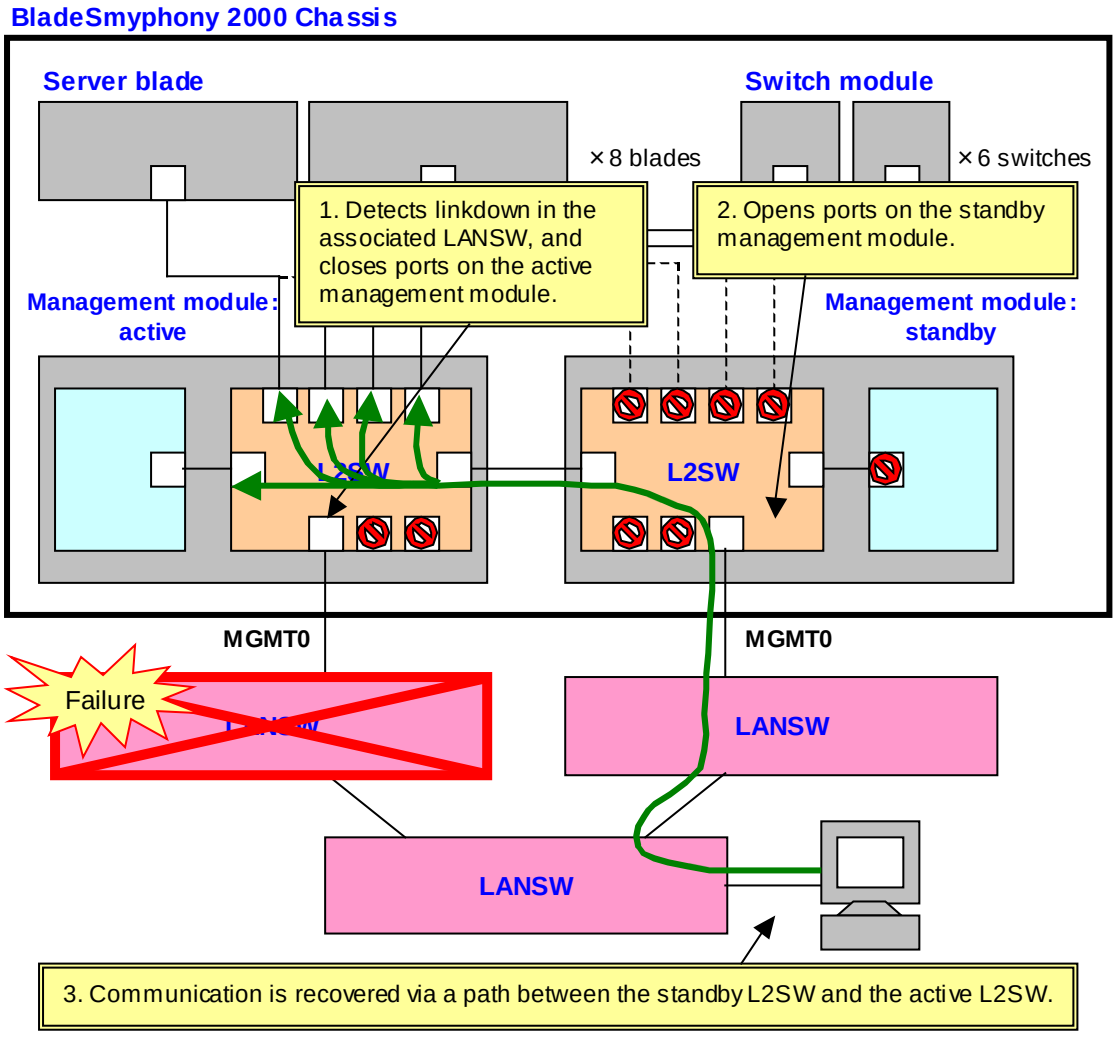


Tip

LAN cables must be connected to both the active and standby management modules to enable continuous connection to the management interfaces at failover.

Link Fault Tolerance (LFT)

When the management module is configured redundantly, you can also build redundancy into the management network. This functionality is known as Link Fault Tolerance (LFT). An overview of LFT is shown in the following figure.



LFT port selection

LFT applies to ports MGMT0 and MGMT1. LFT can be independently enabled or disabled on these two ports. Because they are failed over independently of each other, if each port is connected to a different switch, a failover occurring on the network between one of the ports and its associated switch will affect only that port.

In the factory settings, LFT is enabled on both MGMT0 and MGMT1. You can change this setting from the management module's serial console or from the system Web console. For the procedure, see "Command List" or "List of System Web Console Features" in Chapter 6.

LFT trigger events

When the system detects that the link to the active management module's port MGMT0 or MGMT1 has gone down, the link is switched by the LFT feature. The link may be switched for the following reasons:

Trigger event	Remarks
Broken or loose cable between the port and associated switch	
Hardware fault on the associated switch	Only if the link is deemed broken by the management module.

In initial state, when the link to an LFT-enabled port on the active management module is detected as being down for three seconds continuously, the link is switched to the other port. You can change the number of seconds before link switching begins, using the management module's serial console or the system Web console. The specifiable range is 1 to 3600 seconds. For the procedure, see "Command List" or "List of System Web Console Features" in Chapter 6.

LFT recovery

In initial state, when the link to an LFT-enabled port on the active management module is detected as being up for 180 seconds continuously, the link to that port is restored. You can change the number of seconds before link recovery begins, using the management module's serial console or the system Web console. The specifiable range is 1 to 3600 seconds. For the procedure, see "Command List" or "List of System Web Console Features" in Chapter 6.



The management module monitors the link status at 1-second intervals. Therefore, the time until link switching or recovery is initiated is the specified value plus 1 second. Further allowance must be made for the processing time until switching is completed.

Setting management server information for ServerConductor/Blade Server Manager

Management server information needs to be set when using ServerConductor/Blade Server Manager (BSM). This refers to the information reported to BSM when the management module detects a fault or other event.

❑ Destination BSM setting

(1) On the main menu, enter S and press **Enter**.

At the prompt SVP, type BSM and press **Enter**. The following window appears.

```
chassis≠1(1)SVP>BSM

<< BSM – SC/BSM setting. >>

-- Manager setting --
No. Name           IP address       Alert level
--- -------------  ---------------- -----------
  0  -----------    --------------    ---------
  1  -----------    --------------    ---------
  2  -----------    --------------    ---------
  3  -----------    --------------    ---------

  M. Edit manager setting
  D. Delete manager setting.
 DB. Show/Edit basis detail setting.
 DM. Show/Edit manager detail setting.
  T. Test N+M cold standby.
  Q. Quit.
(M, D, DB, DM, T, [Q]): M
```

Menu		Description
M.	Edit manager setting.	Edit BSM information.
D.	Delete manager setting.	Delete BSM information.
DB.	Show/Edit basis detail setting.	View or edit basic information.
DM.	Show/Edit manager detail setting.	View or edit detailed BSM information.
T.	Test N+M cold standby.	Test N+M cold standby.
Q.	Quit	Quit the BSM setup menu.

(2) If you select **M. Edit manager setting.**, the following window appears.

Enter the host name, IP address and SVP alert level as indicated in the window.

(3) Check the settings and enter Y at the confirmation prompt Confirm?

```
Select manager (0-3, [Q=Quit]): 0
Name                    : BSM_0
([Unchange]):
IP address              :  0. 0. 0. 0
([Unchange]): 192.168.0.20
Alert level             l: All
(0=All, 1=Alert, 2=Information, 3=Disable, [Unchange]):

-- Manager setting --
No. Name           IP address       Alert level
--- -------------- ---------------- -----------
  0 BSM_0          192.168.  0. 20 All
  1  -----------    --------------  ---------
  2  -----------    --------------  ---------
  3  -----------    --------------  ---------

Confirm? (Y, [N]): Y
```

Item	Description
Name	Set the host name of the BSM.
IP address	Set the IP address of the BSM.
Alert level	Set the SVP alert level. All: Report all information. Alert: Report failures. Information: Report information-only data. Disable: Do not report SVP alerts.



Set chassis ID before setting destination BSM. If changing the chassis ID after setting BSM, delete and re-register the host, LPAR manager, server chassis, and IOEU on BSM. Refer to the BSM manual.

If not, the chassis ID information before the change remains on BSM, for which BSM chassis management may not work properly.



If you change the Alert Port setting in the BSM settings from the default (20079), you must change the setting in the BSM services file. You can edit the Alert Port setting by selecting "DM. Show/Edit manager detail setting."

For details, see the BSM documentation.

HCSM (Hitachi Compute Systems Manager)

Hitachi Compute Systems Manager (HCSM) is software for managing the server chassis in a large scale system. A system administrator can efficiently manage hardware resources in the system, monitor operation, and control power consumption using HCSM.

Note

Regardless whether HCSM is used, up to 10 system consoles can be simultaneously connected to the management module.

Notes on connection between HCSM and a management module

Hitachi Compute Server Manager (HCSM) is connected to a management module via Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Thus, you need to enable HTTPS protocol. See Chapter 6 > System Web Console > Service Settings > Service Settings List View > HTTP for details about checking and changing HTTPS settings for a management module.

Note

For HCSM settings, see "Managing Security" in "System Web Console", Chapter 6 for more details.

When the HCSM port number used for communication via HTTPS is changed from the default number 443 to another, set the same port number in the management module.

With firmware versions earlier than A0310, the port number is set to 80 for HTTP protocol by default. Once the firmware is updated to A0310 or later at fields, the port number also needs to be changed from 80 to 443 for HCSM (HTTPS).

Management by HCSM

HCSM has a feature for searching server chassis in the target system, which we will see as Discovery. When interfacing a management module with HCSM, you need not set HCSM information to the management module.

Perform Discovery with HCSM, search a server chassis, add it, and HCSM information including its IP address and alert settings is automatically set to the management module. HCSM information set to the management module can be changed or removed using the System console and the System Web console. You can interface a management module with up to four HCSMs.

Relation with ServerConductor/BladeServer Manager

Even if a management module has settings for ServerConductor/Blade Server Manager, referred to as BSM hereinafter, the management module can be interfaced with HCSM. You need not delete BSM settings.

WWN in the Compute Blade 2000

The Fibre-channel board that can be used in an N+M cold standby system has three different world wide names (WWNs): Default Physical WWN, Optional Physical WWN, and virtual FC WWN. These WWNs are described below.

- Default Physical WWN

  A WWN that is unique and permanent to a specific Fibre-channel board. It corresponds to the traditional Fibre-channel board WWN. The Default Physical WWN can be shown on the label attached to the Fibre-channel board.

  When setting Fibre Channel over Ethernet (FCoE) as Personality on 10 Gb converged network adapter (CNA) adapter or 10 Gb CNA board, you can use the Default Physical WWN unique to the CNA.

- Optional Physical WWN

  An Optional Physical WWN assigned to a Fibre-channel board: This WWN can be changed and is used only in Compute Blade. When a Fibre-channel board is replaced, the Optional Physical WWN remains unchanged, provided the board is installed in the same slot as before.

- When setting FCoE as Personality on 10 Gb CNA adapter or 10 Gb CNA board, you can assign the Optional Physical WWN to the CNA. Even if you change the 10 Gb CNA adapter or 10 Gb CNA board, the Optional Physical WWN will not be changed as long as the new adapter or board is installed in the same slot.

- virtual FC WWN *1

  A WWN managed by LPAR manager: A unique WWN is generated by LPAR manager for each LPAR manager system, based on the seed information for virtual FC WWNs. When a Fibre-channel board is used in LPAR manager mode, the virtual FC WWN is used regardless of whether the peripheral components interconnect (PCI) device is specified as dedicated or shared. When a Fibre-channel board is replaced, the virtual FC WWN remains unchanged, provided the board is installed in the same slot as before.

  *1: See "Shared FC Functions" in Chapter 11.

WWN in Basic mode

- Partition with N+M cold standby Enabled

  Always use the Optional Physical WWN

- Partition with N+M cold standby Disabled

  When the Smart Configure method is inline, you can select between the Default Physical WWN and Optional Physical WWN with WWN settings. When the Smart Configure is pxe, always use the Default Physical WWN.

For Smart Configure, see Overview of Smart Configure.

For Smart Configure method and WWN settings, see “PR Command” in Chapter 6.

By setting the Optional Physical WWN of the Fibre-channel board installed, 10 Gb CNA adapter, or 10 Gb CNA board installed in the active partition to the fibre channel board, 10 Gb CNA adapter, or 10 Gb CNA board in the active partition to the Fibre-channel board of the standby partition, storage area network (SAN) connectivity can be maintained when N+M switching occurs. In an N+M cold standby configuration, because the WWN as viewed from the OS on the partition is unchanged after N+M switching, WWN-dependent software functions such as Persistent Binding can be still available as they are.

Note that only the Default Physical WWN or Optional Physical WWN of a Fibre-channel board can be used. The two WWNs cannot be used in combination.

Virtual fibre channel (FC) WWNs are used in LPAR manager mode. You can check the WWN used by a system in the "Allocated FC Information" screen on LPAR manager. See "Allocated FC Information" in Chapter 12.

Note that the Default Physical WWNs and Optional Physical WWNs cannot be used in LPAR manager mode.



- You can set an Optional Physical WWN to a Fibre-channel board using the 10 Gb CNA adapter or 10 Gb CNA board using the Smart Configure function. For details, see Overview of Smart Configure.
- The WWN unique to the Fibre-channel board 10 Gb CNA adapter or 10 Gb CNA board is not used in N+M cold standby.
- Optional Physical WWNs apply only in Compute Blade. They are not used for Fibre-channel boards implemented in any other hardware.
- Virtual FC WWNs apply only in LP mode. They are not used for Fibre-channel boards implemented in any other hardware.
- Initializing Optional Physical WWNs, following server failover, for example, may result in duplicated WWNs. When you initialize Optional Physical WWNs, always make sure that none have been duplicated.
- After initializing Optional Physical WWNs, you must change the settings in Compute Blade, SAN, and BSM Plus.
- When Smart Configure method is inline, management modules baseboard management controller (BMC), and extensible firmware interface (EFI) firmware are required to support Smart Configure.

MAC address in the Compute Blade 2000

LAN controllers available for N+M cold standby have the following two media access control (MAC) addresses:

- Default Physical MAC address

  The Default Physical MAC address is unique to LAN controllers and unchangeable. Typical LAN controllers have this type of MAC address.

- Optional Physical MAC address

  The Optional Physical MAC address is a MAC address added to a LAN controller and changeable. This can be available for Hitachi Compute Blade, and remains the same address as long as a LAN controller is installed in the same slot even if you changed the LAN controller.

To keep the LAN connection with Compute Blade 2000, assign the Optional Physical MAC address, which is assigned to the LAN controller on an active partition, to the LAN controller on the standby partition at switching partitions with N+M cold standby. MAC address-depending software functions, such as Persistent Binding, can be available after switching partitions because the MAC address viewed from an OS is not changed after switching partitions with N+ M cold standby.

Either Default Physical MAC address or Optional Physical MAC address is available. Both of them cannot be used at the same time. For information about how to select a MAC address, see “PR Command” in Chapter 6.



- Optional Physical MAC address can be available for Hitachi Compute Blade. If you install the LAN controller on another unit, the Optional Physical MAC address will not be used.
- When an Optional Physical MAC address is initialized after switching servers, the Optional Physical MAC address may overlap. Make sure that the MAC address does not overlap when initializing the MAC address.
- You need to set “inline” as a Smart Configure method when assigning an Optional Physical MAC address to a LAN controller. With the inline method, make sure to have management modules, BMC, and EFI firmware support the inline method.
- If a LAN controller does not support Optional Physical MAC address, you cannot operate the LAN controller using Optional Physical MAC address.

Smart Configure

Overview of Smart Configure

The following features use Smart Configure. Smart Configure for each feature is outlined below. If Smart Configure is enabled, the Fibre-channel board 10 Gb CNA adapter or 10 Gb CNA board uses an Optional Physical WWN.

- N+M cold standby

  For N+M cold standby, setting information for the active partition is obtained in advance and stored in the management module.

  When switching N+M, the setting information for the active partition stored in the management module is set for the standby partition.

  In addition, the Optional Physical WWNs assigned to the Fibre-channel board 10 Gb CNA adapter or 10 Gb CNA board in the active and standby partitions are swapped and re-assigned to each Fibre-channel board 10 Gb CNA adapter, or 10 Gb CNA board.

  Smart Configure is performed when the setting information is obtained or set, and when the Optional Physical WWNs are set.

  For details of N+M cold standby, see N+M cold standby.

  For details of Optional Physical WWNs used in N+M cold standby, see N+M cold standby.

> ***NOTICE***
>
> Do not operate the server blade during Smart Configure. If you do, Smart Configure may fail.



- After Smart Configure, the partition cannot start by Wake On LAN.
- Performing Smart Configure causes SAN boot to be automatically assigned the lowest priority in the basic input/output system (BIOS) boot priority setting.

Method of Smart Configure

Smart Configure includes two methods, such as “Preboot eXecution Environment (pxe)” and “inline”. The following table describes both modes.

	pxe	inline
Outline	Obtain and configure the setting information on partitions from the dedicated OS: conventional method.	Obtain and configure the setting information on partitions with EFI.
Required time for Smart Configure	3 to 15 minutes	A few minutes shorter than that of the prex with the same configuration, due to no need of booting the dedicated OS.
Smart Configure execution triggers	- When PC command or PR command is executed. - When N+M is switched or recovered from the switch with BSM Plus. - When the system is powered on. - When the partition configuration is changed. - When BMC (Baseboard management controller) is completely initialized.	- When PC command or PR command is executed. - When the system is powered on. - When the partition configuration is changed. - When BMC (Baseboard management controller) is completely initialized.
Selectable server blade	X55A1 model only (*1)	All blades (*2)

(*1) “pxe” cannot be selected when a host bus adapter (HBA) other than Hitachi 4 Gb 2-port Fibre-channel mezzanine card or Hitachi 4 Gb 2-port Fibre-channel adapter is used, or when an I/O slot expansion unit is connected. If you add the card or unit when “pxe” is selected, the method is automatically switched to “inline” to operate.
If “pxe” is selected with a standard server blade, X55A1, where the Emulex 8 Gb 2-port Fibre-channel adapter, which was shipped on March 2010 or earlier, is installed, set the Smart Configure method to “inline” because the Smart Configure will not automatically work with the “inline” method. See Chapter 6: Management Module Settings > System Console Command Reference > Partition Management > PR Command for details about how to set Smart Configure.

(*2) To use the inline method, management modules, BMC and EFI firmware are required to support Smart Configure.

Since the inline method does not need to execute Smart Configure in switching N+M, it requires a shorter time required for switching N+M than the pxe method.



For executing N+M cold standby, Smart Configure methods for the active and standby partitions can be different.

Smart Configure execution triggers

Smart Configure is performed either manually or automatically to obtain or set information in the following cases:

#	Trigger	Smart Configure method	
		pxe	inline
1	When the PC command or PR command is executed	Executed	Executed
2	When N+M is switched or recovered from N+M switching by BSM Plus	Executed	Not executed (*1)
3	When the power to the system equipment is powered on	Executed	Executed
4	When the partition configuration is changed.	Executed	Executed
5	When BMC (Baseboard Management Controller) initialization is completed.	Executed	Executed

(*1) In the standby partition that recovered from switching, however, Pre-configure is executed.

The following describes how Smart Configure is performed in each case:

(1) When the PCC command or PR command is executed

(a) PC command

You can use the PCC command to perform Smart Configure. This Smart Configure is performed to maintain the partition setting information in the management module after the partition setting is completed and SAN boot is available.

(b) PR command

When the N+M cold standby aid function is enabled using the PR command, Smart Configure is executed to set the Optional Physical world wide name (WWN to the Fibre-channel board.

(2) At N+M switching, or restoration from N+M switching by BSM Plus

With the pxe method, Smart Configure is executed to set the setting information of the active partition to the standby partition. When original partition settings are restored from the N+M switched status, Smart Configure is executed in both the active and standby partitions.

With the inline method, the setting information of the active partition is set to the standby partition during the power on and OS is booted. Thus Smart Configure is not executed at N+M switching. When a partition is restored from the state after the N+M switching, Smart Configure is not executed to the active partition. But Smart Configure is executed to the standby partition so that it can be switched. Smart Configure with this trigger is automatically executed by BSM Plus.

(3) When the power to the system equipment is turned on

When the system equipment powered off and on after the N+M cold standby is configured, Smart Configure is automatically executed to recover the N+M cold standby.

(4) When the partition configuration is changed

When the following changes are executed in the partition configuration, Smart Configure is automatically executed and the setting information in the management module is updated.

(a) When changing the number of server blades that belong to the partition using the PR command.

(b) When inserting a server blade

(c) When powering on the server blade after plugging and unplugging the I/O board module.

(5) When the BMC (Baseboard Management Controller) is completely rebooted

When the power of the server blade is off after BMC is rebooted with the PR command or by BMC itself, Smart Configure is executed by the management module and the setting information in the management module is updated.

Operation of partitions during Smart Configure

The light emitting diode (LED) on the front panel of the server blade blinks during Smart Configure.

While the condition LED (CND) is blinking, the power to the partition is temporarily turned on.

For details of the condition LED that blinks, see "Standard server blade" in Chapter 2 for the description of the names and functions of each part.

Time required for Smart Configure

The time required to perform Smart Configure varies depending on the number of installed central processing unit (CPUs), memory size, and the types and number of PCI cards installed.

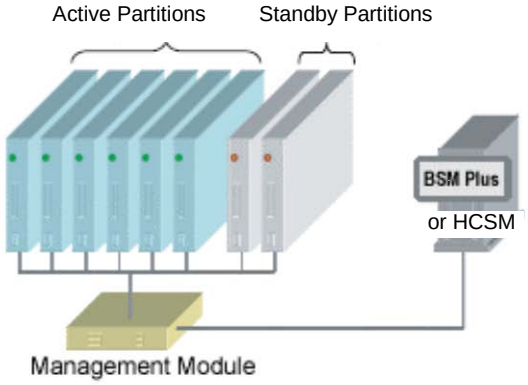
Partition	Required time (minutes)
Xeon server blade	3 to 15

N+M cold standby

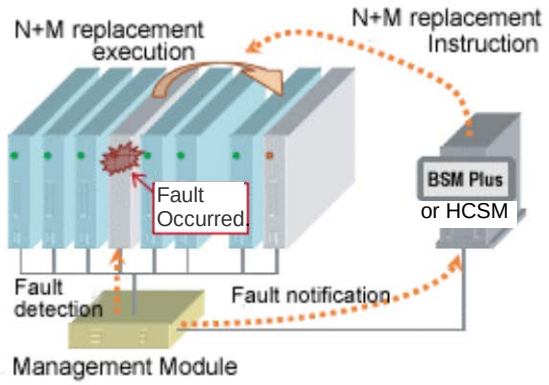
N+M cold standby overview

The N+M cold standby is a function to switch over from the active partition (task partition) to a standby partition in case of hardware failure. It is a management server, ServerConductor/Blade Server Manager Plus (BSM Plus hereinafter) or Hitachi Compute Systems Manager (HCSM) that receives and analyses a report on the hardware failure in the partition.
Providing a standby partition to multiple active partitions enables the operation to resume by activating the standby partition. The operation is temporarily interrupted due to a hardware-failure, but the corrective actions from a failure occurrence to the operation resumption can be streamlined with less hardware resources.

The N+M cold standby function supports LPAR manager (by BSM Plus). When the hardware fault occurs in the active partition on which multiple LPARs are running, those running on the active partition are rebooted on the standby partition. The standby partition can be shared between the active partitions in both Basic mode and LPAR manager mode.



Normal Operation



N+M Replacement

Tip

The N+M cold standby can be set over multiple systems. The active and standby partitions need not exist in the same system.

- Only a partition with the same configuration as the active partition and with the LPAR manager license enabled is available for the standby partition to the active partition with the LPAR manager license enabled.
- When a standby partition is shared by the active partitions in Basic mode and LPAR manager mode, configure the standby partition using the model with LPAR manager that can be used in both Basic mode and LPAR manager mode.
- Implementing the N+M cold standby would require separate installation of ServerConductor/Blade Server Manager Plus. For details, contact the reseller from which you purchased this product.
- When you use the teaming function provided by Intel® PROSet on the server blade, it is necessary to prepare the N+1 Teaming Kit additionally. For details, contact the reseller from which you purchased this product.
- Different Smart Configure methods are allowed for the active and standby partitions.

Note

When recovering N+M cold standby, make sure that an operating mode (LP mode or Basic mode) for the standby server blade is the same as that for the active server blade at N+M group registry. When changing the operating mode for the standby server blade after N+M failover is executed, make sure that the operating mode is returned to the original mode before recovering N+M cold standby. If you try to recover N+M cold standby with the standby server blade having the changed operating mode, the following may occur.

- LPAR manager configuration may not be recovered correctly.
- Recovering N+M cold standby may fail.

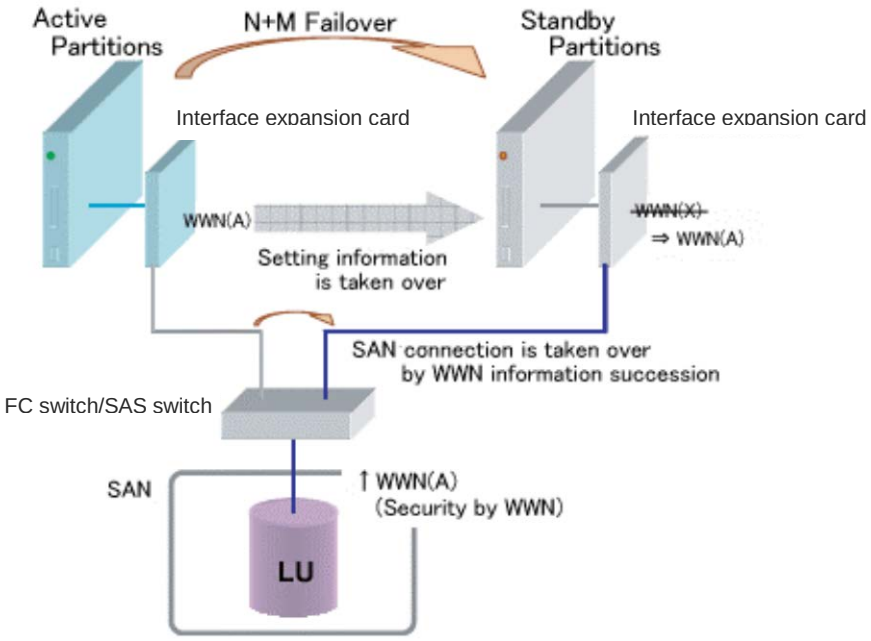
Mechanism of the N+M cold standby

❑ Mechanism of the N+M Cold Standby

(1) Partition in Basic mode

In the N+M cold standby, various settings on active partitions are taken over by the standby partition when N+M failover of partitions occur in the Basic mode.

You can, therefore, boot the server from the same disk logical unit (LU), and resume the same OS environment as the active partition, on the standby partition. Hereinafter, the settings to be taken over are referred to as “partition configuration information” or merely “configuration information”.

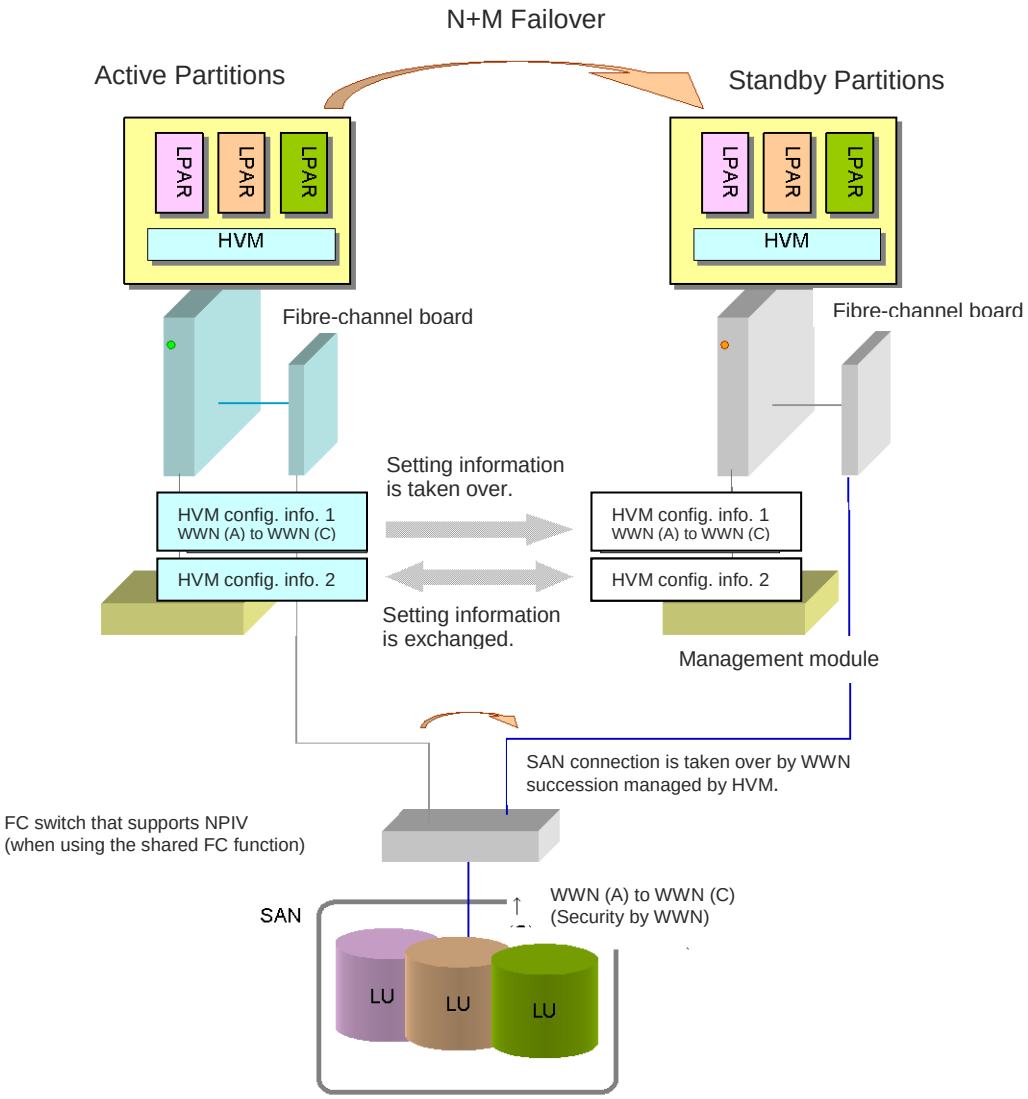


Tip

The same hardware configuration and same firmware version must be installed in the active partition and the standby partition.

(2) Partition in LP mode

In the N+M cold standby, LPAR manager configuration information for the active partition such as LPAR setting, LPAR status, and WWN information, managed by LPAR manager, are copied and taken over to the standby partition, which is booted in the LP mode. This can allow the standby partition to recreate the same LPAR configuration for the active partition even if the server blades are switched. Each LPAR is booted from the same disk (LU) as the active partition to resume the OS environment. Hereinafter, the settings to be taken over are referred to as “partition configuration information” or merely “configuration information”.



Tip

- The trigger to switch to the standby partition is hardware failure of the active partition in the same way as in the Basic mode.
- Use the standby partition with the same hardware configuration and the same firmware version to be installed as the active partition in the same way as in the Basic mode.

NOTICE

- Make sure to apply the same LPAR manager firmware version with the active partition to the standby partition. If you apply different LPAR manager firmware versions to the active and standby partition, N+M failover may fail. If LPAR manager firmware of all server blades cannot be updated at a time in the system with N+M cold standby, discrepancy between LPAR manager firmware versions is allowed as long as the LPAR manager firmware version of the standby server blade is later than that of the active one.
- Select a proper PCI error handling mode for the system configuration. If not, the N+M failover may fail. See PCI error handling mode for details.

❑ Partition configuration information to be taken over by the N+M cold standby

(1) Partition in Basic mode

During N+M failover in the Basic mode, the following information is taken over by the standby partition from the active partition.

Item	Description	Note
WWN	World Wide Node Name	*1
	World Wide Port Name	
MAC address	Media Access Control address	*2
Server blade setting (EFI/BMC)	Whether to use Network Time Protocol (NTP) server or not. Timezone setting , real-time clock (RTC) (basic input/output system (BIOS) time)	*3
	Type of OS (use or not use LPAR manager)	
	Schedule data	
	Remote KVM mouse mode: relative coordinate or absolute coordinate	
	Displayed language setting	
	EFI setting	*4
	Boot order	
HBA BIOS setting for Fibre-channel board	HBA BIOS setting: Enable or Disable	*5
	Boot priority setting: Enable or Disable	
	Boot target WWN	
	Boot target logical unit number (LUN)	
Emulex 10 Gb CNA setting	Preboot eXecution Environment (PXE) Boot Support	*6
	PXE VLAN Support/PXE VLAN ID/PXE VLAN Priority	
	Admin Logical Link (with MultiChannel Support : Enabled)	

Item	Description	Note
	Bandwidth (with MultiChannel Support : Enabled)	
	Logical Port VLAN ID (LPVID) (with MultiChannel Support : Enabled)	
Emulex 10 Gb CNA setting	Internet small computer system interface (iSCSI) setting (with iSCSI for Personality)	
	FCoE setting (with FCoE for Personality)	
PR command setting	Power control cooperation setting	
	N+M cold standby aid function setting	
HA command setting	High availability (HA) monitor system name	
	HA monitor port number	
	HA monitor setting for N+M cold standby aid function	
	HA monitor setting for cluster management	

*1 See WWN in the Compute Blade 2000.

*2 See MAC address in the Compute Blade 2000.

*3 See RTC time synchronization at N+M cold standby failover..

*4 Only items described in the EFI setup menu of the server blade Web console are taken over. See “EFI setting screen” for EFI setup menu of the server blade Web console.

*5 With Emulex 8 Gb 2-port Fibre-channel adapter or Emulex 8 Gb 2-port Fibre-channel mezzanine card, or Emulex 16 Gb 2-port fibre channel adapter, all items in the setup menu are taken over.

*6 You need to configure the same setting for MultiChannel Support and for Personality to the active and standby partitions.
Disable DHCP for iSCSI settings.
Set a unique IP Address for iSCSI Initiator.
Connect to iSCSI Target correctly: Connected.
Up to four iSCSI Traget sessions are available per port.
Do not enter any Default Gateway for iSCSI Initiator: Set as 0. 0. 0. 0.
See product instructions for the 10 Gb converged network for details of each item.



- When the active partition recovers N+M, the information taken over to the standby partition is restored to the active partition. So, the active partition is recovered to the condition before N+M failover. But the standby partition still has the information taken over from the active partition and is not recovered to the condition before N+M failover. Only WWN in standby partition is recovered to the condition before N+M failover.
- When Emulex 10 Gb CNA is used with iSCSI for Personality, information on the IP address, Subnet Mask, and session will be removed from the active partition at N+M failover and from the standby partition at N+M restore.

(2) Partition in LP mode

During N+M failover in the LP mode, information described in Partition in Basic mode and the following LPAR manager information is taken over by the standby partition from the active partition.

Item	Description	Note
LPAR information	LPAR configuration information	
	Logical nonvolatile RAM (NVRAM) information	*1
	Logical schedule data	
Logical partitioning manager (LP) system information	System configuration information	
	PCI device configuration information	
	Virtual network interface card (NIC) configuration information	
	Shared FC information	*2
	Virtual FC WWN seed information	

*1 This includes the boot path, order, boot timer, driver path, and order for the logical EFI. A driver path added manually from the EFI shell cannot be taken over.

*2 See WWN in the Compute Blade 2000.

❑ Time taken for N+M failover

The following describes the time required for N+M failover when a partition fails.

(1) Partition in Basic mode with the standby partition in the pxe method

```
Time taken for N+M failover =
[Time of waiting for a failover start] + [time for Pre-configuration(*1)]
+ [time taken for OS boot]
```

(2) Partition in Basic mode with the standby partition in the inline method

```
Time taken for N+M failover =
[Time of waiting for a failover start] + [time taken for OS boot]
```

(3) Partition in LP mode with a pre-method standby partition

```
Time taken for N+M failover =
[Time of waiting for a failover start] + [time for Pre-configuration(*1)]
+ [time for HVM boot] + [time taken for booting OS on the LPAR]
```

(4) Partition in LP mode with an Inline-method standby partition

```
Time taken for N+M failover =
[Time of waiting for a failover start] + [time for HVM boot] + [time taken
for booting OS on the LPAR]
```

The following shows the time taken for booting LPAR manager.

Partition	Time taken (minutes)
Server blade	5 to 10 (*)

*1 See Time required for Smart Configure for the time taken for executing Smart Configure.



In N+M cold standby using HCSM, HCSM monitors if the OS on the standby server blade starts up within the maximum allotted time for “Host OS Startup” specified by the user after switching server blades.

If the standby OS startup is not completed within the maximum allotted time for “Host OS Startup” specified by the user, an error message displays that N+M failover failed. (KASV00212-E) is shown on the HCSM task result window regardless of whether the standby OS has started. Thus, even if N+M cold standby failover is successful and the standby OS has started, the error message (KASV00212-E) may be displayed on the HCSM task result window.

Standby OS startup completion takes longer on some types of server blade configuration such as CB 540A blade. Set an appropriate time for the maximum allotted time for “Host OS Startup”.

Prerequisites for the N+M cold standby

The followings are prerequisites for the N+M cold standby.

- Supports SAN boot
- The standby partition has the same hardware composition as the active partition.
  - The type and the number of CPU
  - Memory capacity installed
  - Expansion card; I/O board module: type and locations of corresponding slots
  - I/O slot expansion unit; I/O adapter for the I/O slot expansion unit: type and locations of corresponding slots viewed from a partition
- There are the following restrictions when N+M cold standby is configured with standard server blade (X55A1/X55A2).
  - An internal HDD (SAS) is not installed in the Xeon server blade. If an internal HDD (SAS) is installed in the Xeon server blade, disable the internal HDD in the BIOS setting.
  - It cannot be composed of the combination of X55A1 model and X55A2 model.
  - It cannot be composed of the combination of EFI firmware 01-XX/02-XX and EFI firmware 03-XX/04-XX or later.
- When N+M cold standby is configured in the LP mode, the server blade and its peripherals must support LPAR manager.
- A standby partition can be replaced with the active partition that has a different type and number of CPU and memory capacity from the standby partition. However, confirm that requirements for operating OS and application are satisfied and both of them can operate on the standby partition by executing the switching test in advance.
- When N+M cold standby is configured with Emulex 8 Gb 2-port Fibre-channel adapter or Emulex 8 Gb 2-port Fibre-channel mezzanine card, or Emulex 16 Gb 2-port fibre channel adapter, data on all items in HBA BIOS setup menu is mirrored. This requires that the SAN configuration between the active partition and LU should be the same as that between the standby partition and LU.
  - The number of cascaded stages of FC switches
  - The port speed setting on FC switches
  - Speed and topology settings on disk devices



Smart Configure methods can be different between the active and standby partitions. The required time for switching methods of Smart Configure depends on that of the standby partition.

- When configuring N+M cold standby with Emulex 10 Gb CNA, make sure to configure the following settings for the Emulex 10 Gb CAN on active and standby partitions.
  - Set the same Multi Channel Support setting to the active and standby partitions.
  - Set the same Personality setting to the active and standby partitions.
  - Set a unique iSCSI Initiator IP Address.
  - Set Connected as Connection Status for iSCSI Target.
  - The number of sessions for iSCSI Target is up to four sessions per port.
  - iSCSI interface and FCoE interface cannot be mixed on the same partition.

  See the *10Gb Converged Network Production Instruction Manual* for details about Emulex 10 Gb CNA.



- If the prerequisite conditions described above are not satisfied when Emulex 10 Gb CNA is installed on the active and standby partitions, N+M cold standby does not work properly.
- To take over settings Emulex 10 Gb CNA with N+M cold standby, the following conditions need to be satisfied.

Item	Condition
Server blade	Standard server blade: X55S3 BMC firmware: 05-17 or later, or 07-01 or later EFI firmware: 09-40/10-40 or later High-performance server blade: X57A2 BMC firmware: 04-68 or later EFI firmware: 07-40/08-40 or later
Management module firmware	A0330 or later

- To take over settings Emulex 10 Gb CNA (iSCSI for Personality) with N+M cold standby, the following conditions need to be satisfied.

Item	Condition
Server blade	Standard server blade: X55S3 BMC firmware: 05-50 or later, or 07-01 or later EFI firmware: 09-43/10-43 or later High-performance server balde: X57A2 BMC firmware: 04-71 or later EFI firmware: 07-43/08-43 or later
Management module firmware	A0345 or later

- To avoid misconnection with iSCSI for Personality, set the following values to iSCSI on the standby partition.

Item	Setting value
iSCSI Initiator IP Address	0.0.0.0
iSCSI Initiator Subnetmask	0.0.0.0

- To take over NIC settings for Emulex 10 Gb CNA/LAN mezzanine card or for onboard CNA board with N+M cold standby, use the configurations of firmware and driver versions shown in the following table.

CNA firmware on Active server blade	CNA firmware on Standby server blade	LAN driver	
		Windows	Linux
4.1.334.2801	4.1.334.2801	4.1.334.25	4.1.334.18
4.2.433.604	4.1.334.2801	4.1.334.25	4.1.334.18
4.1.334.2801	4.2.433.604	4.1.334.25	4.1.334.18
4.2.433.604	4.2.433.604	4.2.390.6	4.2.456.0

Configuration with LAN driver 4.2.390.6 or 4.2.456.0 and CNA firmware 4.1.334.2801 is not supported.

- To take over settings Emulex 10 Gb CNA (FCoE for Personality) with N+M cold standby, the following conditions need to be satisfied.

Item	Condition
Server blade	Standard server blade: X55S3 BMC firmware: 05-54 or later, or 07-01 or later EFI firmware: 09-56/10-56 or later High-performance server balde: X57A2 BMC firmware: 04-75 or later EFI firmware: 07-54/08-54 or later
Management module firmware	A0360 or later

- To take over settings for Emulex 16 Gb 2-port fibre channel adapter, Hitachi 16 Gb 1-port fibre channel adapter, or Hitachi 16 Gb 2-port fibre channel adapter, the following conditions need to be satisfied.

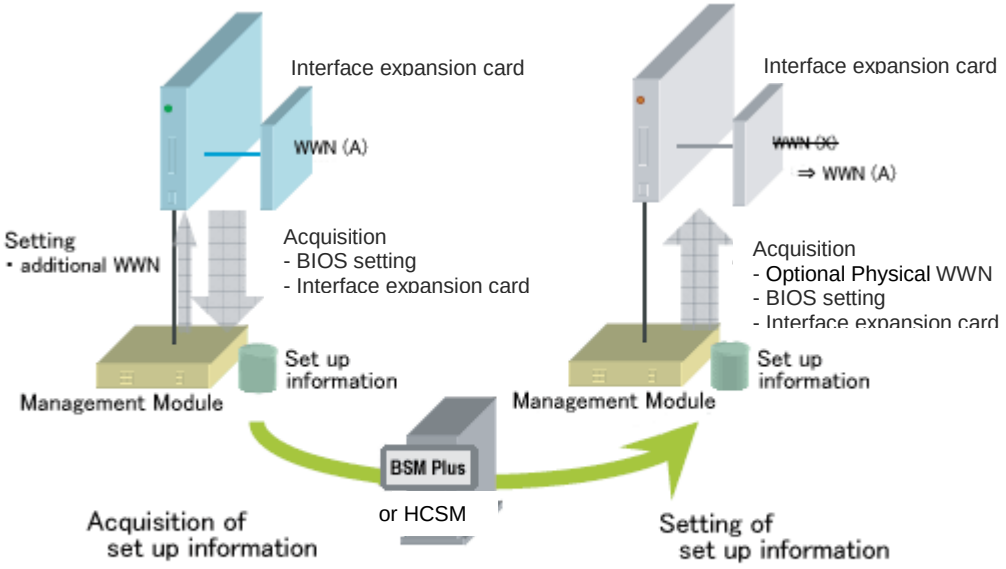
Item	Condition
Server blade	High-performance server balde: X57A2 BMC firmware: 08-08 or later EFI firmware: 07-65/08-65 or later
Management module firmware	A0375 or later

Smart Configure in N+M cold standby

In the N+M cold standby, configuration information on active partitions is acquired in advance and stored in the management module.

During N+M failover, the configuration information stored in the management module is set to the standby partition to be restarted. With the pxe method, Smart Configure is performed during the above acquisition and setting, while with the inline method, Smart Configure is not performed because the setting information is set to the standby partition during the power on.

Configuration information on the active partitions must be acquired by the Smart Configure, when the N+M cold standby is implemented. That is not when N+M failover occurs.
This is because failing partitions may not be able to perform Smart Configure.



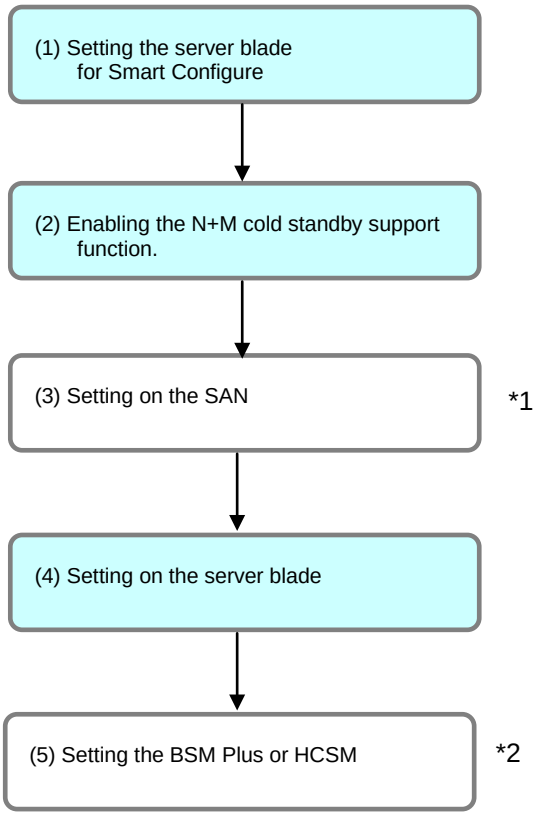
Smart Configure (Acquisition and setting of setup information)

Procedure for Implementing the N+M Cold Standby

You have to implement the N+M cold standby for each of Compute Blade, SAN and BSM Plus or HCSM.
For details about how to configure the SAN and the BSM Plus or HCSM, see the appropriate instruction manual.

❑ Overview of N+M Cold Standby Procedure for Compute Blade

The following outlines the implementing flow on the N+M cold standby.
Each step is described in the subsequent sections.



*1 Setting the SAN: See the manual for the product.

*2 Setting the BSM Plus or HCSM: See the manual or help for the BSM Plus or HCSM. Make sure to test the switching after setting the N+M cold standby.

(1) Setup for pre-configuring a server blade

To configure N+M cold standby, you must first complete the following server blade setup:

- Disable the internal hard disk: serial attached SCSI (SAS)

  The internal hard disk cannot be used in N+M cold standby. If an internal hard disk is installed, disable it in the BIOS setting. The internal hard disk cannot be disabled from BMC's server blade Web console. It can only be disabled using the EFI's BIOS Setup utility.

> ***NOTICE***
>
> Do not move the EFI Shell to the highest booting priority in the EFI Setup menu. If the EFI Shell is on the top of the boot option, the OS will not successfully boot after N+M switching and failback.

(2) Enabling the N+M cold standby support function

Enable the N+M cold standby support function on both the active and standby partitions, using the "PR Command". When this command is executed, the partitions on which the N+M cold standby support function is enabled are immediately Smart Configured. This Smart Configure allows an Optional Physical WWN to be assigned to the Fibre-channel board, 10 Gb CNA adapter, or 10 Gb CNA board.



- Smart Configure is performed immediately on the partitions on which the N+M cold standby support function is enabled. This results in an Optional Physical WWN being assigned to the Fibre-channel boards. The Smart Configure execution time is shown in "Time Required for - Smart Configure Execution".
- The procedures in (1) and (2) above are mandatory even for an N+M cold standby system built in LP mode.

(3) Setting the SAN and FC switches

- Partitions in Basic mode
  - For connection via fibre channel, set the WWNs and other settings on the SAN. Use Optional Physical WWNs.
  - For connection via FCoE, set the WWNs and other settings on the SAN or FCoE switch. Use Optional Physical WWNs.
  - Verify the Optional Physical WWNs using the "WWN Command".
  - For connection via iSCSI, set iSCSI settings including iSCSI Traget on the SAN
- Partitions in LP mode
  - Set the WWNs and other settings in the SAN. Use virtual FC WWNs.
  - Verify the virtual FC WWNs from LPAR manager's "Allocated FC Information" screen.

(This setting applies to FC switches, SAN, and LUN Manager. For details, see the documentation for the product concerned.)

(4) Server blade setup

- Partitions in Basic mode

  Set up the server blade so that the active partition can be booted from the SAN.

  - Fibre-channel board setting
    - Enable the BIOS for the Fibre-channel board, and enable the boot priorities.
    - Select the LU to be booted.
    - For details about the procedure, see your Fibre-channel board documentation.
  - CNA (iSCSI) setting
    - Set iSCSI settings including iSCSI Traget.
    - For further details, see the *10Gb Converged Network Production Instruction Manual*.
  - CNA (FCoE) setting
    - Set FCoE settings including enabling Boot Bios.
    - For further details, see the *10Gb Converged Network Production Instruction Manual*.
  - EFI setup (Xeon Server Blade)
    - Set the booting priority and enable the active partition to be booted from the SAN.
    - For details about the procedure, see "Standard Server Blade Setup Menu (X55A1/X55A2 Models)" in Chapter 5".

> ***NOTICE***
>
> With a standard server blade, executing the Smart Configure changes the SAN boot priority to the lowest automatically.

- Partitions in LP mode

  Set up the server blade so that the LPAR configured in LPAR manager on the active partition can be booted from the SAN.

  - EFI setup (Xeon Server Blade)
    - Confirm that the EFI settings are required for LPAR manager boot.
    - For details about EFI setup, see "Chapter 12: Logical partitioning manager".
  - Auto Activate or Pre-State Auto Activate setting

- To enable the LPAR to be activated automatically after N+M switching, set Auto Activate to the LPAR or Pre-State Auto Activation to "Yes" on the LPAR manager screen.
- For details about the procedure, see “Set Auto Activate to LPAR” or "Options" in Chapter 12.

◆ LPAR configuration

- Assign the necessary processors, memory, dedicated PCI devices, and shared devices (virtual NIC (VNIC), shared FC) to the LPAR.
- Activate the LPAR.
- For details, see "Chapter 12: Logical partitioning manager" in Chapter 12.

◆ Device setting for the Fibre-channel board (dedicated or shared)

- From the LPAR's EFI menus, select the EFI Shell. Then, from the Shell prompt, execute the drvcfg command to call the device setup shell (hfccfg).
- Enable the boot function of the HBA FC port to which the boot target LU is connected.
- For details about the procedure, see the Fibre-channel board documentation.

◆ Boot settings

- From the LPAR's EFI menu, select "Boot option maintenance menu". Enable the LPAR to be booted from the SAN by setting the boot path and boot order.
- For details about the procedure, see "Boot the Guest OS" in: Logical partitioning manager, Chapter 12.

NOTICE

If you change the LPAR configuration (processors, memory, or device assignment), make sure to implement [F9]: "Save Configuration" on the HVM Menu screen. For details, see "Saving Settings on the HVM Screen".

(5) N+M cold standby setup in BSM Plus or HCSM

Set up the N+M cold standby configuration in the BSM Plus or HCSM, such as setting a partition active or standby. This is the setting in the BSM Plus or HCSM. See the BSM Plus or HCSM manual for the details. Before setting up N+M cold standby in the BSM Plus or HCSM, check the following:

■ Make sure the N+M cold standby support function is enabled.

◆ The N+M cold standby support function must be enabled on both the active and standby partitions.

◆ To check that the N+M cold standby support function is enabled on the partitions, use the PR Command.

- If using Basic mode, make sure that the active partition can boot from the SAN.
- If using LP mode, make sure that the LPAR configured in LPAR manager on the active partition can boot from the SAN. (LP mode is supported by BSM Plus.)

After completing these checks, use the BSM Plus or HCSM to set up the N+M cold standby configuration.

(6) N+M switching test run

Before starting operation, conduct an N+M switching test run to confirm that switching is performed successfully by one of the following:

- Performing a manual failover from the BSM Plus
- Operating the test N+M cold standby using HCSM
- Issuing a switching test alert using the BSM Command or HCSM Command

NOTICE

When a switching alert is issued by the BSM command execution, the active partition is forcibly powered off.



For details about the N+M cold standby configuration and N+M switching procedure, see your BSM Plus or HCSM documentation.

Setting change after configuring the N+M cold standby

(1) Partitions in Basic mode

When you change the EFI settings using the BMC' server blade Web console after configuring the N+M cold standby, the new EFI settings take effect the next time the EFI starts. If N+M switching occurs before the new settings are applied, the system will switch over according to the EFI settings from the previous EFI start.

(2) Partitions in LP mode

If you change the LPAR configuration (processors, memory, or device assignment) after configuring the N+M cold standby, make sure that you press F9: Save Configuration on the LPAR manager Menu screen. If not, the LPAR manager configuration information in the management module differs from the actual LPAR manager settings and N+M switching may fail.

Changing CNA after configuring the N+M cold standby

If restoring iSCSI is required after CNA is changed in the configuration where CNA is used with iSCSI for Personality, you need to configure the following settings depending on the N+M cold standby.

Status	Setting value
Active server blade not yet switched by failover	Restore the iSCSI setting of the active server blade before changing CNA.
Standby server blade not yet switched by failover.	Restore the iSCSI setting of the standby server blade before changing CNA if iSCSI is disconnected.
Active server blade switched by failover	Set the iSCSI setting of the standby server blade before changing CNA if iSCSI is disconnected.
Standby server blade switched by failover	Set the iSCSI setting of the active server blade before changing CNA.

UPS connection for the N+M cold standby

When using the UPS, you have to configure automatic partition power on to restore the N+M cold standby automatically after the recovery of the system power source.

- Set the partition to automatically power on after the power supply recovery.
  - Set “Power on” in the “AC recovery” using the “PR command” in Chapter 6. This setting allows partitions to power on after the power supply recovery.
- Then, inhibit the automatic partition power on for standby partition.
  - Set "Stay off" in the “AC recovery” for the standby partition using the “PR command”. This setting inhibits partitions from automatically powering on at the power supply recovery. Smart Configure, however, performs regardless of this setting.



- The above steps are unnecessary if you do not automatically start the partition after the recovery of system power source even though using the uninterruptible power supply (UPS).
- When the N+M cold standby support function is enabled with the PR command, the partition may not automatically boot at the power supply recovery, if the partition “AC recovery” is not set to “Power on” even if the auto power on for the server at the power supply recovery is enabled.
- To automatically turn on the server after the power supply recovery, make sure to set “Power on” in the “AC recovery” using the PR command.

RTC time synchronization at N+M cold standby failover

N+M cold standby has a function to take over RTC (Real Time Clock: BIOS time) to the standby partition. Enabling this function allows the following OSs to co-exist in the N+M group.

- OS, except LPAR manager, which recognizes RTC as the local time
- OS that recognizes RTC as UTC (Universal Coordinate Time)

Note

If this function is disabled, time difference may occur at N+M failover. Thus, the configuration of mixed OSs in the same N+M group is not supported. See Time Setting in Switchover and Recovery with N+M Cold Standby in Chapter 12 for details.

❑ Procedure for enabling RTC time synchronization

This subsection describes how to enable RTC time synchronization.

1. On the Time Setting screen of the management module, set the Time Synchronization for Network Time Protocol (NTP) setting as Enable. See SD Command or Time Setting in Chapter 6.
2. For the Time Synchronization Method on the BMC Time screen, select “Use the NTP server of the Management Modules with RTC time handover on N+M cold standby failover”. See BMC Time in Chapter 5,

Note

When enabling this function, make sure to check the time of the management module and BMC before operation. When N+M cold standby occurs with the incorrect time, the correct RTC time is not taken over to the standby partition. If the incorrect time is set, reset the time of the management module and BMC. Time synchronization, however, takes up to 15 minutes depending on your configuration.

❑ Standby partition behavior in RTC time synchronization failure

If RTC time is not properly taken over to the standby partition due to hardware failure when the function is enabled, you can select a standby partition behavior. See BMC Time in Chapter 5 for BMC time settings,

- Continue boot (default)

  RTC time on the active partition is not taken over to a standby partition. The standby partition boots up with its own RTC.

- Suppressing boot

  TRC time on the active partition is not taken over to a standby partition, and the power to the standby partition is suppressed. Then, the standby partition is not

booted after N+M failover. See “UTL Command” in Chapter 6 for releasing the power-on request suppress setting.



- This function is supported only by the standard server blade X55R4 model.
- Do not enable daylight saving time (DST) adjustment. If DST is enabled, the OS time may have one-hour difference depending on the time when the N+M cold standby failover occurs. When enabling DST, execute the following
  - When N+M failover occurs at the day of starting or finishing DST, adjust the difference on the OS, using NTP or manually.
  - Reboot the OS after DST has started or finished. This can update the system information required for RTC time synchronization to avoid time difference due to DST adjustment.
  - This function is available only for Basic mode partitions. LP mode partitions are not supported.

Digital certificates for the system web console

Overview of digital certificates for the system web console

❑ Functions

You can use the following functions using a digital certificate for the system Web console.

(1) Authenticating a management module

When you use the system Web Console, a management module displays a digital certificate. You can verify the management module by checking the certificate authority (CA) that has signed on the digital certificate.

(2) Encrypting a communication path

You can encrypt a communication path when using the system Web console, which prevents the communication path from tapping and tampering.

❑ Prerequisites

The followings are prerequisites to use digital certificates for the system web console.

To authenticate a management module, a root certificate issued by a certificate authority (CA) and a digital certificate signed by the CA. The digital certificate signed by a CA is shown as (1) and (2) below:

(1) Certificate signed by an external CA

(2) Certificate signed by your own CA

❑ Digital certificate specifications

The following table shows digital certificate specifications for the system web console.

No.	Item	Description
1	Public key algorithm, bit-length	Can select from RSA: the first-described public-key cryptosystem (1024 bits), RSA (2048 bits), DSA (1024 bits).
2	Importable certificate format	Can select from privacy enhanced mail (PEM) and Distinguished Encoding Rules (DER). PEM and DER.
3	Certificate format in downloading	Can select from PEM and DER.
4	Executable certificate signing request (CSR) format	Can select from PEM and DER.
5	Maximum number of	Common name (CN): Up to 60 characters (*1, *2)

No.	Item	Description
	characters used for a certificate and CSR	Country (C): Up to 2 characters (*3)
		State or Province (ST): Up to 60 characters (*4)
		Locality (L): Up to 60 characters (*4)
		Organization name: Up to 60 characters (*4)
		Organization Unit (OU): Up to 60 characters (*4)
		Mail address: Up to 60 characters (*5)
		Distinguished name (DN) qualifier: Up to 60 characters (*4)
		Surname: Up to 60 characters (*4)
		Given name: Up to 60 characters (*4)
		Initials: Up to 30 characters (*4)
		Unstructured name: Up to 60 characters (*4, *6)
		Challenge password: Up to 30 characters (*4, *6)

*1 Make sure to fill in this item.

*2 Alphabetical capital and small letters, Arabic numerals, hyphones (-), and periods (.) can be used for this item.

*3 Alphabetical capital letters can be used.

*4 Alphabetical capital and small letters, Arabic numerals, hyphones (-), periods (.), pluses (+), single quotations (‘), commas (,), left parentheses ((), right parentheses ()), slashes (/), colons (:), equals (=), question marks (?), and spaces can be used for this item.

*5 Printable American Standard Code for Information Interchange (ASCII) characters can be used.

*6 This can be filled in when CSR is created.

Procedures to use digital certificates for the system web console

❑ Procedures

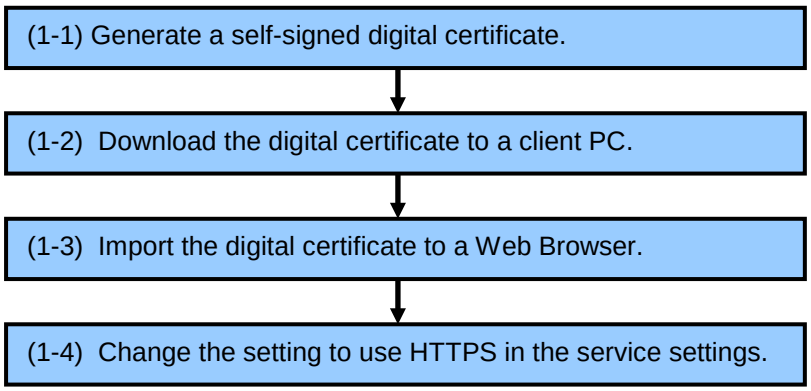
To use a digital certificate with the system web console, the following two ways are available.

(1) Creating a self-signed digital certificate: you can encrypt a communication path.

(2) Importing a digital certificate signed by a certificate authority: you can authenticate a management module and encrypt a communication path.

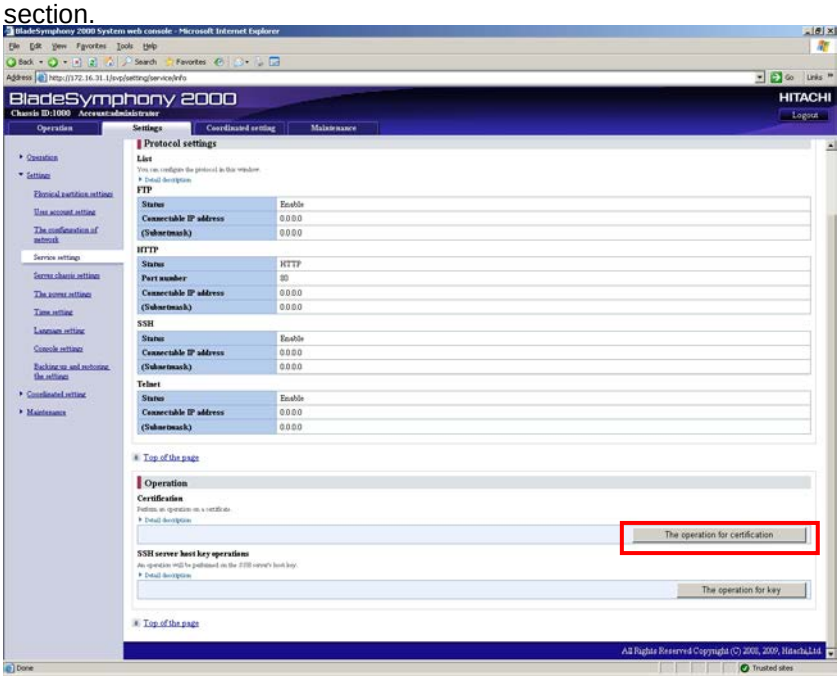
❑ Creating a self-signed digital certificate

The following chart shows the flow for creating a self-signed digital certificate to using the digital certificate.

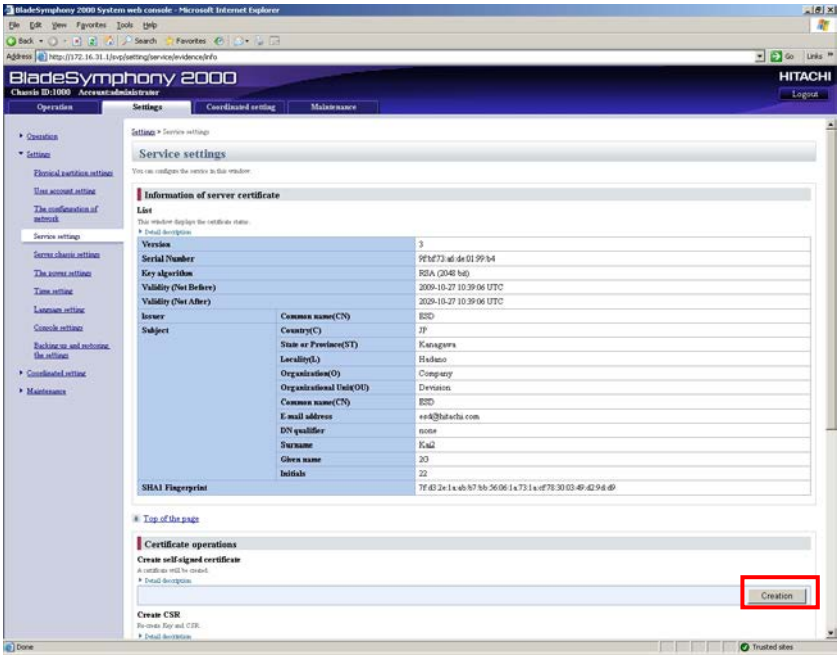


(1-1) Create a self-signed server certificate

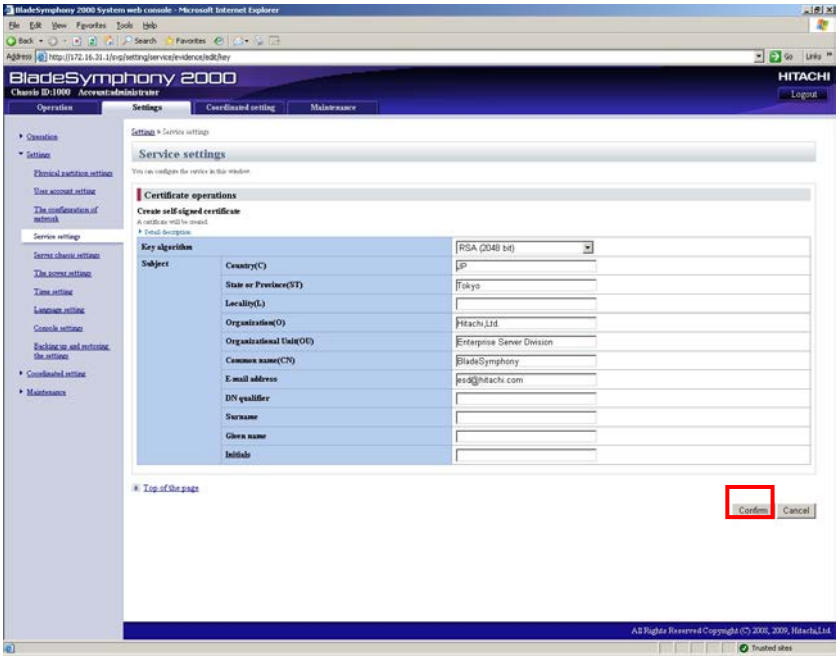
1. Press the **The operation for certification** in the **Service Settings** screen of the system web console to display the Information of server certificate section.



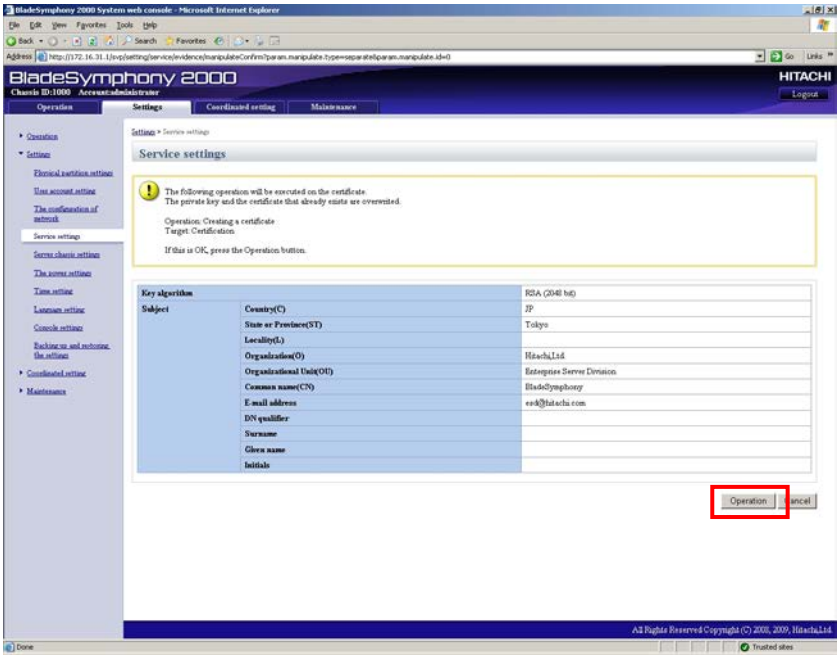
2. Press **Creation** to display the Certificate operations screen.



3. Fill in the fields of **Key algorithm** and **Subject** and press **Confirm**.

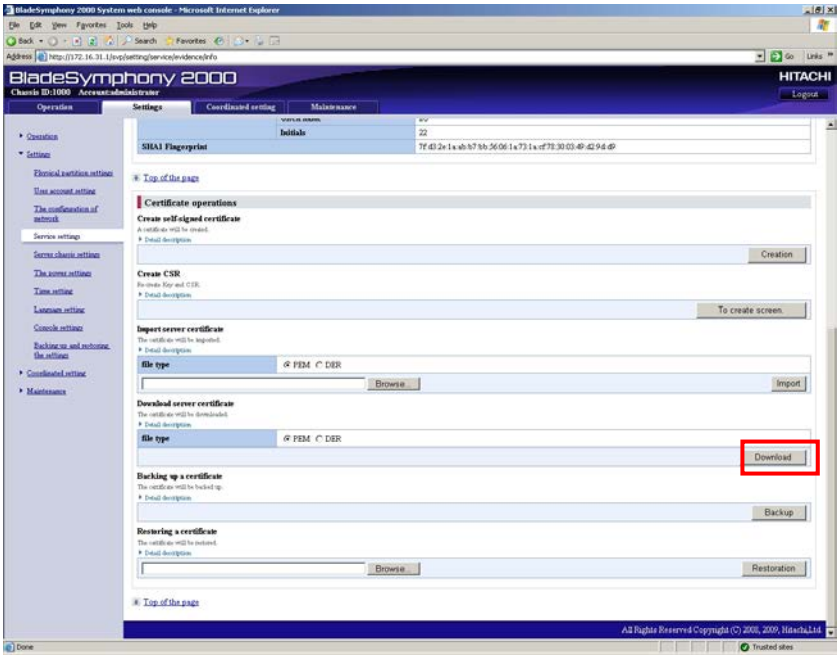


4. Confirm that the values are correct on the following screen, and press **Operation** to generate the server certificate.



(1-2) Download the digital certificate to a client PC

1. Press **The operation for certification** in the **Service settings** screen of the system web console to display the Certificate operations section.
2. Press **Download** to download the digital server certificate generated in step (1-1) to your client PC.

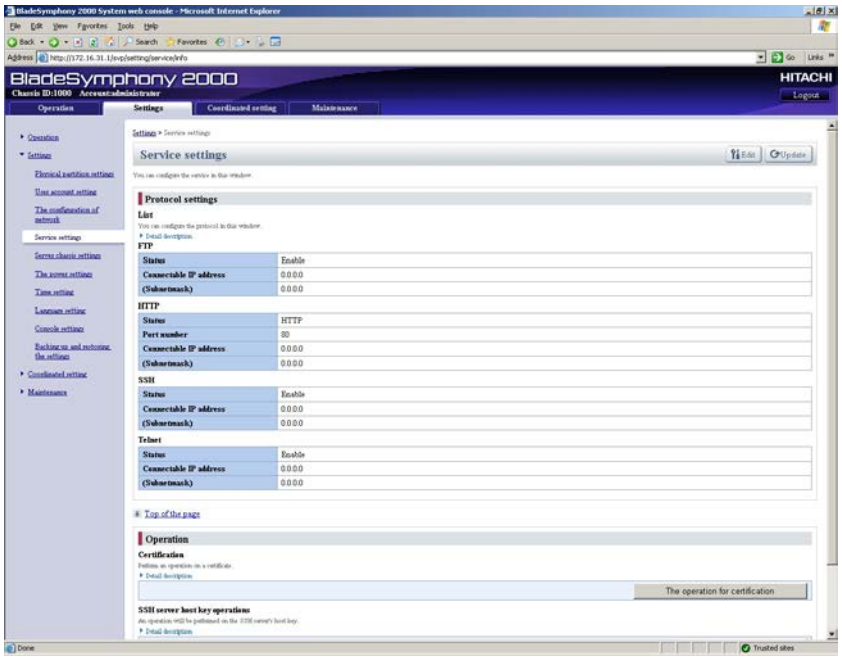


(1-3) Import the digital certificate to a web browser

Import the digital certificate downloaded in step (1-2) to a web browser of your client. For information about how to import it to the web browser, refer to the web browser “Help”.

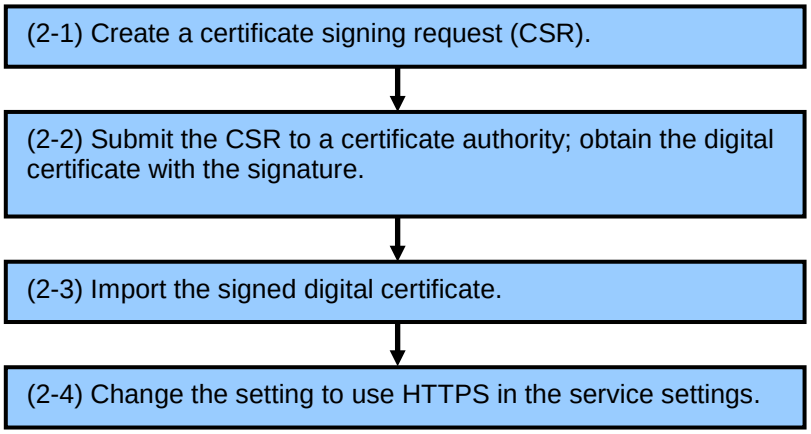
(1-4) Change the service setting for Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Press **Edit** on the **Server settings** screen to change the protocol settings to HTTPS. Encryption of communication paths will be enabled from the next connection.



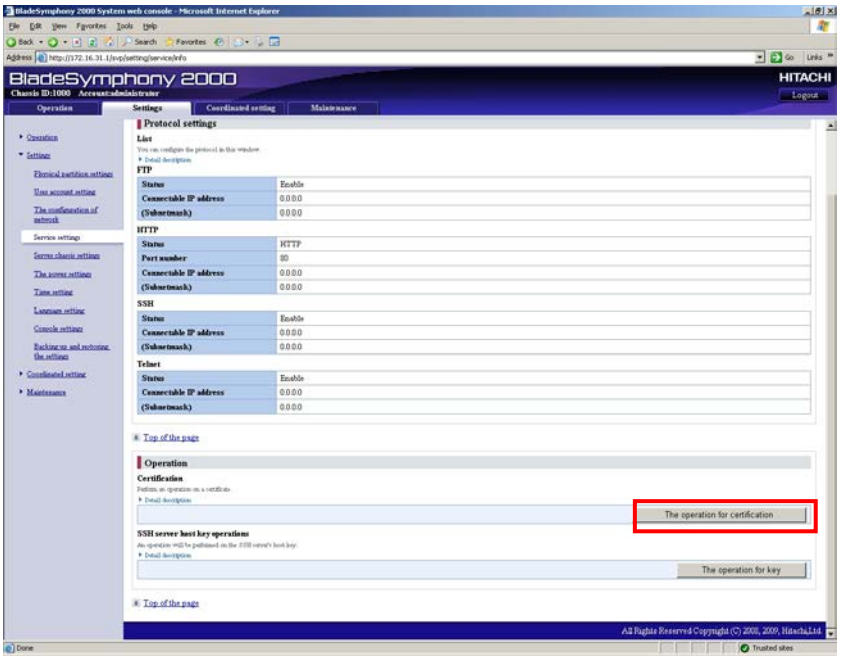
❑ Importing a digital certificate signed by a certificate authority

The following flow chart shows the steps from importing a digital certificate with a certificate authority to using the digital certificate.

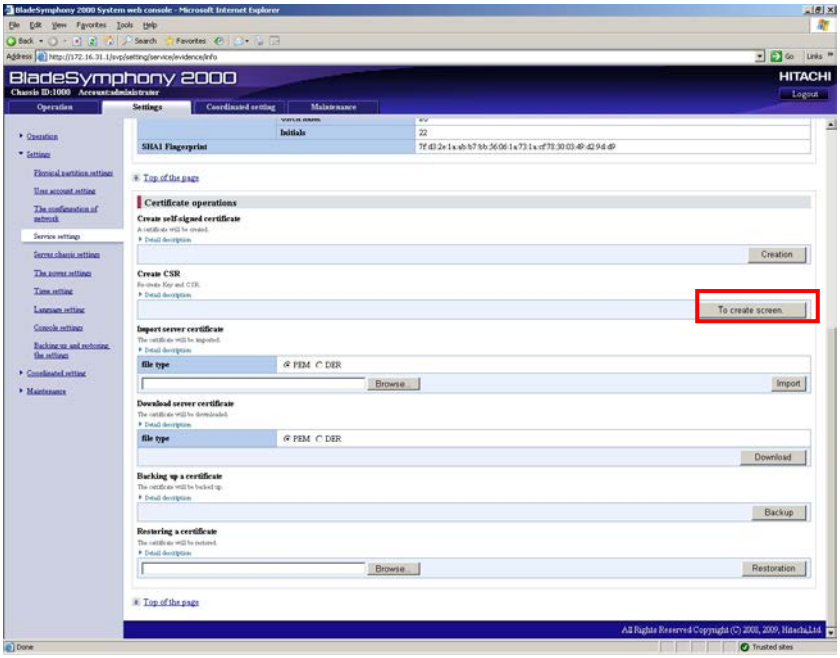


(2-1) Create a certificate signing request (CSR)

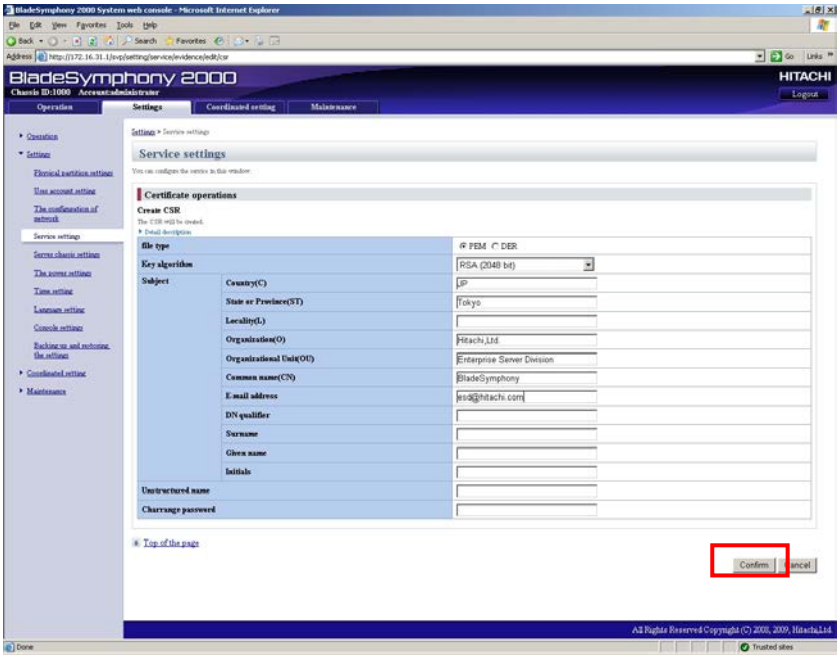
1. Press the **The operation for certification** in the **Service Settings** screen of the system web console to display the information of server certificate section.



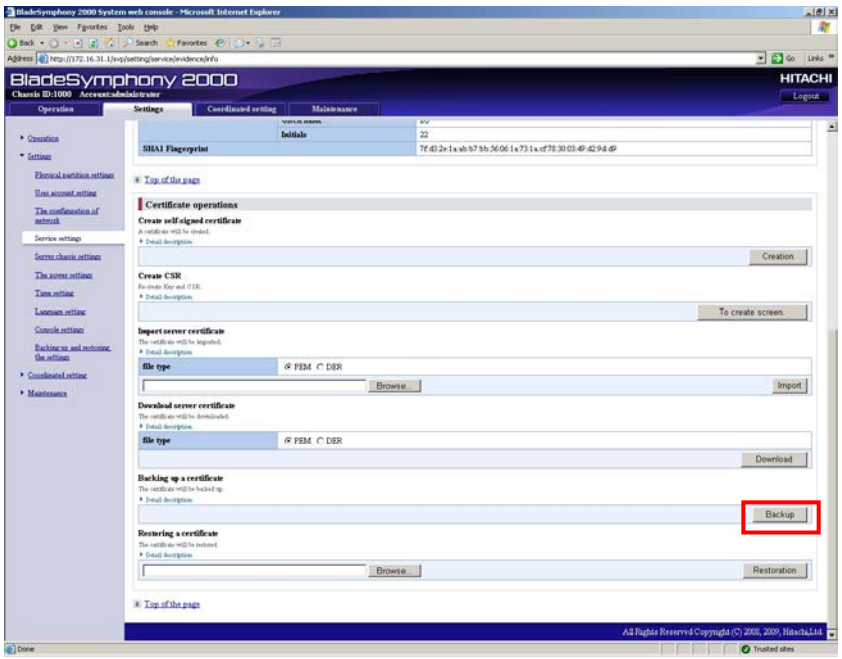
2. Press **To create screen** to go to the screen including the Certificate operations section.



3. Fill in the fields of **Key algorithm** and **Subject** and press **Confirm**. Confirm that the values are correct on the next screen and press **Operation** to create the CSR.



A private key corresponding to the CSR is created simultaneously in the management module. The same key as this one, however, can never be created.It is recommended that you press **Backup** in the Certificate operations section to obtain the backup after creating a CSR.

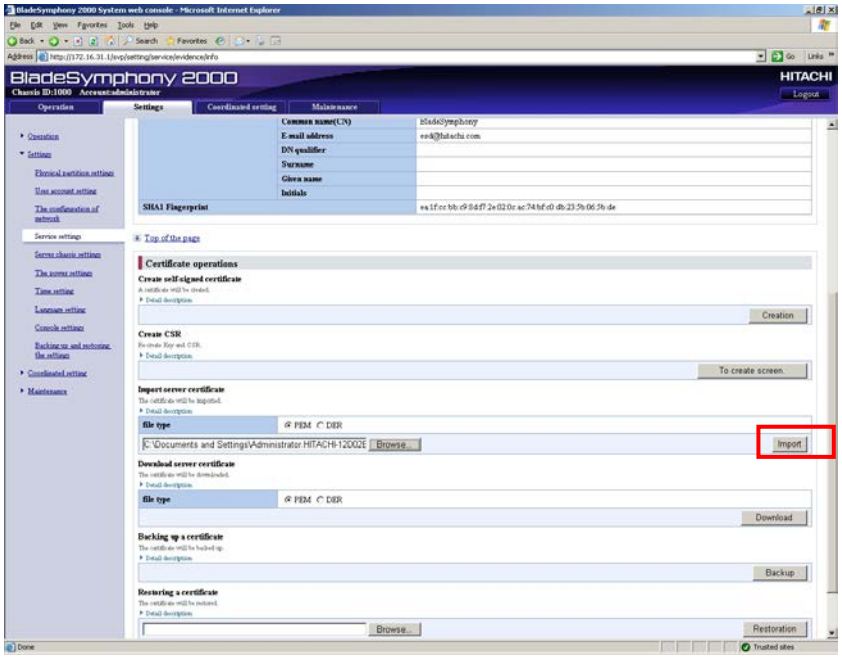


(2-2) Submit the CSR to certificate authority (CA) and obtain the signed digital server certificate

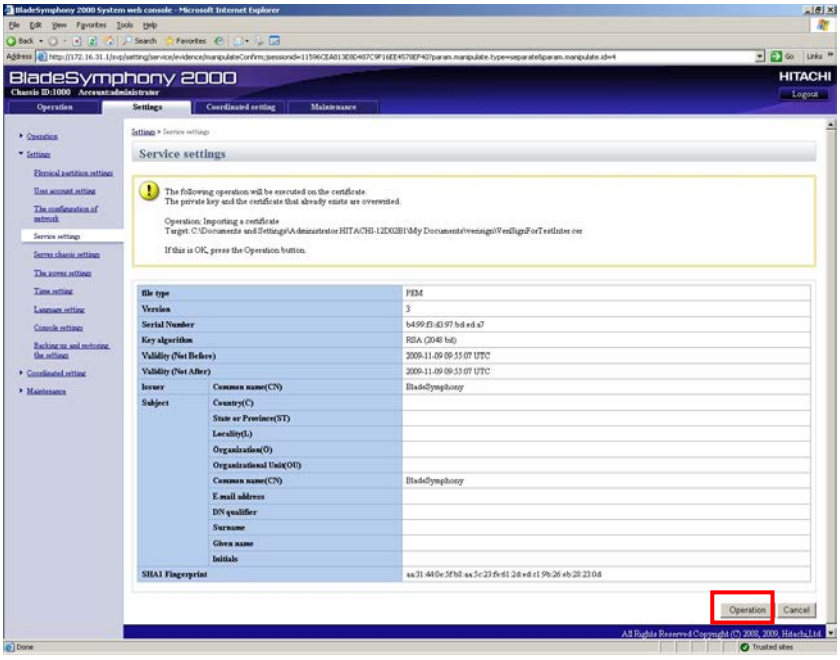
Submit the created CSR to a certificate authority to obtain the signed digital certificate.

(2-3) Import the signed digital server certificate

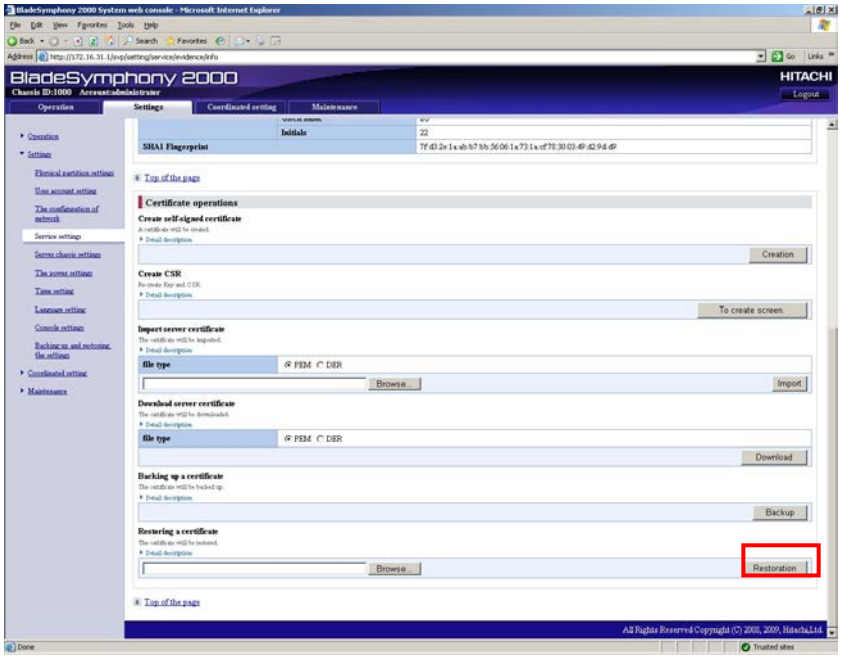
1. Press **The operation for certification** in the **Service Settings** screen of the system Web console to go to the Certificate operations section. Then press **Import** to display the screen for importing.



2. Confirm that the certificate information displayed is the same as the certificate information you have obtained, and press **Operation** to import the server certificate.



3. If you fail to import it, use the backup file obtained in step (2-1): press **Restoration** on the Certificate operations section to restore the certificate. Then import the certificate once more.

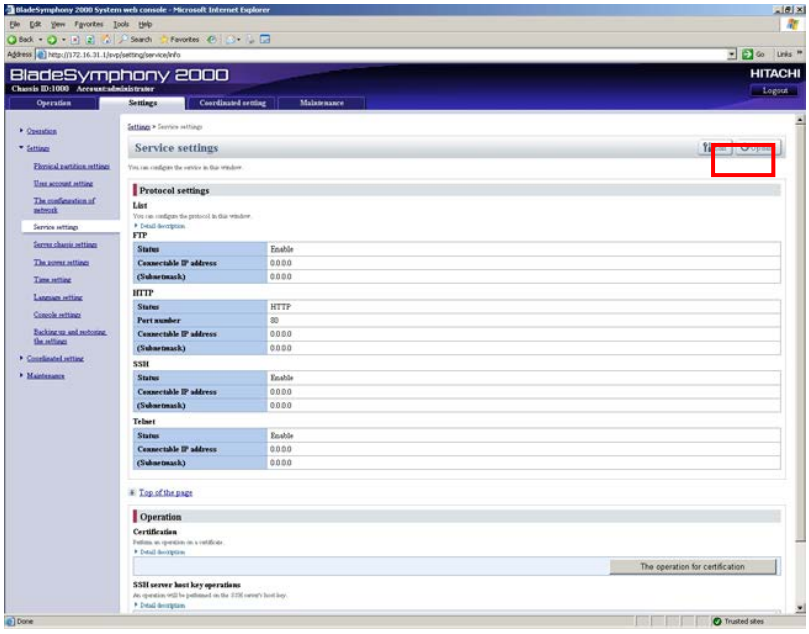


(2-4) Change the service setting for HTTPS

Press **The operation for certification** in the **Service Settings** screen of the system Web console to go to the Information of server certificate screen.

Then press **Edit**, on the upper right of the screen, to change the protocol settings to HTTPS. Encryption of the communication path will be enabled from the next connection.

To enable the management module authentication, the root certificate of CA must have been imported to the Web browser of your client PC. For information about how to check it, access the web browser “Help” or ask the CA.



E-mail notification

E-mail notification overview

❑ E-mail notification

You can perform the following with the e-mailing notification function.

(1) Triggered by failure events

If the equipment has incurred an error, this function collects and e-mails log information necessary for the error analysis.

A record of failure reporting logs is saved in the management module. Up to 32 reports can be saved. Excess reports or logs are deleted chronologically.

To find the report records, select **e-mail remote report -> Operation -> e-mail report (Management LAN)** on the system Web console.

(2) Triggered by log output

With this function, you can send logs attached to e-mail when the log is output from a server blade. This e-mail reports information supplementary to the notification triggered by failure events.



The e-mail notification is executed when logs are output from a server blade by manual operation.

In this case, there is no e-mail notification triggered by failure events before this e-mail.

(3) Triggered by manual operation: the current status

With this function, you can collect information on the current status of the equipment and send it attached to e-mail.

To find the current notification, select **e-mail remote report -> Operation -> e-mail by manual operation (Management LAN)** on the system Web console.

(4) Triggered by manual operation: the selected history

With this function, you can select any history from the failure notification history and resend it.

If Compute Blade fails and the failure notification cannot be sent due to a mail server halt, you can resend the e-mail after the mail server recovery.

To send a specific failure notification, select **e-mail notification > Operation > E-mail notification resend (management LAN)** on the system Web console, and execute it.

❑ Prerequisites

The following are prerequisites for using the e-mailing function.

(1) The e-mailing function is such that the management module as the mail client e-mails the mail server: Simple Mail Transfer Protocol (SMTP). This requires a separate SMTP server.

(2) The management module must be in an environment in which it can communicate with the mail server.

❑ Specifications for e-mail notification

The following list describes specifications for e-mailing function.

NO.	Item		Description
1	Mailing means		E-mail (based on the SMTP)
2	Maximum number of concurrent destinations		4
3	Number of SMTP servers that can be connected		1 (Only the management LAN terminal of the management module.)
4	Trigger for notification		An error occurs.
			A server blade outputs a log.
			By manual operation (Enter the command from the management module or system Web console.)
5	Retry Notification		Retries the e-mail notification If notification triggered by failure or by log output fails.
6	Notification		
	Triggered by failure	Subject	AUTO: Failure report.
		Body	Mail description: “The trouble occurred by the following device.” Information on the server chassis Brief information on the failure
		Attachment *1	svpsts-YYYYMMDD-hhmmss.gz trc-YYYYMMDD-hhmmss.tar.gz (*2) marlog.gz
	Triggered by log output *3	Subject	AUTO: Log dump report.
		Body	Mail description: “The log of the server blade was output with the following device.” Information on the server chassis
		Attachment *1	One of the following files: hvmdumpN-YYYYMMDD-hhmmss.tar.gz uagentN-YYYYMMDD-hhmmss.tar.gz raslogN-YYYYMMDD-hhmmss.tar.gz
	Triggered by manual operation (Current status)	Subject	MANUAL: Current status report.
		Body	Mail description: “This e-mail was sent by manual operation. The log attached to this email shows a current machine state.” Information on the server chassis
		Attachment *1	svpsts-YYYYMMDD-hhmmss.gz trc-YYYYMMDD-hhmmss.tar.gz (*2)

NO.	Item			Description
		Triggered by manual operation (Selected history)	Subject	MANUAL: History report.
			Body	Mail description: “Failure occurred in the following device.” Information on the server chassis Brief information on the failure
			Attachment *1	svpsts-YYYYMMDD-hhmmss.gz trc-YYYYMMDD-hhmmss.tar.gz (*2) marlog.gz
7	SMTP authentication method			Can select from No authentication, PLAIN, LOGIN, or CRAM-MD5.
8	Encryption			Can select from Secure Socket Layer (SSL), TLS, or No encryption.

*1 YYYY.MM.DD.hh:mm:ss indicates e-mailing start time. [YYYY: AD year; MM: Month; DD: Day; hh: Hours; mm: Minutes; ss: Seconds]
N indicates the number of a partition: from 0 to 7.

*2 Logs are not attached to e-mail for a destination with log attachemnt “Disabled” set in the e-mail address setting.

*3 E-mail with logs is not sent to a destination with log attachemnt “Disabled” set in the e-mail address setting.

*4 When security is set to high, select ARAM-MD5. If not, e-mail notification is not performed.

*5 When security is set to high, select d TLS. If not, e-mail notification is not performed.

❑ Attached file specifications

The following table describes files attached to e-mail notification.

NO.	File name	Contents	Maximum size *2 Notified automatically [upper line] Triggered by manual operation [lower line]
1	svpsts-YYYYMMDD-hhmmss.gz	Device information	500 kbyte 500 kbyte
2	trc -YYYYMMDD-hhmmss.tar.gz	Management module logs	1000 kbyte 1500 kbyte
3	hvmdumpN-YYYYMMDD-hhmmss.tar.gz	Server blade logs related to LPAR manager	2000 kbyte No attachment
4	uagentN-YYYYMMDD-hhmmss.tar.gz	Server blade logs related to N+M cold standby	2000 kbyte No attachment
5	raslogN-YYYYMMDD-hhmmss.tar.gz	Server blade logs related to hardware	2000 kbyte No attachment
6	marlog.gz	Failure information: the same as the body of notification triggered by failure	1 kbyte No attachment

*1 YYYY.MM.DD.hh:mm:ss indicates e-mailing start time. [YYYY: AD year; MM: Month; DD: Day; hh: Hours; mm: Minutes; ss: Seconds]
N indicates the number of a partition: from 0 to 7.

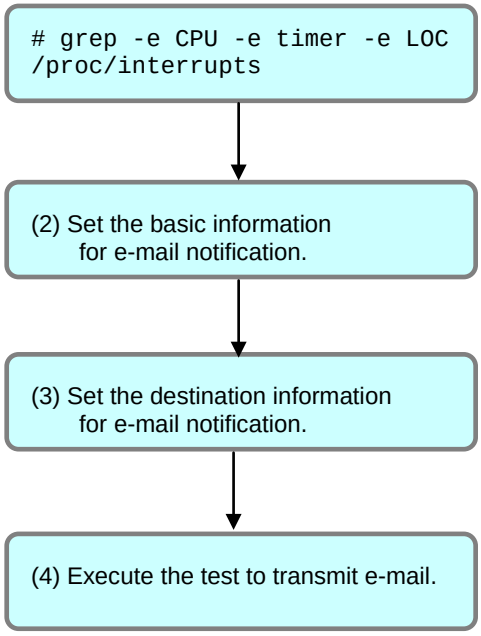
*2 Automatic notification: when triggered by failure, log output, or hand (selected history).
Manual notification: when triggered by manual operation (current status).

E-mail notification setup

❑ Procedure for using e-mail function

The following flow chart shows the procedure for using e-mail functions.

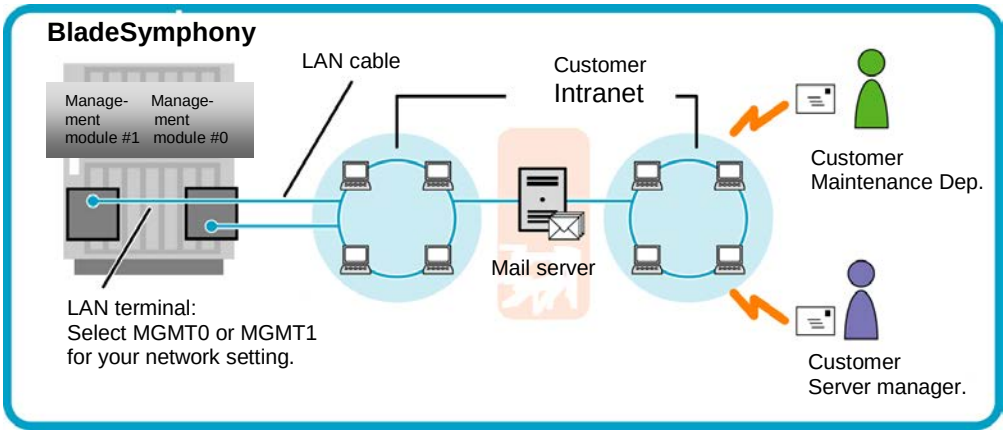
See “System Web Console” in Chapter 6 for information about how to operate the system web console.



(1) Configuring the system environment for e-mail notification

Configure the environment to use e-mail notification.

The following figure shows an example.



(2) Setting the basic information for e-mail notification

- External link setting: shows the e-mail remote notification.
- Input the necessary items in the e-mail transmission setting (management LAN) of the e-mail source setting.

Tip

- To disable the e-mail notification while retaining the setting, disable the e-mail remote notification. Keep other settings unchanged.
- The source e-mail address is an e-mail sender address: from.
- Specify the host name or IP address in the SMTP server field.
- The default port number of the SMTP server is 25.

(3) Setting the destination information for e-mail notification

- External link setting: shows the e-mail remote notification.
- Input or select the necessary items in the e-mail address 0 to 3 fields for e-mail destination settings.

Tip

Make sure to select whether or not to attaché detailed log attached to e-mail.

(4) Executing the e-mailing test

Execute the e-mailing test using e-mail notification by manual operation (the current status).

- Select **e-mail notification > Operation > E-mail notification by manual operation (management LAN)** to execute the test.
- Select the destination address from the list. You can select a specific address or all addresses.
- An inquiry to confirm the e-mail notification, execute it if no problem.
- Logs are collected and then the e-mail notification is executed. Confirm that the e-mail has reached to the destination address.



- Collecting logs takes a few minutes.
- E-mail notification is to finish when the e-mail has been properly transmitted to the mail server.
- When the e-mail is sent to multiple destinations in the test, the email may fail to reach all destinations even if it fails to reach one destination fails.
- If the mailing test fails, review the environment and settings referring to the following description and correct them as necessary.
  - Check if communication between the management module and the mail server is available.
    - If not, check that the LAN cable is properly connected.
    - Check the network setting of the management module.
    - You need to specify DNS in the network setting of the management module when specifying the mail server as the host name.
  - Check if the SMTP service is running on the SMTP server.
  - Check if the basic information and destination information are properly configured.

The following table describes messages showing results from e-mail notification triggered by manual operation.

Message **Description**
The operation for e-mail address % was successful.
Description: The e-mail notification was successfully sent. Checking and Action: None.
The operation for e-mail address % failed. The IP address could not be resolved from the host name.
Description: Failed to obtain an IP address name from the SMTP host name. Checking and Action: Check the e-mail notification setting (SMTP). Check the network setting (DNS: domain name system). Check the connection to LAN.
The operation for e-mail address % failed. The format of the IP address is invalid.

Message Description
Description: An error occurred in the format of the SMTP IP address. Checking and Action: Check the e-mail notification setting (SMTP).
The operation for e-mail address % failed. The failure occurred during the attempt to connect to the SMTP server.
Description: Failed to connect to the SMTP server. Checking and Action: Check all the e-mail notification settings. Check the SMTP server status. Check the connection to LAN.
The operation for e-mail address % failed. The SMTP server does not support SMTP authentication.
Description: The SMTP server does not support the authentication method specified in the e-mail setting. Checking and Action: Check and correct the authentication method in the e-mail notification setting.
The operation for e-mail address % failed because SMTP authentication failed.
Description: The user and password for SMTP authentication are incorrect. Checking and Action: Check and correct the user and password for authentication in the e-mail notification setting.
The operation for e-mail address % failed. The SMTP server does not support the specified encryption system.
Description: The SMTP server does not support the encryption method specified in the email notification setting. Checking and Action: Check and correct the encryption method in the email notification setting.
The operation for e-mail address % failed. The error occurred during communication with the SMTP server.
Description: An error occurred during communication with the SMTP server. Checking and Action: Check the connection to LAN.
The operation for e-mail address % failed. There is no recipient address.
Description: The destination address is not set. Checking and Action: Check the e-mail destination address and put in a correct one.
The operation for e-mail address % failed. The recipient address is invalid.
Description: The destination address is incorrect. The specified user does not exist. Checking and Action: Check the e-mail destination address and put in a correct one.
The operation for e-mail address % failed.
Description: Unexpected error. Checking and Action: Contact your reseller or maintenance personnel.

Note: “%” in messages in the table above stands for the selected e-mail address.

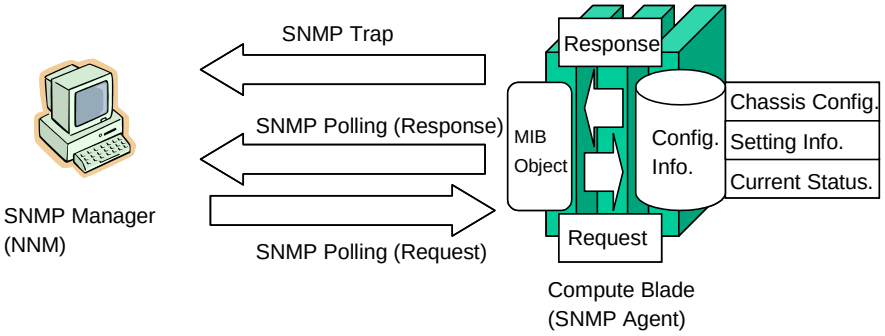
SNMP function

SNMP function overview

(1) Functions

No.	Function	Description
1	Polling	Allows the SNMP manager to recognize Compute Blade as a target to monitor. When the manager requests information on each object of Compute Blade private MIB (Management Information Base), a response corresponding to the information on the Compute Blade private MIB object is returned. This function responds only to requests from the IP address of SNMP Manager registered in the management module.
2	Trap	Sends information spontaneously to the manager according to the Compute Blade private management information base (MIB). This enables the SNMP manager to monitor faults.

The following image shows management by SNMP.



1. SNMP Polling Function

Item	Description
Support command (*1)	SNMPv1/v2c/v3 (Get, GetNext, GetBulk)
Maximum number of SNMP managers that can be notified simultaneously	4
Supported modules	Server blade, management module, switch module, power supply module, fan module, PCI-e riser card (IOCD: input/output control device)

(*1) the Set command is not supported.

2. Specifications of SNMP Trap Function

Item		Description
Means of notification		SNMP (SNMPv2Trap/SNMPv3Trap)
Maximum number of SNMP managers that can be notified simultaneously		4
Event of notification		When the system event log (SEL) of a management module fault is issued.
Content of messaging	Binding of the first variable	Time when the alert was sent.
	Binding of the second variable	Chassis ID
	Binding of the third variable	Alert level
	Binding of the fourth variable	Alert message
	Binding of the fifth variable	Location where the alert occurred
	Binding of the sixth variable	Alert ID See SVP (Service Processor Log) Message in Chapter 6. ID: 14Ex and 17Ex are out of target for SNMP trap.
	Binding of the first variable	Time when the alert was sent.
	Binding of the second variable	Chassis ID

Note: This SNMP trap function does not support the SNMP standard trap.

3. Specifications of SNMPv3

Item	Description
Authentication: Hush method	MD5/SHA-1
Encryption method	DES/AES128

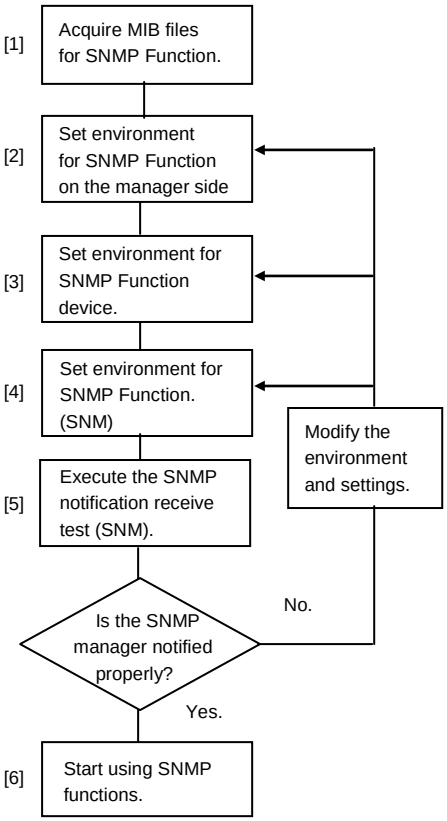
(2) Prerequisites

Prerequisites for using the SNMP function are listed in the table below.

No.	Prerequisites
1	The SNMP manager receiving SNMP traps must be compatible with SNMPv1/v2c/v3.
2	The environment must enable communications between the management module and the management server where the SNMP manager operates.

How to use the SNMP function

(1) Procedure for SNMP



No.	Description
[1]	Acquire a MIB file that is required to perform the SNMP function.
[2]	Register the information in the MIB file acquired in step [1] into the SNMP manager.
[3]	Set the environment that allows SNMP trap function to perform.
[4]	Using the console, set the information required for SNMP functions, including the IP address of the destination SNMP manager and the name of a community for SNMPv1/v2c; the IP address of the destination SNMP manager, engine ID, access type, user name, and password for SNMPv3..
[5]	Using the test notification function, perform a test trap notification. If the SNMP manager fails to receive any test trap notification or receives notification of authentication error in SNMPv3Trap, review steps [2], [3], and [4] for correction.
[6]	The state is in normal operation.

(2) Acquiring MIB files for SNMP

Acquire MIB files from the SNMP agent by executing “Download MIB File” from the SNMP setting menu on the system Web console of the management module.

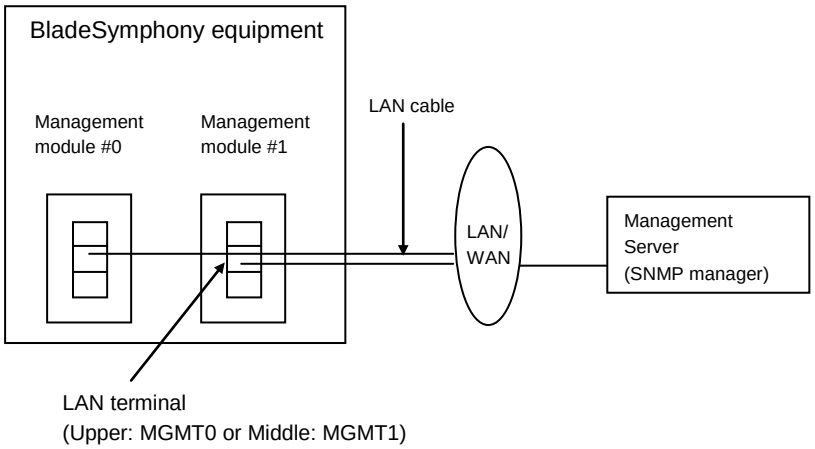
(3) Setting the information on the SNMP manager side

a. Setting the information for using the SNMP trap
Load the MIB for Compute Blade and register the trap event to the manager by following the manual of your SNMP manager. All the trap events notified by this function are as follows:

No.	SNMP trap event name	OID	Description	Fault location
1	hitachiComputeBlade2000AlertTrapMmNon-Recoverable	1.3.6.1.4.1.116.3.39.10.1.1.1	The management module of Compute Blade 2000 encountered a fault at the fault level.	Management module
2	hitachiComputeBlade2000AlertTrapMmSerious	1.3.6.1.4.1.116.3.39.10.1.1.2	The management module of Compute Blade 2000 encountered a fault at the warning level.	Management module
3	hitachiComputeBlade2000AlertTrapMmInformation	1.3.6.1.4.1.116.3.39.10.1.1.3	The management module of Compute Blade 2000 encountered a fault at the information level.	Management module
4	hitachiComputeBlade2000AlertTrapBladeNon-Recoverable	1.3.6.1.4.1.116.3.39.10.1.2.1	The server blade of Compute Blade 2000 encountered a fault at the fault level.	Server blade
5	hitachiComputeBlade2000AlertTrapBladeSerious	1.3.6.1.4.1.116.3.39.10.1.2.2	The server blade of Compute Blade 2000 encountered a fault at the warning level.	Server blade
6	hitachiComputeBlade2000AlertTrapBladeInformation	1.3.6.1.4.1.116.3.39.10.1.2.3	The server blade of Compute Blade 2000 encountered a fault at the information level.	Server blade
7	hitachiComputeBlade2000AlertTrapOtherNon-Recoverable	1.3.6.1.4.1.116.3.39.10.1.20.1	A location except the management module or server blade of Compute Blade 2000 encountered a fault at the fault level.	Excluding the management module and the server blade
8	hitachiComputeBlade2000AlertTrapOtherSerious	1.3.6.1.4.1.116.3.39.10.1.20.2	A location except the management module or server blade of Compute Blade 2000 encountered a fault at the warning level.	Excluding the management module and the server blade
9	hitachiComputeBlade2000AlertTrapOtherInformation	1.3.6.1.4.1.116.3.39.10.1.20.3	A location except the management module or server blade of Compute Blade 2000 encountered a fault at the information level.	Excluding the management module and the server blade
10	hitachiComputeBlade2000AlertTrapOtherEvent	1.3.6.1.4.1.116.3.39.10.1.20.4	A location except the management module or server blade of Compute Blade 2000 encountered an event.	Excluding the management module and the server blade

b. Setting the information for using the SNMP polling
Select MIB objects to acquire the information on Compute Blade and configure the necessary settings to acquire the values by following the manual of your SNMP manager. Information obtained from Compute Blade is shown in MIB reference.

(4) Example of environment configuration for SNMP



No.	Item	Description
1	SNMP manager	- It is necessary for a customer to obtain a management server equipped with an SNMP manager for receiving SNMP traps and processing SNMP requests. - The SNMP protocol essential for the SNMP manager to use is SNMPv1/v2c/v3.

(5) Setting the information on the SNMP agent side

Select **External cooperation -> SNMP setting -> Agent setting** and **Manager setting**, and then set the various items of information on the SNMP agent, the destination of SNMP traps, SNMP manager address, and community name for SNMPv1/v2c. To use SNMPv3, set items of information on the SNMP agent in the same way, including the destination of SNMP traps, user name, access level, types of authentication and encryption, and passwords of authentication and encryption, especially the engine ID is a must.

(6) Performing SNMP tests

Select **External cooperation -> SNMP setting** from the system Web console of the management module and execute **SNMP trap transmit ion** menu to perform the SNMP test trap notification test.

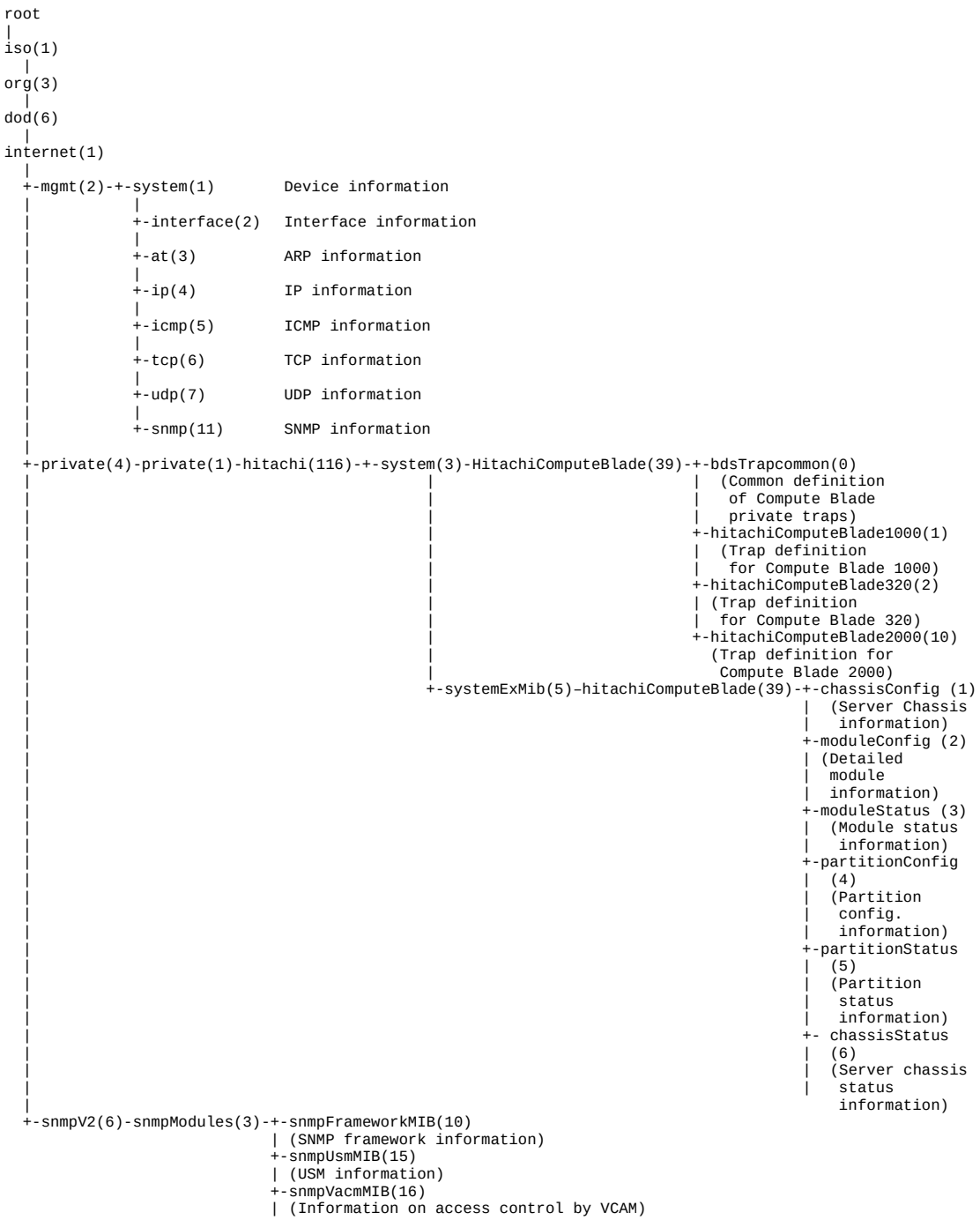
(7) SNMP operation

Operate the SNMP function by following the information that is set with the system Web console. When a fault occurs in the Compute Blade, obtain log files needed for fault analysis using the DL command if there is a request from maintenance personnel.

MIB reference

(1) MIB tree structure

MIB supported by Compute Blade 2000 is comprised of MIB II objects and Compute Blade private MIB objects. The main tree structure is shown as follows:



(2) MIB description in the reference

This section shows the form to describe MIB in this reference, and explains the supported items to be described in the section about MIB objects.

1. Object Identifier

   The name of an MIB object identifier is shown.

2. OID (Object ID)

   OID corresponding to an MIB object identifier is shown.

3. SYNTAX

   The meaning of a syntax used in the private MIB is shown as follows:

No.	SYNTAX	Description
1	Not-Accessible	Access is not allowed.
2	Display String	0 to 2040 characters in a row
3	INTEGER	Integer value from -2147483648 to 2147483647
4	Integer32	Integer value from –2147483648 to 2147483647

4. Access

   RO: shows that MIB access is read-only.

   RW: shows that MIB access is read-write.

   NA: shows that MIB access is not-accessible.

(3) Supported standard MIB objects

Eight groups in the standard MIB, such as system, interfaces, at, ip, icmp, tcp, udp, and snmp, are supported. Objects in each group are partially supported. Supported MIB objects of each group are described in tables (a) to (h) as shown below.

(a) system group

No.	Object identifier	OID	Access	Description
1	sysDescr	.1.3.6.1.2.1 .1.1	NA	Describes the management equipment. This equipment has “Hitachi Compute Blade System Ver XXXXX” as the fixed value. Ver XXXXX shows the firmware version of the management module.
2	sysObjectID	.1.3.6.1.2.1 .1.2	RO	Shows the vender OID of the management equipment. This equipment has the OID value of private.hitachi.system.Compute Blade.2000 (.1.3.6.1.4.1.116.3.39.10) as the fixed value.
3	sysUpTime	.1.3.6.1.2.1 .1.3	RO	Shows the accumulated time by the 10 msec after the SNMP agent boots up.
4	sysContact	.1.3.6.1.2.1 .1.4	RO (*1)	Shows the contact related to the management equipment. The contact, set with the system Web console, is a character row.
5	sysName	.1.3.6.1.2.1 .1.5	RO (*1)	Shows the name related to the management equipment. The name is the chassis ID value.
6	sysLocation	.1.3.6.1.2.1 .1.6	RO (*1)	Shows the contact related to the management equipment. The contact, set with the system Web console, is a character row.

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(b) interfaces group (1/2)

No.	Object identifier	OID	Access	Description
1	ifNumber	.1.3.6.1.2.1.2.1	RO	Shows the number of interfaces that the management equipment has.
2	ifTable	.1.3.6.1.2.1.2.2	NA	Shows the table for setting interfaces.
3	ifEntry	.1.3.6.1.2.1.2.2.1	NA	Shows the list for setting interfaces.
4	ifIndex	.1.3.6.1.2.1.2.2.1.1	RO	Shows the number to identify each interface. The value is from 1 to ifNumber. (*1)
5	ifDescr	.1.3.6.1.2.1.2.2.1.2	RO	Shows the information on each interface. (*1)
6	ifType	.1.3.6.1.2.1.2.2.1.3	RO	Shows the type of each interface: Ethernet-csmacd (6) for this equipment. (*1)
7	ifMtu	.1.3.6.1.2.1.2.2.1.4	RO	Shows the maximum diagram size in octet that each interface can send and receive. (*1)
8	ifSpeed	.1.3.6.1.2.1.2.2.1.5	RO	Shows the current circuit speed of each interface in bit/s. (*1)
9	ifPhysAddress	.1.3.6.1.2.1.2.2.1.6	RO	Shows the physical address of each interface. (*1)
10	ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	RO (*2)	Shows the desirable state of each interface. (*1) One of the following values is shown. * up (1) * down (2) * testing (3)
11	ifOperStatus	.1.3.6.1.2.1.2.2.1.8	RO	Shows the current status of each interface. (*1) One of the following values is shown. * up (1) * down (2) * testing (3)
12	ifInOctets	.1.3.6.1.2.1.2.2.1.10	RO	Shows the total number of octets that each interface has received. (*1)
13	ifInUcastPkts	.1.3.6.1.2.1.2.2.1.11	RO	Shows the number of unicast packets that each interface has received. (*1)
14	IfInNUcastPkts	.1.3.6.1.2.1.2.2.1.12	RO	Shows the number of non-unicast packets that each interface has received. (*1)
15	ifInDiscards	.1.3.6.1.2.1.2.2.1.13	RO	Shows the number of packets discarded not because of an error among incoming packets to each interface. (*1)
16	ifInErrors	.1.3.6.1.2.1.2.2.1.14	RO	Shows the number of error packets among incoming packets to each interface. (*1)
17	ifUnknown Prots	.1.3.6.1.2.1.2.2.1.15	RO	Shows the number of packets discarded due to the unsupported protocol among incoming packets to each interface.
18	ifOutOctets	.1.3.6.1.2.1.2.2.1.16	RO	Shows the total number of octets sent by each interface. (*1)

(*1) This object includes the information only on some interfaces.

(*2) This object is RW in the SNMP standard, but RO for this equipment.

(b) interfaces group (2/2)

No.	Object identifier	OID	Access	Description
19	ifOutUcastPkts	.1.3.6.1.2.1.2.2.1.17	RO	Shows the number of unicast packets sent by each interface. (*1)
20	ifOutDiscards	.1.3.6.1.2.1.2.2.1.19	RO	Shows the number of packets discarded not because of an error among outgoing packets from each interface. (*1)
21	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	RO	Shows the number of error packets among outgoing packets from each interface. (*1)
22	ifOutQLen	.1.3.6.1.2.1.2.2.1.21	RO	Shows the number of packets that each interface can store in the output queue. (*1)
23	ifSpecific	.1.3.6.1.2.1.2.2.1.22	RO	Shows the reference to MIB that specifies features of the interface media. It is the MIB object ID dependent on ifType. (*1)

(*1) This object includes the information only on some interfaces.
(*2) This object is RW in the SNMP standard, but RO for this equipment.

(c) at group

No.	Object identifier	OID	Access	Description
1	atTable	.1.3.6.1.2.1.3.1	NA	Shows the Address Translation Table.
2	atEntry	.1.3.6.1.2.1.3.1.1	NA	Shows the entry of the Address Translation table.
3	atIfIndex	.1.3.6.1.2.1.3.1.1.1	RO	Shows the ifIndex value of the corresponding interface. (*1)
4	atPhysAddress	.1.3.6.1.2.1.3.1.1.2	RO	Shows the physical address. (*1)
5	atNetAddress	.1.3.6.1.2.1.3.1.1.3	RO	Shows the IP address corresponding to atPhysAddress. (*1)

(*1) This object includes the information only on some interfaces.

(d) ip group

No.	Object identifier	OID	Access	Description
1	ipAddrTable	.1.3.6.1.2.1.4.20	NA	Shows the table related to an IP address.
2	ipAddrEntry	.1.3.6.1.2.1.4.20.1	NA	Shows the list of the table related to an IP address.
3	ipAdEntAddr	.1.3.6.1.2.1.4.20.1.1	RO	Shows an IP address. (*1)
4	ipAdEntIfIndex	.1.3.6.1.2.1.4.20.1.2	RO	Shows the index of an interface. (*1)
5	ipAdEntNetMask	.1.3.6.1.2.1.4.20.1.3	RO	Shows a Subnet mask. (*1)
6	ipAdEntBcastAddr	.1.3.6.1.2.1.4.20.1.4	RO	Shows the lowest bit value of a broadcast address. (*1)

(*1) This object includes the information only on some interfaces.

(e) icmp group (1/2)

No.	Object identifier	OID	Access	Description
1	icmpInMsgs	.1.3.6.1.2.1.5.1	RO	Shows the total number of incoming Internet Control Message Protocol (ICMP) messages.
2	icmpInErrors	.1.3.6.1.2.1.5.2	RO	Shows the number of incoming ICMP error messages.
3	icmpInDestUnreachs	.1.3.6.1.2.1.5.3	RO	Shows the total number of incoming “Destination Unreachable” messages.
4	icmpInTimeExcds	.1.3.6.1.2.1.5.4	RO	Shows the total number of incoming “TimeExceeded” messages.
5	icmpInParmProbs	.1.3.6.1.2.1.5.5	RO	Shows the total number of incoming “Parameter Problem” message s.
6	icmpInSrcQuenchs	.1.3.6.1.2.1.5.6	RO	Shows the total number of incoming “Source Quench” messages.
7	icmpInRedirects	.1.3.6.1.2.1.5.7	RO	Shows the total number of incoming “Redirect” messages.
8	icmpInEchos	.1.3.6.1.2.1.5.8	RO	Shows the total number of incoming “Echo Request” messages.
9	icmpInEchosReps	.1.3.6.1.2.1.5.9	RO	Shows the total number of incoming “Echo Reply” messages.
10	icmpInTimestamps	.1.3.6.1.2.1.5.10	RO	Shows the total number of incoming “Timestamp Request” messages.
11	icmpInTimestampsReps	.1.3.6.1.2.1.5.11	RO	Shows the total number of incoming “Timestamp Reply” messages.
12	icmpInAddMasks	.1.3.6.1.2.1.5.12	RO	Shows the total number of incoming “Address Mask Request” messages.
13	icmpInAddMasksReps	.1.3.6.1.2.1.5.13	RO	Shows the total number of t incoming “Address Mask Reply” messages.

(e) icmp group (2/2)

No.	Object identifier	OID	Access	Description
14	icmpOutMsgs	.1.3.6.1.2.1.5.14	RO	Shows the total number of outgoing ICMP messages.
15	icmpOutErrors	.1.3.6.1.2.1.5.15	RO	Shows the total number of outgoing error ICMP messages.
16	icmpOutDestUnreachs	.1.3.6.1.2.1.5.16	RO	Shows the total number of outgoing “Destination Unreachable” messages.
17	icmpOutTimeExcds	.1.3.6.1.2.1.5.17	RO	Shows the total number of outgoing “TimeExceeded” messages.
18	icmpOutParmProbs	.1.3.6.1.2.1.5.18	RO	Shows the total number of outgoing “Parameter Problem” messages.
19	iIcmpOutSrcQuenchs	.1.3.6.1.2.1.5.19	RO	Shows the total number of outgoing “Source Quench” messages.
20	icmpOutRedirects	.1.3.6.1.2.1.5.20	RO	Shows the total number of outgoing “Redirect” messages.
21	icmpOutEchos	.1.3.6.1.2.1.5.21	RO	Shows the total number of outgoing “Echo Request” messages.
22	icmpOutEchosReps	.1.3.6.1.2.1.5.22	RO	Shows the total number of outgoing “Echo Reply” message.
23	icmpOutTimestamps	.1.3.6.1.2.1.5.23	RO	Shows the total number of outgoing “Timestamp Request” messages.
24	icmpOutTimestampsReps	.1.3.6.1.2.1.5.24	RO	Shows the total number of outgoing “Timestamp Reply” message.
25	icmpOutAddMasks	.1.3.6.1.2.1.5.25	RO	Shows the total number of outgoing “Address Mask Request” messages.
26	icmpOutAddMasksReps	.1.3.6.1.2.1.5.26	RO	Shows the total number of t outgoing “Address Mask Reply” messages.

(f) tcp group

No.	Object identifier	OID	Access	Description
1	tcpConnTable	.1.3.6.1.2.1.6.13	NA	Shows the information table of Transmission Checksum Protocol (TCP) connection.
2	tcpConnEntry	.1.3.6.1.2.1.6.13.1	NA	Shows the information table entry of TCP connection.
3	tcpConnState	.1.3.6.1.2.1.6.13.1.1	RO (*1)	Shows the status of TCP connection. (*2) One of the following values is shown. · closed（1） · listen（2） · synSent（3） · synReceived（4） · established（5） · finWait1（6） · finWait2（7） · closeWait（8） · astAck（9） · closing（10） · timeWait（11） · deleteTCB（12）
4	tcpConnLocalAddress	.1.3.6.1.2.1.6.13.1.2	RO	Shows the local IP address of TCP connection. (*2)
5	tcpConnLocalPort	.1.3.6.1.2.1.6.13.1.3	RO	Shows the local port number of TCP connection. (*2)
6	tcpConnRemAddress	.1.3.6.1.2.1.6.13.1.4	RO	Shows the remote IP address of TCP connection. (*2)
7	tcpConnRemPort	.1.3.6.1.2.1.6.13.1.5	RO	Shows the remote port number of TCP connection. (*2)
8	tcpInErrs	.1.3.6.1.2.1.6.14	RO	Shows the number of incoming error segments.
9	tcpOutRsts	.1.3.6.1.2.1.6.15	RO	Shows the number of outgoing segments with the reset (RST) flag.

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object includes the information only on some interfaces.

(g) udp group

No.	Object identifier	OID	Access	Description
1	udpConnTable	.1.3.6.1.2.1.7.5	NA	Shows the information table of User Datagram Protocol (UDP) connection.
2	udpConnEntry	.1.3.6.1.2.1.7.5.1	NA	Shows the information table entry of UDP connection.
3	udpConnLocalAddress	.1.3.6.1.2.1.7.5.1.1	RO	Shows the local IP address of UDP connection. (*1)
4	udpConnLocalPort	.1.3.6.1.2.1.7.5.1.2	RO	Shows the local port number of UDP connection. (*1)

(*1) This object includes the information only on some interfaces.

(h) snmp group (1/2)

No.	Object identifier	OID	Access	Description
1	snmpInPkts	.1.3.6.1.2.1.11.1	RO	Shows the total number of incoming SNMP messages.
2	snmpOutPkts	.1.3.6.1.2.1.11.2	RO	Shows the total number of SNMP outgoing messages.
3	snmpInBadVersions	.1.3.6.1.2.1.11.3	RO	Shows the total number of incoming unsupported version messages.
4	snmpInBadCommunityNames	.1.3.6.1.2.1.11.4	RO	Shows the total number of incoming unused community name messages.
5	snmpInBadCommunityUses	.1.3.6.1.2.1.11.5	RO	Shows the total number of incoming messages that describe the operation not allowed in the community.
6	snmpInASNParseErrs	.1.3.6.1.2.1.11.6	RO	Shows the total number of incoming “ASN.1 Error” messages.
7	snmpInTooBigs	.1.3.6.1.2.1.11.8	RO	Shows the total number of incoming PDUs whose error statuses are tooBig.
8	snmpInNoSuchNames	.1.3.6.1.2.1.11.9	RO	Shows the total number of incoming PDUs whose error statuses are noSuchName.
9	snmpInBadValues	.1.3.6.1.2.1.11.10	RO	Shows the total number of incoming PDUs whose error statuses are badValue.
10	snmpInReadOnlys	.1.3.6.1.2.1.11.11	RO	Shows the total number of incoming PDUs whose error statuses are readOnly.
11	snmpInGenErrs	.1.3.6.1.2.1.11.12	RO	Shows the total number of incoming PDUs whose error statuses are genErr.
12	snmpInTotalReqVars	.1.3.6.1.2.1.11.13	RO	Shows the total number of MIB objects that are successfully collected.
13	snmpInTotalSetVars	.1.3.6.1.2.1.11.14	RO	Shows the total number of MIB objects that are successfully set.
14	snmpInGetRequests	.1.3.6.1.2.1.11.15	RO	Shows the number of incoming “GetRequest” messages.
15	snmpInGetNexts	.1.3.6.1.2.1.11.16	RO	Shows the number of incoming “GetNext” messages.
16	snmpInSetRequests	.1.3.6.1.2.1.11.17	RO	Shows the number of incoming “SetRequest” messages.
17	snmpInGetResponses	.1.3.6.1.2.1.11.18	RO	Shows the number of incoming “GetResponse” messages.
18	snmpInTraps	.1.3.6.1.2.1.11.19	RO	Shows the number of incoming Traps.
19	snmpOutTooBigs	.1.3.6.1.2.1.11.20	RO	Shows the total number of outgoing PDUs whose error status is tooBig.
20	snmpOutNoSuchNames	.1.3.6.1.2.1.11.21	RO	Shows the total number of outgoing PDUs whose error status is noSuchName.
21	snmpOutBadValues	.1.3.6.1.2.1.11.22	RO	Shows the total number of outgoing PDUs whose error status is badValue.

(h) SNMP group (2/2)

No.	Object identifier	OID	Access	Description
22	snmpOutReadOnlys	.1.3.6.1.2.1.11.23	RO	Shows the total number of outgoing PDUs whose error status is readOnly.
23	snmpOutGenErrs	.1.3.6.1.2.1.11.24	RO	Shows the total number of outgoing PDUs whose error status is genErr.
24	snmpOutGetRequests	.1.3.6.1.2.1.11.25	RO	Shows the number of outgoing “GetRequests” messages.
25	snmpOutGetNexts	.1.3.6.1.2.1.11.26	RO	Shows the number of outgoing “GetNexts” messages.
26	snmpOutSetRequests	.1.3.6.1.2.1.11.27	RO	Shows the number of outgoing “SetRequests” messages.
27	snmpOutGetResponces	.1.3.6.1.2.1.11.28	RO	Shows the number of outgoing “GetResponces” messages.
28	snmpOutTraps	.1.3.6.1.2.1.11.29	RO	Shows the number of outgoing Traps.
29	snmpEnableAuthenTraps	.1.3.6.1.2.1.11.30	RO (*1)	Shows whether or not to issue an authentication-failure Trap. · enable（1） · disable（2）
30	snmpSilentDrops	.1.3.6.1.2.1.11.31	RO	Shows the total number of SNMP incoming messages that were silently dropped because the reply size was greater than the maximum message size.
31	snmpProxyDrops	.1.3.6.1.2.1.11.32	RO	Shows the total number of SNMP incoming messages including GetRequest-PDU, GetNextRequest-PDU: power distribution unit, GetBulkRequest-PDU. SetRequest-PDU and InformRequest-PDU that were silently dropped because the transmission of the message to a proxy target failed in a way that no response PDU could be returned.

(*1) This object includes the information only on some interfaces.

(4) Supported SNMPv2 MIB objects

snmpv2 group mainly describes information on SNMPv3.

This equipment supports items consisting of the following three groups: snmpFrameworkMIB, snmpUsmMIB, and snmpVacmMIB.

(a) snmpFrameworkMIB group

No.	Object identifier	OID	Syntax	Description
1	snmpEngineID	.1.3.6.1.6.3.10.2.1.1	RO	Shows the engine ID value for SNMP engine management.
2	snmpEngineBoots	.1.3.6.1.6.3.10.2.1.2	RO	Shows how many times the SNMP engine (SNMP agent) has been booted after the last setting of a snmpEnginID.
3	snmpEngineTime	.1.3.6.1.6.3.10.2.1.3	RO	Shows how many seconds has passed after the last booting of the SNMP engine (SNMP agent).
4	snmpEngineMaxMessageSize	.1.3.6.1.6.3.10.1.1.4	RO	Shows the maximum size of message that the SNMP engine (SNMP agent) can send and receive. The value is fixed at 1,500 in this product.

(b) snmpUsmMIB group (1/2)

No.	Object identifier	OID	Syntax	Description
1	usmStatsUnsupportedSecLevels	.1.3.6.1.6.3.15.1.1.1	RO	Shows the total number of received packets that are discarded for unsupported security levels.
2	usmStatsNotInTimeWindows	.1.3.6.1.6.3.15.1.1.2	RO	Shows the total number of received packets that are discarded for out of Window Time.
3	usmStatsUnknownUserNames	.1.3.6.1.6.3.15.1.1.3	RO	Shows the total number of received packets that are discarded for unknown users.
4	usmStatsUnknownEngineIDs	.1.3.6.1.6.3.15.1.1.4	RO	Shows the total number of received packets discarded for referring to unknown snmpEngine IDs.
5	usmStatsWrongDigests	.1.3.6.1.6.3.15.1.1.5	RO	Shows the total number of received packets discarded for excluding wrong digest values.
6	usmStatsDecryptionErrors	.1.3.6.1.6.3.15.1.1.6	RO	Shows the total number of received packets discarded for decryption errors.
7	usmUserSpinLock	.1.3.6.1.6.3.15.1.2.1	RO (*1)	Used for spin lock operation to change usmUserTable security.
8	usmUserTable	.1.3.6.1.6.3.15.1.2.2	NA	Shows the user table in Local Configuration Datastore (LCD) of the SNMP engine.
9	usmUserEntry	.1.3.6.1.6.3.15.1.1.2.1	NA	Shows the user table entry in Local Configuration Datastore (LCD) of the SNMP engine.
10	usmUserEngineID	.1.3.6.1.6.3.15.1.1.2.1.1	RO	Shows ID for managing the SNMP engine.
11	usmUserName	.1.3.6.1.6.3.15.1.1.2.1.2	RO	Readable user name: security ID on which USM depends.
12	usmUserSecurityName	.1.3.6.1.6.3.15.1.1.2.1.3	RO	Readable user name not depending on the security model: the same value as usmUserName.
13	usmUserCloneFrom	.1.3.6.1.6.3.15.1.1.2.1.4	RO (*1)	Shows a pointer to another entry from which a new entry is cloned. OID fixed at 0.0 (zerodotzero) is responded.
14	usmUserAuthProtocol	.1.3.6.1.6.3.15.1.1.2.1.5	RO	Authentication protocol of the SNMP engine shown in usmUserEngineID. One of the following values is shown: 1: sumNoAuthProtocol (No authentication) 2: usmHMACMD5AuthProtocol (MD5 authenticated) 3: usmHMACSHAAuthProtocol (SHA authenticated)

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(b) snmpUsmMIB group (2/2)

No.	Object identifier	OID	Syntax	Description
15	usmUserAuthKeyChange	.1.3.6.1.6.3.15.1.1.2.1.6	RO (*1)	Object to create an snmp engine authentication key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from usmUserName of this entry. This object is fixed at ‘ ‘H.
16	usmUserOwnAuthKeyChange	.1.3.6.1.6.3.15.1.1.2.1.7	RO (*1)	Object to create a snmp engine authentication key shown in usmUserEngineID. This object is set when usmUserName is different from usmUserName of this entry. This object is fixed at ‘ ‘H.
17	usmUserPrivProtocol	.1.3.6.1.6.3.15.1.1.2.1.8	RO (*1)	Used by the privacy protocol of the SNMP engine shown in usmUserEngineID. One of the following values is shown: 1: usmNoPrivProtocol (No encryption) 2: usmDESPrivProtocol (DES encryption) 4: usmAesCfb128Protocol (AES encryption)
18	usmUserPrivKeyChange	.1.3.6.1.6.3.15.1.1.2.1.9	RO (*1)	Object to create an encryption key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from sumUserName of this entry.
19	usmUserOwnPrivKeyChange	.1.3.6.1.6.3.15.1.1.2.1.10	RO (*1)	Object to create an encryption key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from sumUserName of this entry. This object is fixed at ‘ ‘H.
20	usmUserPublic	.1.3.6.1.6.3.15.1.1.2.1.11	RO (*1)	User authentication key: this value is created when an encryption key is changed. It can be used later to determine if the key change is enabled or not. This object is fixed at ‘ ’H.
21	usmUserStorageType	.1.3.6.1.6.3.15.1.1.2.1.12	RO (*1)	Storage type of the user entry. This value is fixed at permanent (4).
22	usmUserStatus	.1.3.6.1.6.3.15.1.1.2.1.13	RO (*1)	Shows status of the user entry. This value is fixed at activate (1).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(c) snmpVacmMIB group (1/2)

No.	Object identifier	OID	Syntax	Description
1	vacmContext Table	.1.3.6.1.6.3.16 .1.5.1	NA	Shows the context table available locally.
2	vacmContext Entry	.1.3.6.1.6.3.16 .1.5.1.1	NA	Shows the context table entry available locally.
3	vacmContext Name	.1.3.6.1.6.3.16 .1.1.1.1.1	RO	Shows the readable name for a specific context in a specific SNMP entity. The empty contextName is the default context.
4	vacmSecurit yToGroupTa ble	.1.3.6.1.6.3.16 .1.2	RO	Shows the table for defining the access control policy to the operators group.
5	vacmSecurit yToGroupEn try	.1.3.6.1.6.3.16 .1.2.1	RO	Shows the table entry for defining the access control policy to the operators group.
6	vacmGroupN ame	.1.3.6.1.6.3.16 .1.2.1.2.3	RO	Shows the group name to which this entry belongs.
7	vacmSecurit yToGroupSt orageType	.1.3.6.1.6.3.16 .1.2.1.2.4	RO	Shows the method for storing this table entry, which is fixed at active(4).
8	vacmSecurit yToGroupSt atus	.1.3.6.1.6.3.16 .1.2.1.2.5	NA	Shows the method for storing this table entry, which is fixed at active (1).
9	vacmAccess Table	.1.3.6.1.6.3.16 .1.4.1	NA	Shows the table of access rights that the group has.
10	vacmAccess Entry	.1.3.6.1.6.3.16 .1.4.1.1	NA	Shows the table entry of access rights that the group has.
11	vacmAccess ContextMatc h	.1.3.6.1.6.3.16 .1.4.1.1.4	RO (*1)	Shows the method for matching contextName to vacmAccessContextPrefix. The value is fixed at exact (1).
12	vacmAccess ReadViewNa me	.1.3.6.1.6.3.16 .1.4.1.1.5	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for read access authorized by this entry.
13	vacmAccess WriteViewNa me	.1.3.6.1.6.3.16 .1.4.1.1.6	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for write access authorized by this entry.
14	vacmAccess NotifyViewN ame	.1.3.6.1.6.3.16 .1.4.1.1.7	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for notification access authorized by this entry.
15	vacmAccess StorageType	.1.3.6.1.6.3.16 .1.4.1.1.8	RO (*1)	Shows the method for storing this entry. The value is fixed at permanent (4).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object is RC (Read Create) in the SNMP standard, but RO for this equipment.

(c) snmpVacmMIB group (2/2)

No.	Object identifier	OID	Syntax	Description
16	vacmAccess Status	.1.3.6.1.6.3.16 .1.4.1.1.9	RO (*1)	Shows the method for storing the user entry. The value is fixed at active(1).
17	vacmViewSp inLock	.1.3.6.1.6.3.16 .1.5.1	RO (*1)	Shows advisory lock, which allows cooperative SNMP command generator application to cooperate, for SET operation to create or change views. The value is fixed at 0 (zero).
18	vacmViewTr eeFamilyTab le	.1.3.6.1.6.3.16 .1.1.2	NA	Shows the local storage table for information on the sub-tree family of MIB view.
19	vacmViewTr eeFamilyEntr y	.1.3.6.1.6.3.16 .1.1.2.1	NA	Shows the local storage table entry for information on the sub-tree family of MIB view.
20	vacmViewTr eeFamilyMa sk	.1.3.6.1.6.3.16 .1.1.2.3	RO	Shows the mask value of vacmViewTreeFamilySubtree. The value is fixed at ‘ ‘ H.
21	vacmViewTr eeFamilyTyp e	.1.3.6.1.6.3.16 .1.1.2.4	RO (*1)	Shows that MIB view is included or excluded. One of the following values is displayed. 1: included 2: excluded
22	vacmViewTr eeFamilyStor ageType	.1.3.6.1.6.3.16 .1.1.2.5	RO (*1)	Shows the method for storing this entry. The value is fixed at permanent (4).
23	vacmViewTr eeFamilyStat us	.1.3.6.1.6.3.16 .1.1.2.6	RO (*2)	Shows the status of this entry. The value is fixed at active (1).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object is RC (Read Create) in the SNMP standard, but RO for this equipment.

(5) Supported private MIB objects

1 chassisConfig

chassisConfig consists of the following nine groups: chassisCapacity, chassisConfigBlade, chassisConfigMm, chassisConfigSw, chassisConfigFan, chassisConfigPs, chassisConfigPciRiser, chassisConfigSystem, and chassisConfigPcieSw. Each group is described in the following table (a) to (i).

(a) chassisCapacity group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisCapacity	.1.3.6.1.4.1.116.5.39.1.1	Not-Accessible	NA	Shows the maximum number of slots corresponding to each module in Compute Blade.
2	chassisCapacityBlade	.1.3.6.1.4.1.116.5.39.1.1.1	Integer32	RO	Shows the maximum number of slots for server blade installation.
3	chassisCapacityMm	.1.3.6.1.4.1.116.5.39.1.1.2	Integer32	RO	Shows the maximum number of slots for management module installation.
4	chassisCapacitySw	.1.3.6.1.4.1.116.5.39.1.1.3	Integer32	RO	Shows the maximum number of slots for switch module installation.
5	chassisCapacityFan	.1.3.6.1.4.1.116.5.39.1.1.5	Integer32	RO	Shows the maximum number of slots for fan module installation.
6	chassisCapacityPs	.1.3.6.1.4.1.116.5.39.1.1.6	Integer32	RO	Shows the maximum number of slots for power supply module installation.
7	chassisCapacityPciRiser	.1.3.6.1.4.1.116.5.39.1.1.8	Integer32	RO	Shows the maximum number of slots for PCI riser card (IOCD module) installation.
8	chassisCapacityPcieSw*	.1.3.6.1.4.1.116.5.39.1.1.9	Integer32	RO	Shows the maximum number of slots for PCI Express switch modules.
9	chassisCapacityMarlog	.1.3.6.1.4.1.116.5.39.1.1.10	Integer32	RO	Shows the maximum number of index for MAR (Maintenance Action Report) logs.

(*) This item is not supported.

(b) chassisConfigBlade group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigBlade	.1.3.6.1.4.1.116.5.39.1.2	Not-Accessible	NA	Shows the information on server blade installation.
2	bladeInstallTable	.1.3.6.1.4.1.116.5.39.1.2.1	Not-Accessible	NA	Shows the table of information on server blade installation.
3	bladeInstallEntry	.1.3.6.1.4.1.116.5.39.1.2.1.1	Not-Accessible	NA	Shows the table entry describing the information on server blade installation.
4	bladeInstallIndex	.1.3.6.1.4.1.116.5.39.1.2.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityBlade to identify the table entry.
5	bladeInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.2.1.1.2	Integer32	RO	Shows the server blade slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityBlade–1.
6	bladeInstallExist	.1.3.6.1.4.1.116.5.39.1.2.1.1.3	INTEGER	RO	Shows the server blade installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(c) chassisConfigMm group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigMm	.1.3.6.1.4.1.116.5.39.1.3	Not-Accessible	NA	Shows the information on management module installation.
2	mmInstallTable	.1.3.6.1.4.1.116.5.39.1.3.1	Not-Accessible	NA	Shows the table of information on management module installation.
3	mmInstallEntry	.1.3.6.1.4.1.116.5.39.1.3.1.1	Not-Accessible	NA	Shows the table entry describing the information on management module installation.
4	mmInstallIndex	.1.3.6.1.4.1.116.5.39.1.3.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMm to identify the table entry.
5	mmInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.3.1.1.2	Integer32	RO	Shows the management module slot number corresponding to the index shown in #4, ranging from 0 to chassis CapacityMm–1.
6	mmInstallExist	.1.3.6.1.4.1.116.5.39.1.3.1.1.3	INTEGER	RO	Shows the management module installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(d) chassisConfigSw group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigSw	.1.3.6.1.4.1.116.5.39.1.4	Not-Accessible	NA	Shows the information on switch module installation.
2	swInstallTable	.1.3.6.1.4.1.116.5.39.1.4.1	Not-Accessible	NA	Shows the table of information on switch module installation.
3	swInstallEntry	.1.3.6.1.4.1.116.5.39.1.4.1.1	Not-Accessible	NA	Shows the table entry describing the information on switch module installation.
4	swInstallIndex	.1.3.6.1.4.1.116.5.39.1.4.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacitySw to identify the table entry.
5	swInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.4.1.1.2	Integer32	RO	Shows the switch module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacitySw–1.
6	swInstallExist	.1.3.6.1.4.1.116.5.39.1.4.1.1.3	INTEGER	RO	Shows the switch module installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(e) chassisConfigFan group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigFan	.1.3.6.1.4.1.116.5.39.1.6	Not-Accessible	NA	Shows the information on fan module installation.
2	fanInstallTable	.1.3.6.1.4.1.116.5.39.1.6.1	Not-Accessible	NA	Shows the table of information on fan module installation.
3	fanInstallEntry	.1.3.6.1.4.1.116.5.39.1.6.1.1	Not-Accessible	NA	Shows the table entry describing the information on fan module installation.
4	fanInstallIndex	.1.3.6.1.4.1.116.5.39.1.6.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityFan to identify the table entry.
5	fanInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.6.1.1.2	Integer32	RO	Shows the fan module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityFan–1.
6	fanInstallExist	.1.3.6.1.4.1.116.5.39.1.6.1.1.3	INTEGER	RO	Shows the fan module installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(f) chassisConfigPs group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigPs	.1.3.6.1.4.1.116.5.39.1.7	Not-Accessible	NA	Shows the information on power supply module installation.
2	psInstallTable	.1.3.6.1.4.1.116.5.39.1.7.1	Not-Accessible	NA	Shows the table of information on power supply module installation.
3	psInstallEntry	.1.3.6.1.4.1.116.5.39.1.7.1.1	Not-Accessible	NA	Shows the table entry describing the information on power supply module installation.
4	psInstallIndex	.1.3.6.1.4.1.116.5.39.1.7.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPs to identify the table entry.
5	psInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.7.1.1.2	Integer32	RO	Shows the power supply module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPs–1.
6	psInstallExist	.1.3.6.1.4.1.116.5.39.1.7.1.1.3	INTEGER	RO	Shows the power supply module installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(g) chassisConfigPciRiser group

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigPciRiser	.1.3.6.1.4.1.116.5.39.1.9	Not-Accessible	NA	Shows the information on PCI-e riser card (IOCD module) installation.
2	pciRiserInstallTable	.1.3.6.1.4.1.116.5.39.1.9.1	Not-Accessible	NA	Shows the table of information on PCI-e riser card (IOCD module) installation.
3	pciRiserInstallEntry	.1.3.6.1.4.1.116.5.39.1.9.1.1	Not-Accessible	NA	Shows the table entry describing the information on PCI-e riser card (IOCD module) installation.
4	pciRiserInstallIndex	.1.3.6.1.4.1.116.5.39.1.9.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPciRiser to identify the table entry.
5	pciRiserInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.89.1.1.2	Integer32	RO	Shows the PCI-e riser card (IOCD module) slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPciRiser–1.
6	pciRiserInstallExist	.1.3.6.1.4.1.116.5.39.1.9.1.1.3	INTEGER	RO	Shows the PCI-e riser card (IOCD module) installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

(h) chassisConfigSystem group (1/2)

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigSystem	.1.3.6.1.4.1.116.5.39.1.10	Not-Accessible	NA	Shows the information on the entire configuration of the server chassis.
2	chassisConfigModel	.1.3.6.1.4.1.116.5.39.1.10.1	Display String	RO	Shows the server chassis model name.
3	chassisConfigChassisType	.1.3.6.1.4.1.116.5.39.1.10.2	Display String	RO	Shows the backplane type of the server chassis.
4	chassisConfigChassisId	.1.3.6.1.4.1.116.5.39.1.10.3	Display String	RO	Shows the server chassis ID.
5	chassisConfigSerialNo o	.1.3.6.1.4.1.116.5.39.1.10.4	Display String	RO	Shows the server chassis serial number.
6	chassisConfigVoltage	.1.3.6.1.4.1.116.5.39.1.10.5	Integer32	RO	Shows the normal input voltage value of the server chassis. This value is shown as 1 for 0.1V.

(h) chassisConfigSystem group (2/2)

No.	Object identifier	OID	Syntax	Access	Description
7	chassisConfigCurrencyType	.1.3.6.1.4.1.116.5.39.1.10.6	INTEGER	RO	Shows the input currency type of the server chassis. One of the following values is shown. 1: AC 2: DC 3: unknown
8	chassisConfigTempUpper	.1.3.6.1.4.1.116.5.39.1.10.7	Integer32	RO	Shows the upper temperature threshold value of inlet air for warning. This value is shown as 1 for 0.1°C.
9	chassisConfigTempLower	.1.3.6.1.4.1.116.5.39.1.10.8	Integer32	RO	Shows the lower temperature threshold value of inlet air for warning. This value is shown as 1 for 0.1°C.
10	chassisConfigCurrentCurrency	.1.3.6.1.4.1.116.5.39.1.10.9	Integer32	RO	Shows the max current consumption value in the current configuration of the server chassis. This value is shown as 1 for 0.1A.
11	chassisConfigCurrentPower	.1.3.6.1.4.1.116.5.39.1.10.10	Integer32	RO	Shows the rated power value in the current configuration of the server chassis. This value is shown as 1 for 0.1kW.
12	chassisConfigMaxCurrency	.1.3.6.1.4.1.116.5.39.1.10.11	Integer32	RO	Shows the max current consumption value in the max configuration of the server chassis. This value is shown as 1 for 0.1A.
13	chassisConfigMaxPower	.1.3.6.1.4.1.116.5.39.1.10.12	Integer32	RO	Shows the rated power value in the max configuration of the server chassis. This value is shown as 1 for 0.1kW.
14	chassisConfigAirVolume	.1.3.6.1.4.1.116.5.39.1.10.13	Integer32	RO	Shows the max air volume value provided by the server chassis. This value is shown as 1 for 0.1m^3/min.
15	chassisConfigHeight	.1.3.6.1.4.1.116.5.39.1.10.14	Integer32	RO	Shows the max air volume value provided by the server chassis. This value is shown as 1 for 1 U.
16	chassisConfigTotalMass	.1.3.6.1.4.1.116.5.39.1.10.15	Integer32	RO	Shows the max air volume value provided by the server chassis. This value is shown as 1 for 0.1kg.
17	chassisConfigLocationId	.1.3.6.1.4.1.116.5.39.1.10.16	Integer32	RO	Shows the location ID for the server chassis.
18	chassisConfigIofGroupId	.1.3.6.1.4.1.116.5.39.1.10.17	Display string	RO	Shows the IOF group ID for the server chassis.

(i) chassisConfigPcieSw group

This item is not supported.

No.	Object identifier	OID	Syntax	Access	Description
1	chassisConfigPcieSw	.1.3.6.1.4.1.116.5.39.1.11	Not-Accessible	NA	Shows the information on PCI Express switch module installation.
2	pcieSwInstallTable	.1.3.6.1.4.1.116.5.39.1.11.1	Not-Accessible	NA	Shows the table of information on PCI Express switch module installation.
3	pcieSwInstallEntry	.1.3.6.1.4.1.116.5.39.1.11.1.1	Not-Accessible	NA	Shows the table entry describing the information on PCI Express switch module installation.
4	pcieSwInstallIndex	.1.3.6.1.4.1.116.5.39.1.11.1.1.1	Integer32	RO	Shows the index value to identify the table entry ranging from 1 to chassisCapacityPcieSw.
5	pcieSwInstallSlotnum	.1.3.6.1.4.1.116.5.39.1.11.1.1.2	Integer32	RO	Shows the PCI Express switch module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPcieSw-1.
6	pcieSwInstallExist	.1.3.6.1.4.1.116.5.39.1.11.1.1.3	INTEGER	RO	Shows the PCI Express switch module installation status in the slot shown in #5. One of the following values is shown. 1: non-exist 2: exist 3: unknown

2 moduleConfig

moduleConfig consists of the following seven groups: moduleConfigBlade, moduleConfigMm, moduleConfigSw, moduleConfigFan, moduleConfigPs, moduleConfigPciRiser, and moduleConfigPcieSw. Each group is described in the following table (a) to (f).

(a) moduleConfigBlade group (1/25)

No.	Object identifier	OID	Syntax	Access	Description
1	moduleConfigBlade	.1.3.6.1.4.1.116.5.39.2.2	Not-Accessible	NA	Shows the information on server blade configuration.
2	bladeInfoTable	.1.3.6.1.4.1.116.5.39.2.2.1	Not-Accessible	NA	Shows the table of information on server blade configuration.
3	bladeInfoEntry	.1.3.6.1.4.1.116.5.39.2.2.1.1	Not-Accessible	NA	Shows the table entry describing the information on server blade installation.
4	bladeInfoIndex	.1.3.6.1.4.1.116.5.39.2.2.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityBlade to identify the table entry.
5	bladeInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.2.1.1.2	Integer32	RO	Shows the server blade slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityBlade–1.
6	bladeInfoProductName	.1.3.6.1.4.1.116.5.39.2.2.1.1.3	Display String	RO	Shows the Product Name of the server blade installed in the slot shown in #5. (*1)
7	bladeInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.2.1.1.4	Display String	RO	Shows the Product Part Model of the server blade installed in the slot shown in #5. (*1)
8	bladeInfoProductVersion	.1.3.6.1.4.1.116.5.39.2.2.1.1.5	Display String	RO	Shows the Product Version of the server blade installed in the slot shown in #5. (*1)
9	bladeInfoProductManufacture	.1.3.6.1.4.1.116.5.39.2.2.1.1.6	Display String	RO	Shows the Product Manufacturer of the server blade installed in the slot shown in #5. (*1)
10	bladeInfoBoardProductName	.1.3.6.1.4.1.116.5.39.2.2.1.1.7	Display String	RO	Shows the Board Product Name of the server blade installed in the slot shown in #5. (*1)
11	bladeInfoBoardSerialNo	.1.3.6.1.4.1.116.5.39.2.2.1.1.8	Display String	RO	Shows the Board Serial Number of the server blade installed in the slot shown in #5. (*1)
12	bladeInfoChassisId	.1.3.6.1.4.1.116.5.39.2.2.1.1.9	Display String	RO	Shows the Chassis ID of the server blade installed in the slot shown in #5. (*2)

(*1) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the data cannot be obtained.

(*2) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the server blade data cannot be obtained. “Not support” is shown as the response in this equipment.

(a) moduleConfigBlade group (2/25)

No.	Object identifier	OID	Syntax	Access	Description
13	bladeInfoChassisSerialNo	.1.3.6.1.4.1.116.5.39.2.2.1.1.10	Display String	RO	Shows the Chassis Serial Number of the server blade installed in the slot shown in #5. (*2)
14	bladeInfoBelongedPartitionNo	.1.3.6.1.4.1.116.5.39.2.2.1.1.11	Integer32	RO	Shows the Partition Number corresponding to the location of this blade slot. (*3)
15	bladeInfoHvmType	.1.3.6.1.4.1.116.5.39.2.2.1.1.12	INTEGER	RO	Shows that the blade supports LPAR manager or is a basic model. One of the following values is shown. 1: basic 2: hvm (support model for LPAR manager) 3: unknown
16	bladeInfoProductSerialNo	.1.3.6.1.4.1.116.5.39.2.2.1.1.13	Display String	RO	Shows the Product Serial Number of the server blade installed in the slot shown in #5. (*1)
17	bladeInfoUuid	.1.3.6.1.4.1.116.5.39.2.2.1.1.14	Display String	RO	Shows UUID (Universal Unique ID) of the server blade installed in the slot shown in #5. (*1)
18	bladeInfoBoardManufacture	.1.3.6.1.4.1.116.5.39.2.2.1.1.15	Display String	RO	Shows the Board Manufacture of the server blade installed in the slot shown in #5. (*1)
19	bladeInfoCapacityCpu	.1.3.6.1.4.1.116.5.39.2.2.1.1.16	Integer32	RO	Shows the max number of processors mounted on the server blade installed in the slot shown in #5. (*4)
20	bladeInfoCapacityIo	.1.3.6.1.4.1.116.5.39.2.2.1.1.17	Integer32	RO	Shows the max number of mezzanine cards mounted on the server blade installed in the slot shown in #5. (*4)
21	bladeInfoVoltage	.1.3.6.1.4.1.116.5.39.2.2.1.1.18	Integer32	RO	Shows the standard voltage value of the server blade. This value is shown using the unit of 0.1V.
22	bladeInfoCurrencyType	.1.3.6.1.4.1.116.5.39.2.2.1.1.19	INTEGER	RO	Shows the current type of the server chassis. One of the following values is shown. 1: AC 2: DC 3: unknown

(*1) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the data cannot be obtained.

(*2) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the server blade data cannot be obtained. “Not support” is shown as the response in this equipment.

(*3) The response is “-1” if no server blade is installed, or if no partition exists.

(*4) The response is “0” if no server blade or no processor is installed.

(a) moduleConfigBlade group (3/25)

No.	Object identifier	OID	Syntax	Access	Description
23	bladeInfoMaxCurrency	.1.3.6.1.4.1.116.5.39.2.2.1.1.20	Integer32	RO	Shows the max current value of the server blade installed in the slot shown in #5. This value is shown using the unit of 0.1A. (*4)(*8)
24	bladeInfoMaxPower	.1.3.6.1.4.1.116.5.39.2.2.1.1.21	Integer32	RO	Shows the rated power value of the server blade installed in the slot shown in #5. This value is shown using the unit of 1W. (*4)(*8)
25	bladeInfoAmbientTempHigher	.1.3.6.1.4.1.116.5.39.2.2.1.1.22	Integer32	RO	Shows the upper temperature threshold value of inlet air for warning to the server blade installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*4)
26	bladeInfoAmbientTempLower	.1.3.6.1.4.1.116.5.39.2.2.1.1.23	Integer32	RO	Shows the lower temperature threshold value of inlet air for warning to the server blade installed in the slot shown in #5. This value is always shown as 0.
27	bladeInfoCPU0TempHigher	.1.3.6.1.4.1.116.5.39.2.2.1.1.24	Integer32	RO	Shows the upper temperature threshold value of CPU for warning in the server blade installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*4)
28	bladeInfoCPU0TempLower	.1.3.6.1.4.1.116.5.39.2.2.1.1.25	Integer32	RO	Shows the lower temperature threshold value of CPU for warning in the server blade installed in the slot shown in #5. This value is always shown as 0.
29	bladeInfoCPU1TempHigher	.1.3.6.1.4.1.116.5.39.2.2.1.1.26	Integer32	RO	Shows the upper temperature threshold value of CPU for warning in the server blade installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*4)
30	bladeInfoCPU1TempLower	.1.3.6.1.4.1.116.5.39.2.2.1.1.27	Integer32	RO	Shows the lower temperature threshold value of CPU for warning in the server blade installed in the slot shown in #5. This value is always shown as 0.

(*1) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the data cannot be obtained.

(*2) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the server blade data cannot be obtained. “Not support” is shown as the response in this equipment.

(*3) The response is “-1” if no server blade is installed, or if no partition exists.

(*4) The response is “0” if no server blade or no processor is installed.

(*8) With SMP configuration, when the primary blade location is specified in a partition, the values of the entire partition are displayed; when a blade location other than the primary one is specified, “0” is displayed.

(a) moduleConfigBlade group (4/25)

No.	Object identifier	OID	Syntax	Access	Description
31	bladeInfoMass	.1.3.6.1.4.1.116.5.39.2.2.1.1.28	Integer32	RO	Shows the mass of the server blade installed in the slot shown in #5. This is shown using the unit of 0.1kg. (*4)
32	bladeInfoFanRpm	.1.3.6.1.4.1.116.5.39.2.2.1.1.29	Integer32	RO	Shows the max revolutions per minute (rpm) value of the fan in the server blade. This value is always shown as 0.
33	bladeInfoFanAirVolume	.1.3.6.1.4.1.116.5.39.2.2.1.1.30	Integer32	RO	Shows the max air volume value provided by the fan in the server blade. This value is always shown as 0.
34	bladeInfoDetailHvmLicense	.1.3.6.1.4.1.116.5.39.2.2.1.1.31	DisplayString	RO	Shows the detailed LPAR manager license value given to the server blade installed in the slot shown in #5. (*9)
35	bladeInfoCapacityDimm	.1.3.6.1.4.1.116.5.39.2.2.1.1.32	Integer32	RO	Shows the max number of DIMM slots to be installed in a server blade.
36	bladeInfoDimmRedundancy	.1.3.6.1.4.1.116.5.39.2.2.1.1.33	INTEGER	RO	Shows redundancy settings of DIMM in the server blade. One of the following values is shown. (*10) 1: non-redundancy 2: unknown 3: memory-mirroring 4: online-spared-memory
37	bladeInfoTotalAmountOfDimm	.1.3.6.1.4.1.116.5.39.2.2.1.1.34	Integer32	RO	Shows the max amount of DIMM available for a server blade. This value is shown as 1 for 1 GB. (*11)
38	bladeInfoManagementIpAddress	.1.3.6.1.4.1.116.5.39.2.2.1.1.35	DisplayString	RO	Shows the IP address of management port of server blade of the slot shown in #5.
39	bladeInfoCpuInfoTable	1.3.6.1.4.1.116.5.39.2.2.2	Not-Accessible	NA	Show the information table on the processor installed in the server blade.
40	bladeInfoCpuInfoEntry	.1.3.6.1.4.1.116.5.39.2.2.2.1	Not-Accessible	NA	Shows the entry of the information table on the processor installed in the server blade.
41	bladeInfoCpuInfoIndex	.1.3.6.1.4.1.116.5.39.2.2.2.1.1	Integer32	RO	Shows the index of the information table on the processor installed in the server blade.

(*9) “Not install” is shown if no server blade installed or LPAR manager license not given to the server blade,.

(*10) “Unknown” is shown if no information is obtained or no server blade is installed. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(*11) “0” is shown if no information is obtained or no server blade is installed.

(a) moduleConfigBlade group (5/25)

No.	Object identifier	OID	Syntax	Access	Description
42	bladeInfoCpuInfo1SlotNum	.1.3.6.1.4.1.116.5.39.2.2.1.2	Integer32	RO	Shows the slot number of the first processor installed in the server blade in the slot shown in #5. This value is always 0.
43	bladeInfoCpuInfo1Exist	.1.3.6.1.4.1.116.5.39.2.2.1.3	INTEGER	RO	Shows the status of the first processor installed in the server blade in the slot shown in #5. (*5) 1. non-exist 2. exist 3. unknown
44	bladeInfoCpuInfo1CoreNum	.1.3.6.1.4.1.116.5.39.2.2.1.4	Integer32	RO	Shows the core number of the first processor installed in the server blade in the slot shown in #5. (*4)
45	bladeInfoCpuInfo1CpuName	.1.3.6.1.4.1.116.5.39.2.2.1.5	Display String	RO	Shows the name of the first processor installed in the server blade in the slot shown in #5. (*6)
46	bladeInfoCpuInfo1CpuFrequency	.1.3.6.1.4.1.116.5.39.2.2.1.6	Integer32	RO	Shows the frequency of the first processor installed in the server blade in the slot shown in #5. This value is shown as 1 for 1MHz. (*4)
47	bladeInfoCpuInfo1CpuStepping	.1.3.6.1.4.1.116.5.39.2.2.1.7	Display String	RO	Shows the stepping of the first processor installed in the server blade in the slot shown in #5. (*6)
48	bladeInfoCpuInfo2SlotNum	.1.3.6.1.4.1.116.5.39.2.2.1.8	Integer32	RO	Shows the slot number of the second processor installed in the server blade in the slot shown in #5. This value is 1 (one).
49	bladeInfoCpuInfo2Exist	.1.3.6.1.4.1.116.5.39.2.2.1.9	INTEGER	RO	Shows the status of the second processor installed in the server blade in the slot shown in #5. (*5) 1. non-exist 2. exist 3. unknown

(*4) The response is “0” if no server blade or no processor is installed.

(*5) The response is “3” if no server blade is installed or if the server blade data cannot be obtained.
The response is “1” if no server blade is installed or if no processor is installed in the server blade.
The response is “1” if no server blade is installed or if no mezzanine card is installed in the server blade.

(*6) “Not install” is shown if no server blade or no processor in the server blade is installed.
“Cannot get data” is shown if the processor data cannot be obtained.

(a) moduleConfigBlade group (6/25)

No	Object identifier	OID	Syntax	Access	Description
50	bladeInfoCpuInfo2CoreNum	.1.3.6.1.4.1.116.5.39.2.2.2.1.10	Integer32	RO	Shows the core number of the second processor installed in the server blade in the slot shown in #5. (*1)
51	bladeInfoCpuInfo2CpuName	.1.3.6.1.4.1.116.5.39.2.2.2.1.11	Display String	RO	Shows the name of the second processor installed in the server blade in the slot shown in #5. (*6)
52	bladeInfoCpuInfo2CpuFrequency	.1.3.6.1.4.1.116.5.39.2.2.2.1.12	Integer32	RO	Shows the frequency of the second processor installed in the server blade in the slot shown in #5. This value is shown as 1 for 1MHz. (*4)
53	bladeInfoCpuInfo2CpuStepping	.1.3.6.1.4.1.116.5.39.2.2.2.1.13	Display String	RO	Shows the stepping of the second processor installed in the server blade in the slot shown in #5. (*6)
54	bladeInfoIoInfoTable	.1.3.6.1.4.1.116.5.39.2.2. 3	Not-Accessible	NA	Shows the information table on the mezzanine card installed in the server blade shown in #5.
55	bladeInfoIoInfoEntry	.1.3.6.1.4.1.116.5.39.2.2.3.1	Not-Accessible	NA	Shows the entry of the information table on the mezzanine card installed in the server blade shown in #5.
56	bladeInfoIoInfoIndex	.1.3.6.1.4.1.116.5.39.2.2.3.1.1	Integer32	RO	Shows the index of the information table on the mezzanine card installed in the server blade shown in #5.
57	bladeInfoIoInfo1SlotNum	.1.3.6.1.4.1.116.5.39.2.2.3.1.2	Integer32	RO	Shows the slot number of the first mezzanine card installed in the server blade in the slot shown in #5. This value is always 0.
58	bladeInfoIoInfo1Exist	.1.3.6.1.4.1.116.5.39.2.2.3.1.3	INTEGER	RO	Shows the status of the mezzanine card in the first slot of the server blade in the slot shown in #5. (*5) 1. non-exist 2. exist 3. unknown

(*1) “Not install” is shown if no server blade is installed; “Cannot get data” is shown if the data cannot be obtained.

(*4) The response is “0” if no server blade or no processor is installed.

(*5) The response is “3” if no server blade is installed, or if the server blade data cannot be obtained.
The response is “1” if no server blade is installed, or if no processor is installed in the server blade.
The response is “1” if no server blade is installed, or if no mezzanine card is installed in the server blade.

(*6) “Not install” is shown if no server blade or no processor in the server blade is installed; “Cannot get data” is shown if the processor data cannot be obtained.

(a) moduleConfigBlade group (7/25)

No	Object identifier	OID	Syntax	Access	Description
59	bladeInfoIoIn fo1ProductN ame	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.4	Display String	RO	Shows the Product Name of the mezzanine card installed in the first slot in the server blade in the slot shown in #5. (*7)
60	bladeInfoIoIn fo1ProductM odel	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.5	Display String	RO	Shows the Product Model of the mezzanine card installed in the first slot in the server blade in the slot shown in #5. (*7)
61	bladeInfoIoIn fo1ProductV ersion	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.6	Display String	RO	Shows the Product Version of the mezzanine card installed in the first slot in the server blade in the slot shown in #5. (*7)
62	bladeInfoIoIn fo1ProductM anufacture	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.7	Display String	RO	Shows the Product Manufacture of the mezzanine card installed in the first slot in the server blade in the slot shown in #5. (*9)
63	bladeInfoIoIn fo2SlotNum	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.8	Integer32	RO	Shows the slot number of the second mezzanine card in the second slot of the server blade in the slot shown in #5. This value is always 1.
64	bladeInfoIoIn fo2Exist	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.9	INTEGER	RO	Shows the status of the mezzanine card in the second slot in the server blade in the slot shown in #5. (*8) 1. non-exist 2. exist 3. unknown
65	bladeInfoIoIn fo2ProductN ame	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.10	Display String	RO	Shows the Product Name of the mezzanine card installed in the send slot in the server blade in the slot shown in #5. (*7)
66	bladeInfoIoIn fo2ProductM odel	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.11	Display String	RO	Shows the Product Model of the mezzanine card installed in the second slot in the server blade in the slot shown in #5. (*7)
67	bladeInfoIoIn fo2ProductV ersion	.1.3.6.1.4.1 .116.5.39.2 .2.3.1.12	Display String	RO	Shows the Product Version of the mezzanine card installed in the second slot in the server blade in the slot shown in #5. (*7)

(*7) “Not install” is shown if no server blade or no mezzanine card in the server blade is installed; “Cannot get data” is shown if the processor mezzanine card data cannot be obtained.

(*8) With SMP configuration, when the primary blade location is specified in a partition, the values of the entire partition are displayed; when a blade location other than the primary one is specified, “0” is displayed.

(*9) “Not install” is shown if no server blade installed or LPAR manager license not given to the server blade,.

(a) moduleConfigBlade group (8/25)

No	Object identifier	OID	Syntax	Access	Description
68	bladeInfoIoInfo2ProductManufacture	.1.3.6.1.4.1.116.5.39.2.2.3.1.13	Display String	RO	Shows the Product Manufacture of the mezzanine card installed in the second slot in the server blade in the slot shown in #5. (*7)
69	bladeInfoDimmInfoTable	.1.3.6.1.4.1.116.5.39. 2.2.4	Not-Accessible	NA	Show the information table on DIMM installed in the server blade.
70	bladeInfoDimmInfoEntry	.1.3.6.1.4.1.116.5.39. 2.2.4.1	Not-Accessible	NA	Show the entry of the information table on DIMM installed in the server blade.
71	bladeInfoDimmInfoIndex	.1.3.6.1.4.1.116.5.39.2.2.4.1.1	Integer32	RO	Show the index of the information table on DIMM installed in the server blade.
72	bladeInfoDimmInfo1Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.2	INTEGER	RO	Shows the status of DIMM installed in the first slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
73	bladeInfoDimmInfo1Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.3	Integer32	RO	Shows the capacity of DIMM installed in the first slot of the server blade. This value is shown as 1 for 1 GB. (*13)
74	bladeInfoDimmInfo1Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.4	Display String	RO	Shows the type of DIMM installed in the first slot of the server blade. (*14)
75	bladeInfoDimmInfo1Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.5	Integer32	RO	Shows the frequency of DIMM installed in the first slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
76	bladeInfoDimmInfo1CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.6	Integer32	RO	Shows the column address strobe (CAS) latency of DIMM installed in the first slot of the server blade. (*13)

(*7) “Not install” is shown if no server blade or no mezzanine card in the server blade is installed; “Cannot get data” is shown if the processor mezzanine card data cannot be obtained.

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (9/25)

No	Object identifier	OID	Syntax	Access	Description
77	bladeInfoDimmInfo2Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.7	INTEGER	RO	Shows the status of DIMM installed in the second slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
78	bladeInfoDimmInfo2Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.8	Integer32	RO	Shows the capacity of DIMM installed in the second slot of the server blade. This value is shown as 1 for 1 GB. (*13)
79	bladeInfoDimmInfo2Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.9	Display String	RO	Shows the type of DIMM installed in the second slot of the server blade. (*14)
80	bladeInfoDimmInfo2Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.10	Integer32	RO	Shows the frequency of DIMM installed in the second slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
81	bladeInfoDimmInfo2CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.11	Integer32	RO	Shows the CAS latency of DIMM installed in the second slot of the server blade. (*13)
82	bladeInfoDimmInfo3Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.12	INTEGER	RO	Shows the status of DIMM installed in the third slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
83	bladeInfoDimmInfo3Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.13	Integer32	RO	Shows the capacity of DIMM installed in the third slot of the server blade. This value is shown as 1 for 1 GB. (*13)
84	bladeInfoDimmInfo3Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.14	Display String	RO	Shows the type of DIMM installed in the third slot of the server blade. (*14)
85	bladeInfoDimmInfo3Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.15	Integer32	RO	Shows the frequency of DIMM installed in the third slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
86	bladeInfoDimmInfo3CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.16	Integer32	RO	Shows the CAS latency of DIMM installed in the third slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (10/25)

No	Object identifier	OID	Syntax	Access	Description
87	bladeInfoDimmInfo4Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.17	INTEGER	RO	Shows the status of DIMM installed in the 4th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
88	bladeInfoDimmInfo4Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.18	Integer32	RO	Shows the capacity of DIMM installed in the 4th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
89	bladeInfoDimmInfo4Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.19	Display String	RO	Shows the type of DIMM installed in the 4th slot of the server blade. (*14)
90	bladeInfoDimmInfo4Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.20	Integer32	RO	Shows the frequency of DIMM installed in the 4th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
91	bladeInfoDimmInfo4CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.21	Integer32	RO	Shows the CAS latency of DIMM installed in the 4th slot of the server blade. (*13)
92	bladeInfoDimmInfo5Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.22	INTEGER	RO	Shows the status of DIMM installed in the 5th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
93	bladeInfoDimmInfo5Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.23	Integer32	RO	Shows the capacity of DIMM installed in the 5th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
94	bladeInfoDimmInfo5Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.24	Display String	RO	Shows the type of DIMM installed in the 5th slot of the server blade. (*14)
95	bladeInfoDimmInfo5Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.25	Integer32	RO	Shows the frequency of DIMM installed in the 5th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
96	bladeInfoDimmInfo5CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.26	Integer32	RO	Shows the CAS latency of DIMM installed in the 5th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (11/25)

No	Object identifier	OID	Syntax	Access	Description
97	bladeInfoDimmInfo6Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.27	INTEGER	RO	Shows the status of DIMM installed in the 6th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
98	bladeInfoDimmInfo6Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.28	Integer32	RO	Shows the capacity of DIMM installed in the 6th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
99	bladeInfoDimmInfo6Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.29	Display String	RO	Shows the type of DIMM installed in the 6th slot of the server blade. (*14)
100	bladeInfoDimmInfo6Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.30	Integer32	RO	Shows the frequency of DIMM installed in the 6th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
101	bladeInfoDimmInfo6CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.31	Integer32	RO	Shows the CAS latency of DIMM installed in the 6th slot of the server blade. (*13)
102	bladeInfoDimmInfo7Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.32	INTEGER	RO	Shows the status of DIMM installed in the 7th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
103	bladeInfoDimmInfo7Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.33	Integer32	RO	Shows the capacity of DIMM installed in the 7th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
104	bladeInfoDimmInfo7Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.34	Display String	RO	Shows the type of DIMM installed in the 7th slot of the server blade. (*14)
105	bladeInfoDimmInfo7Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.35	Integer32	RO	Shows the frequency of DIMM installed in the 7th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
106	bladeInfoDimmInfo7CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.36	Integer32	RO	Shows the CAS latency of DIMM installed in the 7th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (12/25)

No	Object identifier	OID	Syntax	Access	Description
107	bladeInfoDimmInfo8Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.37	INTEGER	RO	Shows the status of DIMM installed in the 8th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
108	bladeInfoDimmInfo8Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.38	Integer32	RO	Shows the capacity of DIMM installed in the 8th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
109	bladeInfoDimmInfo8Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.39	Display String	RO	Shows the type of DIMM installed in the 8th slot of the server blade. (*14)
110	bladeInfoDimmInfo8Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.40	Integer32	RO	Shows the frequency of DIMM installed in the 8th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
111	bladeInfoDimmInfo8CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.41	Integer32	RO	Shows the CAS latency of DIMM installed in the 8th slot of the server blade. (*13)
112	bladeInfoDimmInfo9Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.42	INTEGER	RO	Shows the status of DIMM installed in the 9th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
113	bladeInfoDimmInfo9Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.43	Integer32	RO	Shows the capacity of DIMM installed in the 9th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
114	bladeInfoDimmInfo9Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.44	Display String	RO	Shows the type of DIMM installed in the 9th slot of the server blade. (*14)
115	bladeInfoDimmInfo9Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.45	Integer32	RO	Shows the frequency of DIMM installed in the 9th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
116	bladeInfoDimmInfo9CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.46	Integer32	RO	Shows the CAS latency of DIMM installed in the 9th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (13/25)

No	Object identifier	OID	Syntax	Access	Description
117	bladeInfoDimmInfo10Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.47	INTEGER	RO	Shows the status of DIMM installed in the 10th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
118	bladeInfoDimmInfo10Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.48	Integer32	RO	Shows the capacity of DIMM installed in the 10th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
119	bladeInfoDimmInfo10Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.49	Display String	RO	Shows the type of DIMM installed in the 10th slot of the server blade. (*14)
120	bladeInfoDimmInfo10Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.50	Integer32	RO	Shows the frequency of DIMM installed in the 10th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
121	bladeInfoDimmInfo10CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.51	Integer32	RO	Shows the CAS latency of DIMM installed in the 10th slot of the server blade. (*13)
122	bladeInfoDimmInfo11Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.52	INTEGER	RO	Shows the status of DIMM installed in the 11th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
123	bladeInfoDimmInfo11Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.53	Integer32	RO	Shows the capacity of DIMM installed in the 11th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
124	bladeInfoDimmInfo11Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.54	Display String	RO	Shows the type of DIMM installed in the 11th slot of the server blade. (*14)
125	bladeInfoDimmInfo11Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.55	Integer32	RO	Shows the frequency of DIMM installed in the 11th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
126	bladeInfoDimmInfo11CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.56	Integer32	RO	Shows the CAS latency of DIMM installed in the 11th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (14/25)

No	Object identifier	OID	Syntax	Access	Description
127	bladeInfoDimmInfo12Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.57	INTEGER	RO	Shows the status of DIMM installed in the 12th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
128	bladeInfoDimmInfo12Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.58	Integer32	RO	Shows the capacity of DIMM installed in the 12th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
129	bladeInfoDimmInfo12Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.59	Display String	RO	Shows the type of DIMM installed in the 12th slot of the server blade. (*14)
130	bladeInfoDimmInfo12Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.60	Integer32	RO	Shows the frequency of DIMM installed in the 12th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
131	bladeInfoDimmInfo12CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.61	Integer32	RO	Shows the CAS latency of DIMM installed in the 12th slot of the server blade. (*13)
132	bladeInfoDimmInfo13Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.62	INTEGER	RO	Shows the status of DIMM installed in the 13th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
133	bladeInfoDimmInfo13Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.63	Integer32	RO	Shows the capacity of DIMM installed in the 13th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
134	bladeInfoDimmInfo13Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.64	Display String	RO	Shows the type of DIMM installed in the 13th slot of the server blade. (*14)
135	bladeInfoDimmInfo13Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.65	Integer32	RO	Shows the frequency of DIMM installed in the 13th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
136	bladeInfoDimmInfo13CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.66	Integer32	RO	Shows the CAS latency of DIMM installed in the 13th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (15/25)

No	Object identifier	OID	Syntax	Access	Description
137	bladeInfoDimmInfo14Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.67	INTEGER	RO	Shows the status of DIMM installed in the 14th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
138	bladeInfoDimmInfo14Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.68	Integer32	RO	Shows the capacity of DIMM installed in the 14th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
139	bladeInfoDimmInfo14Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.69	Display String	RO	Shows the type of DIMM installed in the 14th slot of the server blade. (*14)
140	bladeInfoDimmInfo14Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.70	Integer32	RO	Shows the frequency of DIMM installed in the 14th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
141	bladeInfoDimmInfo14CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.71	Integer32	RO	Shows the CAS latency of DIMM installed in the 14th slot of the server blade. (*13)
142	bladeInfoDimmInfo15Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.72	INTEGER	RO	Shows the status of DIMM installed in the 15th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
143	bladeInfoDimmInfo15Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.73	Integer32	RO	Shows the capacity of DIMM installed in the 15th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
144	bladeInfoDimmInfo15Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.74	Display String	RO	Shows the type of DIMM installed in the 15th slot of the server blade. (*14)
145	bladeInfoDimmInfo15Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.75	Integer32	RO	Shows the frequency of DIMM installed in the 15th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
146	bladeInfoDimmInfo15CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.76	Integer32	RO	Shows the CAS latency of DIMM installed in the 15th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (16/25)

No	Object identifier	OID	Syntax	Access	Description
147	bladeInfoDimmInfo16Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.77	INTEGER	RO	Shows the status of DIMM installed in the 16th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
148	bladeInfoDimmInfo16Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.78	Integer32	RO	Shows the capacity of DIMM installed in the 16th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
149	bladeInfoDimmInfo16Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.79	Display String	RO	Shows the type of DIMM installed in the 16th slot of the server blade. (*14)
150	bladeInfoDimmInfo16Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.80	Integer32	RO	Shows the frequency of DIMM installed in the 16th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
151	bladeInfoDimmInfo16CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.81	Integer32	RO	Shows the CAS latency of DIMM installed in the 16th slot of the server blade. (*13)
152	bladeInfoDimmInfo17Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.82	INTEGER	RO	Shows the status of DIMM installed in the 17th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
153	bladeInfoDimmInfo17Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.83	Integer32	RO	Shows the capacity of DIMM installed in the 17th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
154	bladeInfoDimmInfo17Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.84	Display String	RO	Shows the type of DIMM installed in the 17th slot of the server blade. (*14)
155	bladeInfoDimmInfo17Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.85	Integer32	RO	Shows the frequency of DIMM installed in the 17th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
156	bladeInfoDimmInfo17CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.86	Integer32	RO	Shows the CAS latency of DIMM installed in the 17th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (17/25)

No	Object identifier	OID	Syntax	Access	Description
157	bladeInfoDimmInfo18Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.87	INTEGER	RO	Shows the status of DIMM installed in the 18th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
158	bladeInfoDimmInfo18Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.88	Integer32	RO	Shows the capacity of DIMM installed in the 18th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
159	bladeInfoDimmInfo18Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.89	Display String	RO	Shows the type of DIMM installed in the 18th slot of the server blade. (*14)
160	bladeInfoDimmInfo18Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.90	Integer32	RO	Shows the frequency of DIMM installed in the 18th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
161	bladeInfoDimmInfo18CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.91	Integer32	RO	Shows the CAS latency of DIMM installed in the 18th slot of the server blade. (*13)
162	bladeInfoDimmInfo19Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.92	INTEGER	RO	Shows the status of DIMM installed in the 19th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
163	bladeInfoDimmInfo19Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.93	Integer32	RO	Shows the capacity of DIMM installed in the 19th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
164	bladeInfoDimmInfo19Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.94	Display String	RO	Shows the type of DIMM installed in the 19th slot of the server blade. (*14)
165	bladeInfoDimmInfo19Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.95	Integer32	RO	Shows the frequency of DIMM installed in the 19th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
166	bladeInfoDimmInfo19CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.96	Integer32	RO	Shows the CAS latency of DIMM installed in the 19th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (18/25)

No	Object identifier	OID	Syntax	Access	Description
167	bladeInfoDimmInfo20Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.97	INTEGER	RO	Shows the status of DIMM installed in the 20th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
168	bladeInfoDimmInfo20Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.98	Integer32	RO	Shows the capacity of DIMM installed in the 20th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
169	bladeInfoDimmInfo20Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.99	Display String	RO	Shows the type of DIMM installed in the 20th slot of the server blade. (*14)
170	bladeInfoDimmInfo20Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.100	Integer32	RO	Shows the frequency of DIMM installed in the 20th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
171	bladeInfoDimmInfo20CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.101	Integer32	RO	Shows the CAS latency of DIMM installed in the 20th slot of the server blade. (*13)
172	bladeInfoDimmInfo21Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.102	INTEGER	RO	Shows the status of DIMM installed in the 21st slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
173	bladeInfoDimmInfo21Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.103	Integer32	RO	Shows the capacity of DIMM installed in the 21st slot of the server blade. This value is shown as 1 for 1 GB. (*13)
174	bladeInfoDimmInfo21Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.104	Display String	RO	Shows the type of DIMM installed in the 21st slot of the server blade. (*14)
175	bladeInfoDimmInfo21Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.105	Integer32	RO	Shows the frequency of DIMM installed in the 21st slot of the server blade. This value is shown as 1 fo 1 Mhz. (*13)
176	bladeInfoDimm Info21CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.106	Integer32	RO	Shows the CAS latency of DIMM installed in the 21st slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (19/25)

No	Object identifier	OID	Syntax	Access	Description
177	bladeInfoDimmInfo22Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.107	INTEGER	RO	Shows the status of DIMM installed in the 22nd slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
178	bladeInfoDimmInfo22Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.108	Integer32	RO	Shows the capacity of DIMM installed in the 22nd slot of the server blade. This value is shown as 1 for 1 GB. (*13)
179	bladeInfoDimmInfo22Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.109	Display String	RO	Shows the type of DIMM installed in the 22nd slot of the server blade. (*14)
180	bladeInfoDimmInfo22Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.110	Integer32	RO	Shows the frequency of DIMM installed in the 22nd slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
181	bladeInfoDimmInfo22CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.111	Integer32	RO	Shows the CAS latency of DIMM installed in the 22nd slot of the server blade. (*13)
182	bladeInfoDimmInfo23Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.112	INTEGER	RO	Shows the status of DIMM installed in the 23rd slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
183	bladeInfoDimmInfo23Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.113	Integer32	RO	Shows the capacity of DIMM installed in the 23rd slot of the server blade. This value is shown as 1 for 1 GB. (*13)
184	bladeInfoDimmInfo23Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.114	Display String	RO	Shows the type of DIMM installed in the 23rd slot of the server blade. (*14)
185	bladeInfoDimmInfo23Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.115	Integer32	RO	Shows the frequency of DIMM installed in the 23rd slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
186	bladeInfoDimmInfo23CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.116	Integer32	RO	Shows the CAS latency of DIMM installed in the 23rd slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (20/25)

No	Object identifier	OID	Syntax	Access	Description
187	bladeInfoDimmInfo24Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.117	INTEGER	RO	Shows the status of DIMM installed in the 24th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
188	bladeInfoDimmInfo24Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.118	Integer32	RO	Shows the capacity of DIMM installed in the 24th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
189	bladeInfoDimmInfo24Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.119	Display String	RO	Shows the type of DIMM installed in the 24th slot of the server blade. (*14)
190	bladeInfoDimmInfo24Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.120	Integer32	RO	Shows the frequency of DIMM installed in the 24th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
191	bladeInfoDimmInfo24CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.121	Integer32	RO	Shows the CAS latency of DIMM installed in the 24th slot of the server blade. (*13)
192	bladeInfoDimmInfo25Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.122	INTEGER	RO	Shows the status of DIMM installed in the 25th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
193	bladeInfoDimmInfo25Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.123	Integer32	RO	Shows the capacity of DIMM installed in the 25th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
194	bladeInfoDimmInfo25Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.124	Display String	RO	Shows the type of DIMM installed in the 25th slot of the server blade. (*14)
195	bladeInfoDimmInfo25Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.125	Integer32	RO	Shows the frequency of DIMM installed in the 25th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
196	bladeInfoDimmInfo25CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.126	Integer32	RO	Shows the CAS latency of DIMM installed in the 25th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (21/25)

No	Object identifier	OID	Syntax	Access	Description
197	bladeInfoDimmInfo26Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.127	INTEGER	RO	Shows the status of DIMM installed in the 26th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
198	bladeInfoDimmInfo26Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.128	Integer32	RO	Shows the capacity of DIMM installed in the 26th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
199	bladeInfoDimmInfo26Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.129	Display String	RO	Shows the type of DIMM installed in the 26th slot of the server blade. (*14)
200	bladeInfoDimmInfo26Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.130	Integer32	RO	Shows the frequency of DIMM installed in the 26th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
201	bladeInfoDimmInfo26CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.131	Integer32	RO	Shows the CAS latency of DIMM installed in the 26th slot of the server blade. (*13)
202	bladeInfoDimmInfo27Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.132	INTEGER	RO	Shows the status of DIMM installed in the 27th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
203	bladeInfoDimmInfo27Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.133	Integer32	RO	Shows the capacity of DIMM installed in the 27th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
204	bladeInfoDimmInfo27Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.134	Display String	RO	Shows the type of DIMM installed in the 27th slot of the server blade. (*14)
205	bladeInfoDimmInfo27Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.135	Integer32	RO	Shows the frequency of DIMM installed in the 27th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
206	bladeInfoDimmInfo27CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.136	Integer32	RO	Shows the CAS latency of DIMM installed in the 27th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (22/25)

No	Object identifier	OID	Syntax	Access	Description
207	bladeInfoDimmInfo28Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.137	INTEGER	RO	Shows the status of DIMM installed in the 28th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
208	bladeInfoDimmInfo28Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.138	Integer32	RO	Shows the capacity of DIMM installed in the 28th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
209	bladeInfoDimmInfo28Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.139	Display String	RO	Shows the type of DIMM installed in the 28th slot of the server blade. (*14)
210	bladeInfoDimmInfo28Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.140	Integer32	RO	Shows the frequency of DIMM installed in the 28th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
211	bladeInfoDimmInfo28CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.141	Integer32	RO	Shows the CAS latency of DIMM installed in the 28th slot of the server blade. (*13)
212	bladeInfoDimmInfo29Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.142	INTEGER	RO	Shows the status of DIMM installed in the 29th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
213	bladeInfoDimmInfo29Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.143	Integer32	RO	Shows the capacity of DIMM installed in the 29th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
214	bladeInfoDimmInfo29Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.144	Display String	RO	Shows the type of DIMM installed in the 29th slot of the server blade. (*14)
215	bladeInfoDimmInfo29Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.145	Integer32	RO	Shows the frequency of DIMM installed in the 29th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
216	bladeInfoDimmInfo29CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.146	Integer32	RO	Shows the CAS latency of DIMM installed in the 29th slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (23/25)

No	Object identifier	OID	Syntax	Access	Description
217	bladeInfoDimmInfo30Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.147	INTEGER	RO	Shows the status of DIMM installed in the 30th slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
218	bladeInfoDimmInfo30Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.148	Integer32	RO	Shows the capacity of DIMM installed in the 30th slot of the server blade. This value is shown as 1 for 1 GB. (*13)
219	bladeInfoDimmInfo30Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.149	Display String	RO	Shows the type of DIMM installed in the 30th slot of the server blade. (*14)
220	bladeInfoDimmInfo30Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.150	Integer32	RO	Shows the frequency of DIMM installed in the 30th slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
221	bladeInfoDimmInfo30CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.151	Integer32	RO	Shows the CAS latency of DIMM installed in the 30th slot of the server blade. (*13)
222	bladeInfoDimmInfo31Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.152	INTEGER	RO	Shows the status of DIMM installed in the 31st slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
223	bladeInfoDimmInfo31Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.153	Integer32	RO	Shows the capacity of DIMM installed in the 31st slot of the server blade. This value is shown as 1 for 1 GB. (*13)
224	bladeInfoDimmInfo31Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.154	Display String	RO	Shows the type of DIMM installed in the 31st slot of the server blade. (*14)
225	bladeInfoDimmInfo31Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.155	Integer32	RO	Shows the frequency of DIMM installed in the 31st slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
226	bladeInfoDimmInfo31CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.156	Integer32	RO	Shows the CAS latency of DIMM installed in the 31st slot of the server blade. (*13)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (24/25)

No	Object identifier	OID	Syntax	Access	Description
227	bladeInfoDimmInfo32Exist	.1.3.6.1.4.1.116.5.39.2.2.4.1.157	INTEGER	RO	Shows the status of DIMM installed in the 32nd slot of the server blade. One of the following values is shown. (*12) 1: exist 2: non-exist 3: unknown
228	bladeInfoDimmInfo32Capacity	.1.3.6.1.4.1.116.5.39.2.2.4.1.158	Integer32	RO	Shows the capacity of DIMM installed in the 32nd slot of the server blade. This value is shown as 1 for 1 GB. (*13)
229	bladeInfoDimmInfo32Type	.1.3.6.1.4.1.116.5.39.2.2.4.1.159	Display String	RO	Shows the type of DIMM installed in the 32nd slot of the server blade. (*14)
230	bladeInfoDimmInfo32Frequency	.1.3.6.1.4.1.116.5.39.2.2.4.1.160	Integer32	RO	Shows the frequency of DIMM installed in the 32nd slot of the server blade. This value is shown as 1 for 1 Mhz. (*13)
231	bladeInfoDimmInfo32CasLatency	.1.3.6.1.4.1.116.5.39.2.2.4.1.161	Integer32	RO	Shows the CAS latency of DIMM installed in the 32nd slot of the server blade. (*13)
232	bladeInfoFwInfoTable	.1.3.6.1.4.1.116.5.39.2.2.5	Not-Accessible	NA	Shows the information table of the firmware version on the server blade.
233	bladeInfoFwInfoEntry	.1.3.6.1.4.1.116.5.39.2.2.5.1	Not-Accessible	NA	Shows the entry of the information table on the server blade.
234	bladeInfoFwInfoIndex	.1.3.6.1.4.1.116.5.39.2.2.5.1.1	Integer32	RO	Shows the index of the information table on the server blade.
235	bladeInfoFwActBmcVersion	.1.3.6.1.4.1.116.5.39.2.2.5.1.2	Display String	RO	Shows the BMC firmware version currently used on the server blade. (*15)
236	bladeInfoFwAltBmcVersion	.1.3.6.1.4.1.116.5.39.2.2.5.1.3	Display String	RO	Shows the BMC firmware version currently not used on the server blade. (*15)
237	bladeInfoFwActEfiBiosVersion	.1.3.6.1.4.1.116.5.39.2.2.5.1.4	Display String	RO	Shows the BMC/EFI firmware versions currently used on the server blade. (*15)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(*15) “Not install” is shown if no server blade or no firmware is installed. “Cannot get data” is shown if no information is obtained.

(a) moduleConfigBlade group (25/25)

No	Object identifier	OID	Syntax	Access	Description
238	bladeInfoFwAltEfiBiosVersion	1.3.6.1.4.1.116.5.39.2.2.5.1.5	Display String	RO	Shows the BMC/EFI firmware versions currently not used on the server blade. (*15)
239	bladeInfoFwActHvmVersion	.1.3.6.1.4.1.116.5.39.2.2.5.1.6	Display String	RO	Shows the LPAR manager firmware version currently used on the server blade. (*15)
240	bladeInfoFwAltHvmVersion	.1.3.6.1.4.1.116.5.39.2.2.5.1.7	Display String	RO	Shows the LPAR manager firmware version currently not used on the server blade. (*15)

(*12) “non-exist” is shown if no server blade or no DIMM is installed. “unknown” is shown if no information is obtained.

(*13) “0” is shown if no information is obtained, or if no server blade or no DIMM is installed.

(*14) “Not install” is shown if no server blade or no DIMM is installed. “Cannot get data” is shown if no information is obtained.

(*15) “Not install” is shown if no server blade or no firmware is installed. “Cannot get data” is shown if no information is obtained.

(b) moduleConfigMm group (1/3)

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigMm	.1.3.6.1.4.1.116.5.39.2.3	Not-Accessible	NA	Shows the information on management module configuration.
2	mmInfoTable	.1.3.6.1.4.1.116.5.39.2.3.1	Not-Accessible	NA	Shows the table of information on management module installation.
3	mmInfoEntry	.1.3.6.1.4.1.116.5.39.2.3.1.1	Not-Accessible	NA	Shows the table entry describing the information on management module installation.
4	mmInfoIndex	.1.3.6.1.4.1.116.5.39.2.3.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMm to identify the table entry.
5	mmInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.3.1.1.2	Integer32	RO	Shows the management module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityMm–1.
6	mmInfoProductName	.1.3.6.1.4.1.116.5.39.2.3.1.1.3	Display String	RO	Shows the Product Name of the management module of the server blade in the slot shown in #5. (*1)
7	mmInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.3.1.1.4	Display String	RO	Shows the Product Part Model of the management module of the server blade in the slot shown in #5. (*1)
8	mmInfoProductPartModel2	.1.3.6.1.4.1.116.5.39.2.3.1.1.5	Display String	RO	Shows the Product Part Model2 of the management module of the server blade in the slot shown in #5. (*2).
9	mmInfoProductSerialNo	.1.3.6.1.4.1.116.5.39.2.3.1.1.6	Display String	RO	Shows the Product Serial Number of the management module of the server blade in the slot shown in #5. (*1)

(*1) “Not install” is shown if no management module is installed; “Cannot get data” is shown if the management module data cannot be obtained.

(*2) “Not install” is shown if no management module is installed; “Cannot get data” is shown if the management module data cannot be obtained. “Not support” is shown as the response in this equipment.

(*3) The response is “0” if no management module is installed, or if the management module data cannot be obtained.

(b) moduleConfigMm group (2/3)

No	Object identifier	OID	Syntax	Access	Description
10	mmInfoProductManufacture	.1.3.6.1.4.1.116.5.39.2.3.1.1.7	Display String	RO	Shows the Product Manufacturer of the management module installed in the slot shown in #5. (*1)
11	mmInfoBoardProductName	.1.3.6.1.4.1.116.5.39.2.3.1.1.8	Display String	RO	Shows the Board Product Name of the management module installed in the slot shown in #5. (*1)
12	mmInfoBoardSerialNo	.1.3.6.1.4.1.116.5.39.2.3.1.1.9	Display String	RO	Shows the Board Serial Number of the management module installed in the slot shown in #5. (*1)
13	mmInfoChassisSerialNo	.1.3.6.1.4.1.116.5.39.2.3.1.1.10	Display String	RO	Shows the Chassis Serial Number of the management module installed in the slot shown in #5. (*2)
14	mmInfoChassisId	.1.3.6.1.4.1.116.5.39.2.3.1.1.11	Display String	RO	Shows the Chassis ID of the management module installed in the slot shown in #5. (*2)
15	mmInfoUuid	.1.3.6.1.4.1.116.5.39.2.3.1.1.12	Display String	RO	Shows the UUID of the management module installed in the slot shown in #5. (*2)
16	mmInfoBoardManufacture	.1.3.6.1.4.1.116.5.39.2.3.1.1.13	Display String	RO	Shows the Board Manufacture of the management module installed in the slot shown in #5. (*1)
17	mmInfoHigherTemp	.1.3.6.1.4.1.116.5.39.2.3.1.1.14	Integer32	RO	Shows the upper temperature threshold value of inlet air for warning to the management module of the server blade installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*3)
18	mmInfoLowerTemp	.1.3.6.1.4.1.116.5.39.2.3.1.1.15	Integer32	RO	Shows the lower temperature threshold value of inlet air for warning to the management module of the server blade installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*3)
19	mmInfoManagementIpAddress	.1.3.6.1.4.1.116.5.39.2.3.1.1.16	DisplayString	RO	Shows the IP address of management port of management module of the slot shown in #5.

(*1) “Not install” is shown if no management module is installed; “Cannot get data” is shown if the management module data cannot be obtained.

(*2) “Not install” is shown if no management module is installed; “Cannot get data” is shown if the management module data cannot be obtained. “Not support” is shown as the response in this equipment.

(*3) The response is “0” if no management module is installed, or if the management module data cannot be obtained.

(b) moduleConfigMm group (3/3)

No	Object identifier	OID	Syntax	Access	Description
20	mmInfoFwInfoTable	.1.3.6.1.4.1.116.5.39.2.3.2	Not-Accessible	NA	Shows the information table on the firmware version of the management module.
21	mmInfoFwInfoEntry	.1.3.6.1.4.1.116.5.39.2.3.2.1	Not-Accessible	NA	Shows the entry of the information table on the firmware version of the management module.
22	mmInfoFwInfoIndex	.1.3.6.1.4.1.116.5.39.2.3.2.1.1	Integer32	RO	Shows the index of the information table on the firmware version of the management module.
23	mmInfoFwActMmVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.2	Display String	RO	Shows the firmware version of a bank currently used by the management module. (*4)
24	mmInfoFwAltMmVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.3	Display String	RO	Shows the firmware version of a bank currently not used by the management module. (*4)
25	mmInfoFwActDictionaryVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.4	Display String	RO	Shows the SEL dictionary version of a bank currently used by the management module. (*4)
26	mmInfoFwAltDictionaryVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.5	Display String	RO	Shows the SEL dictionary version of a bank currently not used by the management module. “Not support” is shown as this value. (*4)
27	mmInfoFwActEquipmentParameterVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.6	Display String	RO	Shows the equipment parameter version of a bank currently used by the management module. (*4)
28	mmInfoFwAltEquipmentParameterVersion	.1.3.6.1.4.1.116.5.39.2.3.2.1.7	Display String	RO	Shows the equipment parameter version of a bank currently not used by the management module. (*4)

(*4) “Not install” is shown if no management module is installed; “Cannot get data” is shown if the management module is in P.ON or in boot disable.

(c) moduleConfigSw group

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigSw	.1.3.6.1.4.1.116.5.39.2.4	Not-Accessible	NA	Shows the information on the switch module configuration.
2	swInfoTable	.1.3.6.1.4.1.116.5.39.2.4.1	Not-Accessible	NA	Shows the table of information on the switch module configuration.
3	swInfoEntry	.1.3.6.1.4.1.116.5.39.2.4.1.1	Not-Accessible	NA	Shows the table entry describing the information on the switch module installation.
4	swInfoIndex	.1.3.6.1.4.1.116.5.39.2.4.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacitySw to identify the table entry.
5	swInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.4.1.1.2	Integer32	RO	Shows the switch module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacitySw–1.
6	swInfoProductName	.1.3.6.1.4.1.116.5.39.2.4.1.1.3	Display String	RO	Shows the Product type of the switch module installed in the slot shown in #5. (*1)
7	swInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.4.1.1.4	Display String	RO	Shows the Product Part Model of the switch module installed in the slot shown in #5. (*1)
8	swInfoProductSerialNo	.1.3.6.1.4.1.116.5.39.2.4.1.1.5	Display String	RO	Shows the Product Serial Number of the switch module installed in the slot shown in #5. (*1)
9	swInfoProductManufacture	.1.3.6.1.4.1.116.5.39.2.4.1.1.6	Display String	RO	Shows the Board Product Manufacturer of the switch module installed in the slot shown in #5. (*2)
10	swInfoProductVersion	.1.3.6.1.4.1.116.5.39.2.4.1.1.7	Display String	RO	Shows the Board Product Version of the switch module installed in the slot shown in #5. (*2)
11	swInfoBoardProductName	.1.3.6.1.4.1.116.5.39.2.4.1.1.8	Display String	RO	Shows the Board Product Name of the switch module installed in the slot shown in #5. (*2)
12	swInfoBoardSerialNo	.1.3.6.1.4.1.116.5.39.2.4.1.1.9	Display String	RO	Shows the Board Serial Number of the switch module installed in the slot shown in #5. (*2)
13	swInfoBoardManufacture	.1.3.6.1.4.1.116.5.39.2.4.1.1.10	Display String	RO	Shows the Board Manufacture of the switch module installed in the slot shown in #5. (*2)
14	swInfoBoardPartNo	.1.3.6.1.4.1.116.5.39.2.4.1.1.11	Display String	RO	Shows the Board Part Number of the switch module installed in the slot shown in #5. (*2)

(*1) “Not install” is shown if no switch module is installed; “Cannot get data” is shown if the switch module data cannot be obtained.

(*2) “Not install” is shown if no switch module is installed; “Cannot get data” is shown if the switch module data cannot be obtained. “Not support” is shown as the response in this equipment because this model does not collect information on those items.

(d) moduleConfigFan group

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigFan	.1.3.6.1.4.1.116.5.39.2.6	Not-Accessible	NA	Shows the information on fan module configuration.
2	fanInfoTable	.1.3.6.1.4.1.116.5.39.2.6.1	Not-Accessible	NA	Shows the table of information on fan module configuration.
3	fanInfoEntry	.1.3.6.1.4.1.116.5.39.2.6.1.1	Not-Accessible	NA	Shows the table entry describing the information on fan module installation.
4	fanInfoIndex	.1.3.6.1.4.1.116.5.39.2.6.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityFan to identify the table entry.
5	fanInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.6.1.1.2	Integer32	RO	Shows the fan module slot number corresponding to the index shown in #4, ranging from 0 to chassis CapacityFan–1.
6	fanInfoType	.1.3.6.1.4.1.116.5.39.2.6.1.1.3	Display String	RO	Shows the board type of a fan module installed in the slot shown in #5. (*1)
7	fanInfoMaxRpm	.1.3.6.1.4.1.116.5.39.2.6.1.1.4	Integer32	RO	Shows the maximum RPM of a fanmodule.

(*1) “Not install” is shown if no fan module is installed; “System Fan” is shown if a fan module is installed.

(e) moduleConfigPs group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigPs	.1.3.6.1.4.1.116.5.39.2.7	Not-Accessible	NA	Shows the information on power supply module configuration.
2	psInfoTable	.1.3.6.1.4.1.116.5.39.2.7.1	Not-Accessible	NA	Shows the table of information on power supply module installation.
3	psInfoEntry	.1.3.6.1.4.1.116.5.39.2.7.1.1	Not-Accessible	NA	Shows the table entry describing the information on power supply module installation.
4	psInfoIndex	.1.3.6.1.4.1.116.5.39.2.7.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPs to identify the table entry.
5	psInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.7.1.1.2	Integer32	RO	Shows the power supply module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPs–1.
6	psInfoProductSerialNo	.1.3.6.1.4.1.116.5.39.2.7.1.1.3	Display String	RO	Shows the serial number of a power supply module installed in the slot shown in #5. (*1)
7	psInfoProductName	.1.3.6.1.4.1.116.5.39.2.7.1.1.4	Display String	RO	Shows the Product Name of the power supply module installed in the slot shown in #5. (*1)
8	psInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.7.1.1.5	Display String	RO	Shows the Product Part Model of the power supply module installed in the slot shown in #5. (*1)
9	psInfoProductVersion	.1.3.6.1.4.1.116.5.39.2.7.1.1.6	Display String	RO	Shows the Product Version of the power supply module installed in the slot shown in #5. (*1)
10	psInfoProductManufacuture	.1.3.6.1.4.1.116.5.39.2.7.1.1.7	Display String	RO	Shows the Product Manufacturer of the power supply module installed in the slot shown in #5. (*1)
11	psInfoAmbientTempHigher	.1.3.6.1.4.1.116.5.39.2.7.1.1.8	Integer32	RO	Shows the upper temperature threshold value of inlet air for warning to the power supply module installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*2)
12	psInfoAmbientTempLower	.1.3.6.1.4.1.116.5.39.2.7.1.1.9	Integer32	RO	Shows the lower temperature threshold value of inlet air for warning to the power supply module installed in the slot shown in #5. This value is always shown as 0.

(*1) “Not install” is shown if no power supply module is installed; “Cannot get data” is shown if the power supply module data cannot be obtained.

(*2) “0” is shown if no power supply module is installed or if no power supply module data can be obtained.

(e) moduleConfigPs group (2/2)

No	Object identifier	OID	Syntax	Access	Description
13	psInfoHotspotTempHigher	.1.3.6.1.4.1.1166.5.39.2.7.1.1.10	Integer32	RO	Shows the upper temperature threshold value of HotSpot for warning to the power supply module installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*2)
14	psInfoHotSpotTempLower	.1.3.6.1.4.1.1166.5.39.2.7.1.1.11	Integer32	RO	Shows the lower temperature threshold value of HotSpot for warning to the power supply module installed in the slot shown in #5. This value is always shown as 0.
15	psInfoExhaustTempHigher	.1.3.6.1.4.1.1166.5.39.2.7.1.1.12	Integer32	RO	Shows the upper temperature threshold value of exhaust air for warning to the power supply module installed in the slot shown in #5. This value is shown as 1 for 0.1°C. (*2)
16	psInfoExhaustTempLower	.1.3.6.1.4.1.1166.5.39.2.7.1.1.13	Integer32	RO	Shows the lower temperature threshold value of exhaust air for warning to the power supply module installed in the slot shown in #5. This value is always shown as 0.

(*1) “Not install” is shown if no power supply module is installed; “Cannot get data” is shown if the power supply module data cannot be obtained.

(*2) “0” is shown if no power supply module is installed or if no power supply module data can be obtained.

(f) moduleConfigPciRiser group (1/4)

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigPciRiser	.1.3.6.1.4.1.116.5.39.2.9	Not-Accessible	NA	Shows the information on PCI-e Riser card (IOCD module) configuration.
2	pciRiserInfoTable	.1.3.6.1.4.1.116.5.39.2.9.1	Not-Accessible	NA	Shows the table of information on PCI-e Riser card (IOCD module) installation.
3	pciRiserInfoEntry	.1.3.6.1.4.1.116.5.39.2.9.1.1	Not-Accessible	NA	Shows the table entry describing the information on PCI-e Riser card (IOCD module) installation.
4	pciRiserInfoIndex	.1.3.6.1.4.1.116.5.39.2.9.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPciRiser to identify the table entry.
5	pciRiserInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.9.1.1.2	Integer32	RO	Shows the PCI-e Riser card (IOCD module) slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPciRiser–1.
6	pciRiserInfoProductName	.1.3.6.1.4.1.116.5.39.2.9.1.1.3	Display String	RO	Shows the Product Name of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
7	pciRiserInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.9.1.1.4	Display String	RO	Shows the Product Part Model of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
8	pciRiserInfoProductVersion	.1.3.6.1.4.1.116.5.39.2.9.1.1.5	Display String	RO	Shows the Product Version of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
9	pciRiserInfoProductManufacture	.1.3.6.1.4.1.116.5.39.2.9.1.1.6	Display String	RO	Shows the Product Manufacture of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
10	pciRiserInfoBoardProductName	.1.3.6.1.4.1.116.5.39.2.9.1.1.7	Display String	RO	Shows the Board Product Name of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
11	pciRiserInfoBoardSerialNo	.1.3.6.1.4.1.116.5.39.2.9.1.1.8	Display String	RO	Shows the Board Serial Number of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. (*1)
12	pciRiserInfoBoardManufacture	.1.3.6.1.4.1.116.5.39.2.9.1.1.9	Display String	RO	Shows the Board Manufacture of the PCI-e Riser card (IOCD module), installed in the slot shown in #5. (*1)

(*1) “Not install” is shown if no PCI-e Riser card (IOCD module) is installed; “Cannot get data” is shown if the PCI-e Riser card (IOCD module) data cannot be obtained.

(f) moduleConfigPciRiser group (2/4)

No	Object identifier	OID	Syntax	Access	Description
13	pciRiserCapacityIoExpansion	.1.3.6.1.4.1.116.5.39.2.9.1.1.10	Integer32	RO	Shows the number of I/O slot expansion units that can be connected to the I/O board module installed in the slot shown in #5
14	pciRiserInfoIoExpansionTable	.1.3.6.1.4.1.116.5.39.2.9.2	Not-Accessible	NA	Shows the table of information on I/O slot expansion unit connected to the I/O board module.
15	pciRiserInfoIoExpansionEntry	.1.3.6.1.4.1.116.5.39.2.9.2.1	Not-Accessible	NA	Shows the table entry describing the information on I/O slot expansion units connected to the I/O board module.
16	pciRiserIoExpansionIndex	.1.3.6.1.4.1.116.5.39.2.9.2.1.1	Integer32	RO	Shows the index of information on I/O slot expansion units connected to the I/O board module.
17	pciRiserIoExpansionExist	.1.3.6.1.4.1.116.5.39.2.9.2.1.2	INTEGER	RO	Shows the status of information on I/O slot expansion units connected to the I/O board module installed in the slot shown in #5. 1. non-exist 2. exist
18	pciRiserIoExpansionProductPartModel	.1.3.6.1.4.1.116.5.39.2.9.2.1.3	DisplayString	RO	Shows the ProductPartModel of I/O slot expansion units connected to the I/O board module installed in the slot shown in #5. (*3)
19	pciRiserIoExpansionProductSerialNum	.1.3.6.1.4.1.116.5.39.2.9.2.1.4	DisplayString	RO	Shows the ProductSerialNo of I/O slot expansion units connected to the I/O board module installed in the slot shown in #5. (*3)
20	pciRiserIoExpansionConnectedIoaNo	.1.3.6.1.4.1.116.5.39.2.9.2.1.5	Integer32	RO	Shows the I/O module number of I/O slot expansion units connected to the I/O board module installed in the slot shown in #5. (*4)

(*2) "1" is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*3) “Not Install” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*4) “0” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*5) “1” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(f) moduleConfigPciRiser group (3/4)

No	Object identifier	OID	Syntax	Access	Description
21	pciRiserIoExpansionConnectedIoaPortNo	.1.3.6.1.4.1.116.5.39.2.9.2.1.6	Integer32	RO	Shows the port number of the I/O module in I/O slot expansion units on the I/O board module installed in the slot shown in #5. (*4)
22	pciRiserIoExpansionConnectedPciNum	.1.3.6.1.4.1.116.5.39.2.9.2.1.7	Integer32	RO	Shows the number of PCI riser cards to be connected to the I/O slot expansion unit connected to the I/O board module installed in the slot shown in #5. (*5)
23	pciRiserInfoIoExpansionBelongedPciTable	.1.3.6.1.4.1.116.5.39.2.9.3	Not-Accessible	NA	Shows the table of information on PCI riser card connection on the I/O slot expansion unit connected to the I/O board module.
24	pciRiserInfoIoExpansionBelongedPciEntry	.1.3.6.1.4.1.116.5.39.2.9.3.1	Not-Accessible	NA	Shows the table entry describing information on PI riser cards on the I/O slot expansion units connected to the I/O board module.
25	pciRiserIoExpansionBelongedPciIndex	.1.3.6.1.4.1.116.5.39.2.9.3.1.1	Integer32	RO	Shows the index of information on of PCI riser cards connection on the I/O slot expansion unit connected to the I/O board module.
26	pciRiserIoExpansionBelongedPciSlot1	.1.3.6.1.4.1.116.5.39.2.9.3.1.2	Integer32	RO	Shows the 1st slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
27	pciRiserIoExpansionBelongedPciSlot2	.1.3.6.1.4.1.116.5.39.2.9.3.1.3	Integer32	RO	Shows the 2nd slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
28	pciRiserIoExpansionBelongedPciSlot3	.1.3.6.1.4.1.116.5.39.2.9.3.1.4	Integer32	RO	Shows the 3rd slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)

(*2) "1" is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*3) “Not Install” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*4) “0” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*5) “1” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(f) moduleConfigPciRiser group (4/4)

No	Object identifier	OID	Syntax	Access	Description
29	pciRiserIoExpansionBelongedPciSlot4	.1.3.6.1.4.1.116.5.39.2.9.3.1.5	Integer32	RO	Shows the 4th slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
30	pciRiserIoExpansionBelongedPciSlot5	.1.3.6.1.4.1.116.5.39.2.9.3.1.6	Integer32	RO	Shows the 5th slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
31	pciRiserIoExpansionBelongedPciSlot6	.1.3.6.1.4.1.116.5.39.2.9.3.1.7	Integer32	RO	Shows the 6th slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
32	pciRiserIoExpansionBelongedPciSlot7	.1.3.6.1.4.1.116.5.39.2.9.3.1.8	Integer32	RO	Shows the 7th slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)
33	pciRiserIoExpansionBelongedPciSlot8	.1.3.6.1.4.1.116.5.39.2.9.3.1.9	Integer32	RO	Shows the 8th slot for a PCI riser card to be connected to the I/o slot expansion unit connected to the I/O board module shown in #5. (*4)

(*2) "1" is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*3) “Not Install” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*4) “0” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(*5) “1” is shown if no I/O board module installed, no I/O slot expansion unit connected, or no I/O slot expansion unit can be identified.

(g) moduleConfigPcieSw group (1/2)

This item is not supported.

No	Object identifier	OID	Syntax	Access	Description
1	moduleConfigPcieSw	.1.3.6.1.4.1.116.5.39.2.10	Not-Accessible	NA	Shows the information on peripheral components interconnect (PCI) Express switch module configuration.
2	pcieSwInfoTable	.1.3.6.1.4.1.116.5.39.2.10.1	Not-Accessible	NA	Shows the table of information on PCI Express switch module installation.
3	pcieSwInfoEntry	.1.3.6.1.4.1.116.5.39.2.10.1.1	Not-Accessible	NA	Shows the table entry describing the information on PCI Express switch module installation.

(g) moduleConfigPcieSw group (2/2)

This item is not supported.

No	Object identifier	OID	Syntax	Access	Description
4	pcieSwInfoIndex	.1.3.6.1.4.1.116.5.39.2.10.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPcieSw to identify the table entry.
5	pcieSwInfoSlotnum	.1.3.6.1.4.1.116.5.39.2.10.1.1.2	Integer32	RO	Shows the PCI Express switch module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityPcieSw –1.
6	pcieSwInfoProductName	.1.3.6.1.4.1.116.5.39.2.10.1.1.3	DisplayString	RO	Shows the type of the PCI Express switch module installed in the slot shown in #5. (*1)
7	pcieSwInfoProductPartModel	.1.3.6.1.4.1.116.5.39.2.10.1.1.4	DisplayString	RO	Shows the ProductPartModel of the PCI Express switch module installed in the slot shown in #5. (*1)
8	pcieSwInfoProductSerialNo	.1.3.6.1.4.1.116.5.39.2.10.1.1.5	DisplayString	RO	Shows the ProductSerialNo of the PCI Express switch module installed in the slot shown in #5. (*1)
9	pcieSwInfoProductManufacture	.1.3.6.1.4.1.116.5.39.2.10.1.1.6	DisplayString	RO	Shows the ProductManufacturer of the PCI Express switch module installed in the slot shown in #5. (*2)
10	pcieSwInfoProductVersion	.1.3.6.1.4.1.116.5.39.2.10.1.1.7	DisplayString	RO	Shows the ProductVersion of the PCI Express switch module installed in the slot shown in #5. (*2)
11	pcieSwInfoBoardProductName	.1.3.6.1.4.1.116.5.39.2.10.1.1.8	DisplayString	RO	Shows the BoardProductName of the PCI Express switch module installed in the slot shown in #5. (*2)
12	pcieSwInfoBoardSerialNo	.1.3.6.1.4.1.116.5.39.2.10.1.1.9	DisplayString	RO	Shows the BoardSerialNo of the PCI Express switch module installed in the slot shown in #5. (*2)
13	pcieSwInfoBoardManufacture	.1.3.6.1.4.1.116.5.39.2.10.1.1.10	DisplayString	RO	Shows the BoardManufacture of the PCI Express switch module installed in the slot shown in #5. (*2)
14	pcieSwInfoBoardPartNo	.1.3.6.1.4.1.116.5.39.2.10.1.1.11	DisplayString	RO	Shows the BoardPartNo of the PCI Express switch module installed in the slot shown in #5. (*2)

(*1) “Not Install” is shown if no PCI Express switch module installed, “Cannot get data” is shown if no information on the PCI Express switch module can be collected.

(*2) “Not Install” is shown if no PCI Express switch module installed, “Cannot get data” is shown if no information on the PCI Express switch module can be collected. Since information on this item is not collected on this model, “No support” is shown.

3 moduleStatus

moduleStatus consists of the following seven groups: moduleStatusBlade, moduleStatusMm, moduleStatusSw, moduleStatusFan, moduleStatusPs, moduleStatusPciRiser, and moduleStatusPcieSw. Each group is described in the following table (a) to (g).

(a) moduleStatusBlade group (1/34)

This group consists of three tables: bladeStatusTable for the entire server blade information, bladeVoltageTable for the voltage sensor information, and bladeTemperatureTable for the temperature sensor information.

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusBlade	.1.3.6.1.4.1.116.5.39.3.2	Not-Accessible	NA	Shows the server blade status.
2	bladeStatusTable	.1.3.6.1.4.1.116.5.39.3.2.1	Not-Accessible	NA	Shows the table of information on the server blade status.
3	bladeStatusEntry	.1.3.6.1.4.1.116.5.39.3.2.1.1	Not-Accessible	NA	Shows the table entry describing the information on the server blade status.
4	bladeStatusIndex	.1.3.6.1.4.1.116.5.39.3.2.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityBlade to identify the table entry.
5	bladeStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.2.1.1.2	Integer32	RO	Shows the server blade slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityBlade–1.
6	bladeStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.2.1.1.3	INTEGER	RO	Shows the status of the server blade installed in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	bladeStatusSensorCapacityVoltage	.1.3.6.1.4.1.116.5.39.3.2.1.1.4	Integer32	RO	Shows the maximum number of voltage sensors for a server blade. (*2)

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (2/34)

No	Object identifier	OID	Syntax	Access	Description
8	bladeStatusSensorCapacityTemperature	.1.3.6.1.4.1.116.5.39.3.2.1.1.5	Integer32	RO	Shows the maximum number of temperature sensors for a server blade. (*2)
9	bladeStatusCurrentCurrency	.1.3.6.1.4.1.116.5.39.3.2.1.1.6	Integer32	RO	Shows the current being consumed at present by the server blade installed in the slot shown in #5. This is shown as 1 for 0.1A. (*2)(*7)
10	bladeStatusCurrentPower	.1.3.6.1.4.1.116.5.39.3.2.1.1.7	Integer32	RO	Shows the power being consumed at present by the server blade installed in the slot shown in #5. This is shown as 1 for 1W. (*2)(*7)
11	bladeStatusFanRpm	.1.3.6.1.4.1.116.5.39.3.2.1.1.8	Integer32	RO	Shows the Rpm number of the fan in the server blade. This is shown as “0”.
12	bladeStatusFanAirVolume	.1.3.6.1.4.1.116.5.39.3.2.1.1.9	Integer32	RO	Shows the air volume provided by the fan in the server blade. This is shown as “0”.
13	bladeStatusIntakeTemp	.1.3.6.1.4.1.116.5.39.3.2.1.1.10	INTEGER	RO	Shows the inlet air temperature status to the server blade installed in the slot shown in #5. (*3) 1: normal 2: higher-warning 3: error-warning 4: lower-warning
14	bladeVoltageTable	.1.3.6.1.4.1.116.5.39.3.2.2	Not-Accessible	NA	Shows the table of information on the voltage sensor with the server blade.
15	bladeVoltageEntry	.1.3.6.1.4.1.116.5.39.3.2.2.1	Not-Accessible	NA	Shows the table entry of information on the voltage sensor with the server blade.
16	bladeVoltIndex	.1.3.6.1.4.1.116.5.39.3.2.2.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityBalde to identify the table entry.
17	bladeVoltSensor1Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.2	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(*7) With SMP configuration, when the primary blade location in a partition is specified, the values of the entire partition are displayed; when a blade location other than the primary one is specified, “0” is displayed.

(a) moduleStatusBlade group (3/34)

No	Object identifier	OID	Syntax	Access	Description
18	bladeVoltSensor1Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.3	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) This value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
19	bladeVoltSensor1Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.4	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in # 5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
20	bladeVoltSensor2Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.5	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
21	bladeVoltSensor2Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.6	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The actual value is one-tenth of the response value.
22	bladeVoltSensor2Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.7	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
23	bladeVoltSensor3Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.8	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
24	bladeVoltSensor3Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.9	Integer32	RO	Shows the voltage value of the server blade installed in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (4/34)

No	Object identifier	OID	Syntax	Access	Description
25	bladeVoltSensor3Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.10	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. (*3) One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
26	bladeVoltSensor4Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.11	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
27	bladeVoltSensor4Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.12	Integer32	RO	Shows the voltage value of the server blade installed in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
28	bladeVoltSensor4Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.13	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
29	bladeVoltSensor5Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.14	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
30	bladeVoltSensor5Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.15	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
31	bladeVoltSensor5Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.16	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (5/34)

No	Object identifier	OID	Syntax	Access	Description
32	bladeVoltSensor6Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.17	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
33	bladeVoltSensor6Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.18	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
34	bladeVoltSensor6Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.19	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
35	bladeVoltSensor7Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.20	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
36	bladeVoltSensor7Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.21	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
37	bladeVoltSensor7Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.22	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
38	bladeVoltSensor8Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.23	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
39	bladeVoltSensor8Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.24	Integer32	RO	Shows the voltage value of the server blade installed in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (6/34)

No	Object identifier	OID	Syntax	Access	Description
40	bladeVoltSensor8Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.25	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
41	bladeVoltSensor9Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.26	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
42	bladeVoltSensor9Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.27	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
43	bladeVoltSensor9Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.28	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
44	bladeVoltSensor10Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.29	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
45	bladeVoltSensor10Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.30	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
46	bladeVoltSensor10Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.31	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (7/34)

No	Object identifier	OID	Syntax	Access	Description
47	bladeVoltSensor11Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.32	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
48	bladeVoltSensor11Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.33	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
49	bladeVoltSensor11Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.34	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
50	bladeVoltSensor12Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.35	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
51	bladeVoltSensor12Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.36	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
52	bladeVoltSensor12Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.37	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
53	bladeVoltSensor13Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.38	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
54	bladeVoltSensor13Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.39	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5.) (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (8/34)

No	Object identifier	OID	Syntax	Access	Description
55	bladeVoltSensor13Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.40	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
56	bladeVoltSensor14Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.41	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
57	bladeVoltSensor14Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.42	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
58	bladeVoltSensor14Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.43	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
59	bladeVoltSensor15Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.44	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
60	bladeVoltSensor15Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.45	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
61	bladeVoltSensor15Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.46	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (9/34)

No	Object identifier	OID	Syntax	Access	Description
62	bladeVoltSensor16Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.47	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
63	bladeVoltSensor16Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.48	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
64	bladeVoltSensor16Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.49	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
65	bladeVoltSensor17Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.50	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
66	bladeVoltSensor17Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.51	Integer32	RO	Shows the voltage value of the server blade installed in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
67	bladeVoltSensor17Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.52	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
68	bladeVoltSensor18Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.53	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
69	bladeVoltSensor18Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.54	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (10/34)

No	Object identifier	OID	Syntax	Access	Description
70	bladeVoltSensor18Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.55	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
71	bladeVoltSensor19Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.56	Display String	RO	Shows the voltage sensor name for the server blade installed in the slot shown in #5. (*4)
72	bladeVoltSensor19Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.57	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
73	bladeVoltSensor19Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.58	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
74	bladeVoltSensor20Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.59	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
75	bladeVoltSensor20Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.60	Display String	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
76	bladeVoltSensor20Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.61	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (11/34)

No	Object identifier	OID	Syntax	Access	Description
77	bladeVoltSensor21Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.62	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
78	bladeVoltSensor21Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.63	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
79	bladeVoltSensor21Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.64	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
80	bladeVoltSensor22Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.65	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
81	bladeVoltSensor22Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.66	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
82	bladeVoltSensor22Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.67	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
83	bladeVoltSensor23Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.68	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
84	bladeVoltSensor23Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.69	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (12/34)

No	Object identifier	OID	Syntax	Access	Description
85	bladeVoltSensor23Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.70	INTEGER	RO	Shows the voltage value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
86	bladeVoltSensor24Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.71	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
87	bladeVoltSensor24Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.72	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
88	bladeVoltSensor24Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.73	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
89	bladeVoltSensor25Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.74	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
90	bladeVoltSensor25Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.75	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
91	bladeVoltSensor25Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.76	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (13/34)

No	Object identifier	OID	Syntax	Access	Description
92	bladeVoltSensor26Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.77	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
93	bladeVoltSensor26Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.78	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
94	bladeVoltSensor26Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.79	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
95	bladeVoltSensor27Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.80	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
96	bladeVoltSensor27Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.81	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
97	bladeVoltSensor27Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.82	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
98	bladeVoltSensor28Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.83	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
99	bladeVoltSensor28Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.84	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (14/34)

No	Object identifier	OID	Syntax	Access	Description
100	bladeVoltSensor28Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.85	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
101	bladeVoltSensor29Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.86	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
102	bladeVoltSensor29Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.87	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
103	bladeVoltSensor29Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.88	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. (*3) One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
104	bladeVoltSensor30Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.89	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
105	bladeVoltSensor30Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.90	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
106	bladeVoltSensor30Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.91	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (15/34)

No	Object identifier	OID	Syntax	Access	Description
107	bladeVoltSensor31Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.92	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
108	bladeVoltSensor31Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.93	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
109	bladeVoltSensor31Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.94	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
110	bladeVoltSensor32Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.95	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
111	bladeVoltSensor32Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.96	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
112	bladeVoltSensor32Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.97	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
113	bladeVoltSensor33Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.98	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
114	bladeVoltSensor33Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.99	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (16/34)

No	Object identifier	OID	Syntax	Access	Description
115	bladeVoltSensor33Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.100	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
116	bladeVoltSensor34Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.101	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
117	bladeVoltSensor34Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.102	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
118	bladeVoltSensor34Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.103	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
119	bladeVoltSensor35Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.104	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
120	bladeVoltSensor35Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.105	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
121	bladeVoltSensor35Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.106	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (17/34)

No	Object identifier	OID	Syntax	Access	Description
122	bladeVoltSensor36Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.107	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
123	bladeVoltSensor36Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.108	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
124	bladeVoltSensor36Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.109	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
125	bladeVoltSensor37Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.110	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
126	bladeVoltSensor37Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.111	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
127	bladeVoltSensor37Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.112	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
128	bladeVoltSensor38Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.113	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
129	bladeVoltSensor38Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.114	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (18/34)

No	Object identifier	OID	Syntax	Access	Description
130	bladeVoltSensor38Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.115	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
131	bladeVoltSensor39Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.116	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
132	bladeVoltSensor39Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.117	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
133	bladeVoltSensor39Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.118	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
134	bladeVoltSensor40Name	.1.3.6.1.4.1.116.5.39.3.2.2.1.119	Display String	RO	Shows the voltage sensor name for the server blade in the slot shown in #5. (*4)
135	bladeVoltSensor40Value	.1.3.6.1.4.1.116.5.39.3.2.2.1.120	Integer32	RO	Shows the voltage value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
136	bladeVoltSensor40Valid	.1.3.6.1.4.1.116.5.39.3.2.2.1.121	INTEGER	RO	Shows the voltage value validity of the server blade installed in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
137	bladeTemperatureTable	.1.3.6.1.4.1.116.5.39.3.2.3	Not-Accessible	NA	Shows the table of information on the server blade temperature sensor.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (19/34)

No	Object identifier	OID	Syntax	Access	Description
138	bladeTemperatureEntry	.1.3.6.1.4.1.116.5.39.3.2.3.1	Not-Accessible	NA	Shows the table entry describing the information on the server blade temperature sensor.
139	bladeTempIndex	.1.3.6.1.4.1.116.5.39.3.2.3.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityBlade to identify the table entry.
140	bladeTempSensor1Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.2	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
141	bladeTempSensor1Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.3	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
142	bladeTempSensor1Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.4	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
143	bladeTempSensor2Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.5	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
144	bladeTempSensor2Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.6	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
145	bladeTempSensor2Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.7	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (20/34)

No	Object identifier	OID	Syntax	Access	Description
146	bladeTempSensor3Name	.1.3.6.1.4.1.1166.5.39.3.2.3.1.8	Display String	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
147	bladeTempSensor3Value	.1.3.6.1.4.1.1166.5.39.3.2.3.1.9	Integer32	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
148	bladeTempSensor3Valid	.1.3.6.1.4.1.1166.5.39.3.2.3.1.10	INTEGER	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
149	bladeTempSensor4Name	.1.3.6.1.4.1.1166.5.39.3.2.3.1.11	Display String	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
150	bladeTempSensor4Value	.1.3.6.1.4.1.1166.5.39.3.2.3.1.12	Integer32	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
151	bladeTempSensor4Valid	.1.3.6.1.4.1.1166.5.39.3.2.3.1.13	INTEGER	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
152	bladeTempSensor5Name	.1.3.6.1.4.1.1166.5.39.3.2.3.1.14	Display String		

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (21/34)

No	Object identifier	OID	Syntax	Access	Description
153	bladeTempSensor9Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.28	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
154	bladeTempSensor10Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.29	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
155	bladeTempSensor10Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.30	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
156	bladeTempSensor10Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.31	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
157	bladeTempSensor11Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.32	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
158	bladeTempSensor11Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.33	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
159	bladeTempSensor7Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.21	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (22/34)

No	Object identifier	OID	Syntax	Access	Description
160	bladeTempSensor11Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.34	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
161	bladeTempSensor12Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.35	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
162	bladeTempSensor12Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.36	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
163	bladeTempSensor12Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.37	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
164	bladeTempSensor13Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.38	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
165	bladeTempSensor13Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.39	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (23/34)

No	Object identifier	OID	Syntax	Access	Description
166	bladeTempSensor13Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.40	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
167	bladeTempSensor14Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.41	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
168	bladeTempSensor140Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.42	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
169	bladeTempSensor14Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.43	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
170	bladeTempSensor15Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.44	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
171	bladeTempSensor15Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.45	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (24/34)

No	Object identifier	OID	Syntax	Access	Description
172	bladeTempSensor15Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.46	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
173	bladeTempSensor16Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.47	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
174	bladeTempSensor16Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.48	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
175	bladeTempSensor16Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.49	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
176	bladeTempSensor17Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.50	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
177	bladeTempSensor17Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.51	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (25/34)

No	Object identifier	OID	Syntax	Access	Description
178	bladeTempSensor17Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.52	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
179	bladeTempSensor18Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.53	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
180	bladeTempSensor14Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.54	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
181	bladeTempSensor18Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.55	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
182	bladeTempSensor19Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.56	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
183	bladeTempSensor19Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.57	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (26/34)

No	Object identifier	OID	Syntax	Access	Description
184	bladeTempSensor15Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.46	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
185	bladeTempSensor16Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.47	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
186	bladeTempSensor16Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.48	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
187	bladeTempSensor16Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.49	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
188	bladeTempSensor17Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.50	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
189	bladeTempSensor17Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.51	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (27/34)

No	Object identifier	OID	Syntax	Access	Description
190	bladeTempSensor17Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.52	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
191	bladeTempSensor18Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.53	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
192	bladeTempSensor18Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.54	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
193	bladeTempSensor18Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.55	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
194	bladeTempSensor19Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.56	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
195	bladeTempSensor19Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.57	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.

(*1) The reply is “unknown”, if no server blade is installed or the status cannot be obtained.

(*2) A value that the server blade obtains from a voltage and temperature sensor is shown. “0” is shown if no server blade or no sensor is installed.

(*3) The reply is “normal” if no server blade is installed or the server blade power is off.

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(a) moduleStatusBlade group (28/34)

No	Object identifier	OID	Syntax	Access	Description
196	bladeTempSensor19Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.58	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
197	bladeTempSensor20Name	.1.3.6.1.4.1.116.5.39.3.2.3.1.59	Display String	RO	Shows the temperature sensor name for the server blade in the slot shown in #5. (*4)
198	bladeTempSensor20Value	.1.3.6.1.4.1.116.5.39.3.2.3.1.60	Integer32	RO	Shows the temperature value of the server blade in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
199	bladeTempSensor20Valid	.1.3.6.1.4.1.116.5.39.3.2.3.1.61	INTEGER	RO	Shows the temperature value validity of the server blade in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
200	bladeDimmStatusTable	.1.3.6.1.4.1.116.5.39.3.2.4	Not-Accessible	NA	Shows the information table on DIMM installed in the server blade.
201	bladeDimmStatus Entry	.1.3.6.1.4.1.116.5.39.3.2.4.1	Not-Accessible	NA	Shows the entry of the information table on DIMM installed in the server blade.
202	bladeDimmStatus Index	.1.3.6.1.4.1.116.5.39.3.2.4.1.1	Integer32	RO	Shows the index of the information table on DIMM installed in the server blade.
203	bladeDimm1Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.2	INTEGER	RO	Shows the status of DIMM installed in the first DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*4) “Not install” is shown if no server blade is installed; “Not support” is shown if a server blade is installed without any sensor; “Cannot get data” is shown if the data cannot be obtained.

(*5) The response is “0” if no server blade or no sensor is installed. Obtain the MIB object of the next OID, and determine whether or not the replied value is valid.

(*6) “invalid” is shown if no server blade or no sensor is installed; “unknown” is shown if no information can be obtained”.

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (29/34)

No	Object identifier	OID	Syntax	Access	Description
204	bladeDimm2Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.3	INTEGER	RO	Shows the status of DIMM installed in the second DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
205	bladeDimm3Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.4	INTEGER	RO	Shows the status of DIMM installed in the third DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
206	bladeDimm4Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.5	INTEGER	RO	Shows the status of DIMM installed in the 4th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
207	bladeDimm5Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.6	INTEGER	RO	Shows the status of DIMM installed in the 5th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
208	bladeDimm6Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.7	INTEGER	RO	Shows the status of DIMM installed in the 6th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (30/34)

No	Object identifier	OID	Syntax	Access	Description
209	bladeDimm7Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.8	INTEGER	RO	Shows the status of DIMM installed in the 7th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
210	bladeDimm8Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.9	INTEGER	RO	Shows the status of DIMM installed in the 8th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
211	bladeDimm9Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.10	INTEGER	RO	Shows the status of DIMM installed in the 9th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
212	bladeDimm10Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.11	INTEGER	RO	Shows the status of DIMM installed in the 10th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
213	bladeDimm11Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.12	INTEGER	RO	Shows the status of DIMM installed in the 11th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
214	bladeDimm12Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.13	INTEGER	RO	Shows the status of DIMM installed in the 12th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (31/34)

No	Object identifier	OID	Syntax	Access	Description
215	bladeDimm13Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.14	INTEGER	RO	Shows the status of DIMM installed in the 13th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
216	bladeDimm14Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.15	INTEGER	RO	Shows the status of DIMM installed in the 14th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
217	bladeDimm15Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.16	INTEGER	RO	Shows the status of DIMM installed in the 15th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
218	bladeDimm16Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.17	INTEGER	RO	Shows the status of DIMM installed in the 16th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
219	bladeDimm17Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.18	INTEGER	RO	Shows the status of DIMM installed in the 17th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
220	bladeDimm18Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.19	INTEGER	RO	Shows the status of DIMM installed in the 18th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (32/34)

No	Object identifier	OID	Syntax	Access	Description
221	bladeDimm19Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.20	INTEGER	RO	Shows the status of DIMM installed in the 19th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
222	bladeDimm20Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.21	INTEGER	RO	Shows the status of DIMM installed in the 20th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
223	bladeDimm21Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.22	INTEGER	RO	Shows the status of DIMM installed in the 21st DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
224	bladeDimm22Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.23	INTEGER	RO	Shows the status of DIMM installed in the 22nd DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
225	bladeDimm23Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.24	INTEGER	RO	Shows the status of DIMM installed in the 23rd DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
226	bladeDimm24Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.25	INTEGER	RO	Shows the status of DIMM installed in the 24th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (33/34)

No	Object identifier	OID	Syntax	Access	Description
227	bladeDimm25Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.26	INTEGER	RO	Shows the status of DIMM installed in the 25th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
228	bladeDimm26Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.27	INTEGER	RO	Shows the status of DIMM installed in the 26th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
229	bladeDimm27Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.28	INTEGER	RO	Shows the status of DIMM installed in the 27th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
230	bladeDimm28Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.29	INTEGER	RO	Shows the status of DIMM installed in the 28th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
231	bladeDimm29Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.30	INTEGER	RO	Shows the status of DIMM installed in the 29th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
232	bladeDimm30Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.31	INTEGER	RO	Shows the status of DIMM installed in the 30th DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(a) moduleStatusBlade group (34/34)

No	Object identifier	OID	Syntax	Access	Description
233	bladeDimm31Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.32	INTEGER	RO	Shows the status of DIMM installed in the 31st DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated
234	bladeDimm32Status	.1.3.6.1.4.1.116.5.39.3.2.4.1.33	INTEGER	RO	Shows the status of DIMM installed in the 32nd DIMM slot of the server blade. One of the following values is shown. (*8) 1. normal 2. unknown 3. degenerated 4. planned-degenerated

(*8) “Unknown” is shown if no server blade is installed or if no DIMM in the DIMM slot; if CPU is in failure or degenerated as planned. This value is determined when POST (Power-on self-test) is completed: a server blade is powered on.

(b) moduleStatusMm group (1/7)

This group consists of three tables: mmStatusTable for the entire information on the management module, mmVoltageTable for the voltage sensor information on the management module, and mmTemperatureTable for the temperature sensor information on the management module

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusMm	.1.3.6.1.4.1.116.5.39.3.3	Not-Accessible	NA	Shows the management module status.
2	mmStatusTable	.1.3.6.1.4.1.116.5.39.3.3.1	Not-Accessible	NA	Shows the table of information on the management module status.
3	mmStatusEntry	.1.3.6.1.4.1.116.5.39.3.3.1.1	Not-Accessible	NA	Shows the table entry describing the information on the management module status.
4	mmStatusIndex	.1.3.6.1.4.1.116.5.39.3.3.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMm to identify the table entry.
5	mmStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.3.1.1.2	Integer32	RO	Shows the management module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityMm–1.
6	mmStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.3.1.1.3	INTEGER	RO	Shows the status of the management module in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	mmStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.3.1.1.4	INTEGER	RO	Shows the status of the management module installed in the slot shown in #5. One of the following messages is shown. (*2) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing Software Defined Networking (SDN) in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (2/7)

No	Object identifier	OID	Syntax	Access	Description
8	mmStatusRunningStatus	.1.3.6.1.4.1.116.5.39.3.3.1.1.5	INTEGER	RO	Shows the running status of the management module in the slot shown in #5. One of the following messages is shown. (*2) 1: active 2: standby 3: unknown
9	mmStatusSensorCapacityVoltage	.1.3.6.1.4.1.116.5.39.3.3.1.1.6	Integer32	RO	Shows the max number of voltage sensors for the management module in the slot shown in #5. (*3)
10	mmStatusSensorCapacityTemperature	.1.3.6.1.4.1.116.5.39.3.3.1.1.7	Integer32	RO	Shows the max number of temperature sensors for the management module in the slot shown in #5. (*3)
11	mmVoltageTable	.1.3.6.1.4.1.116.5.39.3.3.2	Not-Accessible	NA	Shows the table of information on the voltage sensor for the management module.
12	mmVoltageEntry	.1.3.6.1.4.1.116.5.39.3.3.2.1	Not-Accessible	NA	Shows the table entry describing the information on the voltage sensor for the management module.
13	mmVoltIndex	.1.3.6.1.4.1.116.5.39.3.3.2.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMm to identify the table entry.
14	mmVoltSensor1Name	.1.3.6.1.4.1.116.5.39.3.3.2.1.2	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
15	mmVoltSensor1Value	.1.3.6.1.4.1.116.5.39.3.3.2.1.3	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (3/7)

No	Object identifier	OID	Syntax	Access	Description
16	mmVoltSensor1Valid	.1.3.6.1.4.1.116.5.39.3.3.2.1.4	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
17	mmVoltSensor2Name	.1.3.6.1.4.1.116.5.39.3.3.2.1.5	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
18	mmVoltSensor2Value	.1.3.6.1.4.1.116.5.39.3.3.2.1.6	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
19	mmVoltSensor2Valid	.1.3.6.1.4.1.116.5.39.3.3.2.1.7	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
20	mmVoltSensor3Name	.1.3.6.1.4.1.116.5.39.3.3.2.1.8	Display String	RO	Shows the voltage sensor name for the management module installed in the slot shown in #5. (*4)
21	mmVoltSensor3Value	.1.3.6.1.4.1.116.5.39.3.3.2.1.9	Integer32	RO	Shows the voltage value of the management module installed in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
22	mmVoltSensor3Valid	.1.3.6.1.4.1.116.5.39.3.3.2.1.10	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (4/7)

No	Object identifier	OID	Syntax	Access	Description
23	mmVoltSensor 4Name	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.11	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
24	mmVoltSensor 4Value	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.12	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
25	mmVoltSensor 4Valid	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.13	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
26	mmVoltSensor 5Name	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.14	Display String	RO	Shows the voltage sensor name for the switch and management module installed in the slot shown in #5. (*4)
27	mmVoltSensor 5Value	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.15	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1 V. The actual value is one-tenth of the response value.
28	mmVoltSensor 5Valid	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.16	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
29	mmVoltSensor 6Name	.1.3.6.1.4.1.1 16.5.39.3.3.2 .1.17	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (5/7)

No	Object identifier	OID	Syntax	Access	Description
30	mmVoltSensor6 Value	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.18	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
31	mmVoltSensor6 Valid	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.19	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
32	mmVoltSensor7 Name	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.20	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
33	mmVoltSensor7 Value	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.21	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
34	mmVoltSensor7 Valid	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.22	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
35	mmVoltSensor8 Name	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.23	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
36	mmVoltSensor8 Value	.1.3.6.1.4.1 .116.5.39.3 .3.2.1.24	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (6/7)

No	Object identifier	OID	Syntax	Access	Description
37	mmVoltSensor8Valid	.1.3.6.1.4.1.116.5.39.3.3.2.1.25	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
38	mmVoltSensor9Name	.1.3.6.1.4.1.116.5.39.3.3.2.1.26	Display String	RO	Shows the voltage sensor name for the management module in the slot shown in #5. (*4)
39	mmVoltSensor9Value	.1.3.6.1.4.1.116.5.39.3.3.2.1.27	Integer32	RO	Shows the voltage value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1V. The actual value is one-tenth of the response value.
40	mmVoltSensor9Valid	.1.3.6.1.4.1.116.5.39.3.3.2.1.28	INTEGER	RO	Shows the voltage value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
41	mmTemperatureTable	.1.3.6.1.4.1.116.5.39.3.3.3	Not-Accessible	NA	Shows the table of information on the management module temperature sensor.
42	mmTemperatureEntry	.1.3.6.1.4.1.116.5.39.3.3.3.1	Not-Accessible	NA	Shows the table entry describing the information on the management module temperature sensor.
43	mmTempIndex	.1.3.6.1.4.1.116.5.39.3.3.3.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMm to identify the table entry.
44	mmTempSensor1Name	.1.3.6.1.4.1.116.5.39.3.3.3.1.2	Display String	RO	Shows the temperature sensor name for the management module in the slot shown in #5. (*4)

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(b) moduleStatusMm group (7/7)

No	Object identifier	OID	Syntax	Access	Description
45	mmTempSensor1Value	.1.3.6.1.4.1.116.5.39.3.3.3.1.3	Integer32	RO	Shows the temperature value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
46	mmTempSensor1Valid	.1.3.6.1.4.1.116.5.39.3.3.3.1.4	INTEGER	RO	Shows the temperature value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown
47	mmTempSensor2Name	.1.3.6.1.4.1.116.5.39.3.3.3.1.5	Display String	RO	Shows the temperature sensor name for the management module in the slot shown in #5. (*4)
48	mmTempSensor2Value	.1.3.6.1.4.1.116.5.39.3.3.3.1.6	Integer32	RO	Shows the temperature value of the management module in the slot shown in #5. (*5) The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value.
49	mmTempSensor2Valid	.1.3.6.1.4.1.116.5.39.3.3.3.1.7	INTEGER	RO	Shows the temperature value validity of the management module in the slot shown in #5. One of the following values is shown. (*6) 1: invalid 2: valid 3: unknown

(*1) “unknown” is shown in the process of setting redundancy, or when no management module is installed or the status cannot be obtained.

(*2) “unknown” is shown when no management module is installed or the status cannot be obtained. ”power-off” is shown after executing SDN in the process of setting redundancy.

(*3) “0” is shown as the number of sensor when no management module is installed.

(*4) “Not install” is shown if no management module is installed or redundancy setting is on the process; “Cannot get data” is shown if the data cannot be obtained.

(*5) “0” is shown if no management module is installed or redundancy setting is on the process, if the data cannot be obtained, or if no sensor exists.

(*6) “invalid” is shown if no management module is installed or redundancy setting is on the process; “unknown” is shown if no data is obtained”.

(c) moduleStatusSw group

This group consists of one table: swStatusTable for the entire information on the switch module.

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusSw	.1.3.6.1.4.1.116.5.39.3.4	Not-Accessible	NA	Shows the switch module status.
2	swStatusTable	.1.3.6.1.4.1.116.5.39.3.4.1	Not-Accessible	NA	Shows the table of information on the switch module status.
3	swStatusEntry	.1.3.6.1.4.1.116.5.39.3.4.1.1	Not-Accessible	NA	Shows the table entry describing the information on the switch module status.
4	swStatusIndex	.1.3.6.1.4.1.116.5.39.3.4.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityISw to identify the table entry.
5	swStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.4.1.1.2	Integer32	RO	Shows the switch module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacitySw–1.
6	swStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.4.1.1.3	INTEGER	RO	Shows the status of the switch module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	swStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.4.1.1.4	INTEGER	RO	Shows the status of the switch module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown

(*1) “unknown” is shown when no switch module is installed or the status data cannot be obtained.

(d) moduleStatusFan group (1/2)

This group consists of two tables: fanStatusTable for the entire information on the fan module, and fanRpmTable for the RPM information on the fan module.

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusFan	.1.3.6.1.4.1.116.5.39.3.6	Not-Accessible	NA	Shows the status of a fan module.
2	fanStatusTable	.1.3.6.1.4.1.116.5.39.3.6.1	Not-Accessible	NA	Shows the table of information on the fan module status.
3	fanStatusEntry	.1.3.6.1.4.1.116.5.39.3.6.1.1	Not-Accessible	NA	Shows the table entry describing the information on the fan module status.
4	fanStatusIndex	.1.3.6.1.4.1.116.5.39.3.6.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityFan to identify the table entry.
5	fanStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.6.1.1.2	Integer32	RO	Shows the fan module slot number corresponding to the index shown in #4, ranging from 0 to chassisCapacityFan–1.
6	fanStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.6.1.1.3	INTEGER	RO	Shows the status of the fan module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	fanStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.6.1.1.4	INTEGER	RO	Shows the status of the fan module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown
8	fanStatusSensorCapacityTacho	.1.3.6.1.4.1.116.5.39.3.6.1.1.5	Integer32	RO	Shows the number of fan units in the fan module in the slot shown in #5. “3” is always shown.
9	fanRpmTable	.1.3.6.1.4.1.116.5.39.3.6.2	Not-Accessible	NA	Shows the table describing RPM status of a fan module.

(*1) “unknown” is shown when no fan module is installed or the status data cannot be obtained.

(d) moduleStatusFan group (2/2)

No	Object identifier	OID	Syntax	Access	Description
10	fanRpmEntry	.1.3.6.1.4.1.116.5.39.3.6.2.1	Not-Accessible	NA	Shows the entry of the table describing RPM status of a fan module.
11	fanRpmIndex	.1.3.6.1.4.1.116.5.39.3.6.2.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityFan to identify the table entry.
12	fan1RpmValue	.1.3.6.1.4.1.116.5.39.3.6.2.1.2	Integer32	RO	Shows the RPM value of the first fan in the fan module installed in the slot shown in #5.
13	fan1RpmValid	.1.3.6.1.4.1.116.5.39.3.6.2.1.3	INTEGER	RO	Shows the RPM validity of the first fan in the fan module installed in the slot shown in #5. Usually one of the following messages is shown. (*1) 1: invalid 2: valid 3: unknown
14	fan2RpmValue	1.3.6.1.4.1.116.5.39.3.6.2.1.4	Integer32	RO	Shows the RPM value of the second fan in the fan module installed in the slot shown in #5.
15	fan2RpmValid	1.3.6.1.4.1.116.5.39.3.6.2.1.5	INTEGER	RO	Shows the RPM validity of the second fan in the fan module installed in the slot shown in #5. Usually one of the following messages is shown. (*1) 1: invalid 2: valid 3: unknown
16	fan3RpmValue	1.3.6.1.4.1.116.5.39.3.6.2.1.6	Integer32	RO	Shows the RPM value of the third fan in the fan module installed in the slot shown in #5.
17	fan3RpmValid	1.3.6.1.4.1.116.5.39.3.6.2.1.7	INTEGER	RO	Shows the RPM validity of the third fan in the fan module installed in the slot shown in #5. Usually one of the following messages is shown. (*1) 1: invalid 2: valid 3: unknown

(*1) “unknown” is shown when no fan module is installed or the status data cannot be obtained.

(e) moduleStatusPs group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusPs	.1.3.6.1.4.1.116.5.39.3.7	Not-Accessible	NA	Shows the status of a power supply.
2	psStatusTable	.1.3.6.1.4.1.116.5.39.3.7.1	Not-Accessible	NA	Shows the table of information on the power supply module status.
3	psStatusEntry	.1.3.6.1.4.1.116.5.39.3.7.1.1	Not-Accessible	NA	Shows the table entry describing the information on the power supply module status.
4	psStatusIndex	.1.3.6.1.4.1.116.5.39.3.7.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPs to identify the table entry.
5	psStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.7.1.1.2	Integer32	RO	Shows the slot number of the power supply corresponding to the index value shown in #4 ranging from 0 to chassisCapacityPs-1.
6	psStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.7.1.1.3	INTEGER	RO	Shows the status of the power supply module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	psStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.7.1.1.4	INTEGER	RO	Shows the status of the power supply module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown
8	psTemperatureTable	.1.3.6.1.4.1.116.5.39.3.7.2	Not-Accessible	NA	Shows the table of information on the power supply module temperature.
9	psTemperatureEntry	.1.3.6.1.4.1.116.5.39.3.7.2.1	Not-Accessible	NA	Shows the table entry describing the information on the power supply module temperature.
10	psTempIndex	.1.3.6.1.4.1.116.5.39.3.7.2.1.1	Integer32	RO	Shows the index value of the power supply module temperature.

(*1) “unknown” is shown when no power supply module is installed or no data can be obtained.

(*2) ”0” is shown when no power supply module is installed or no data can be obtained.

(*3) “invalid” is shown if no power supply module is installed.

(e) moduleStatusPs group (2/2)

No	Object identifier	OID	Syntax	Access	Description
11	psTempAmbientValue	.1.3.6.1.4.1.116.5.39.3.7.2.1.2	Integer32	RO	Shows the inlet air temperature value of the power supply module in the slot shown in #5. The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value. (*2)
12	psTempAmbientValid	.1.3.6.1.4.1.116.5.39.3.7.2.1.3	INTEGER	RO	Shows the inlet air temperature value validity of the power supply module in the slot shown in #5. One of the following values is shown. (*3) 1: invalid 2: valid 3: unknown
13	psTempHotSpotValue	.1.3.6.1.4.1.116.5.39.3.7.2.1.4	Integer32	RO	Shows the HotSpot temperature value of the power supply module in the slot shown in #5. The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value. (*2)
14	psTempHotSpotValid	.1.3.6.1.4.1.116.5.39.3.7.2.1.5	INTEGER	RO	Shows the HotSpot temperature value validity of the power supply module in the slot shown in #5. One of the following values is shown. (*3) 1: invalid 2: valid 3: unknown
15	psTempExhaustValue	.1.3.6.1.4.1.116.5.39.3.7.2.1.6	Integer32	RO	Shows the exhaust air temperature value of the power supply module in the slot shown in #5. The value is shown using the unit of 0.1°C. The actual value is one-tenth of the response value. (*2)
16	psTempExhaustValid	.1.3.6.1.4.1.116.5.39.3.7.2.1.7	INTEGER	RO	Shows the exhaust air temperature value validity of the power supply module in the slot shown in #5. One of the following values is shown. (*3) 1: invalid 2: valid 3: unknown

(*1) “unknown” is shown when no power supply module is installed or no data can be obtained.

(*2) ”0” is shown when no power supply module is installed or no data can be obtained.

(*3) “invalid” is shown if no power supply module is installed.

(f) moduleStatusPciRiser group

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusPciRiser	.1.3.6.1.4.1.116.5.39.3.9	Not-Accessible	NA	Shows the status of a PCI-e Riser card (IOCD module).
2	pciRiserStatusTable	.1.3.6.1.4.1.116.5.39.3.9.1	Not-Accessible	NA	Shows the table of information on the PCI-e Riser card (IOCD module) status.
3	pciRiserStatusEntry	.1.3.6.1.4.1.116.5.39.3.9.1.1	Not-Accessible	NA	Shows the table entry describing the information on the PCI-e Riser card (IOCD module) status.
4	pciRiserStatusIndex	.1.3.6.1.4.1.116.5.39.3.9.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPciRiser to identify the table entry.
5	pciRiserStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.9.1.1.2	Integer32	RO	Shows the slot number of the power supply corresponding to the index value shown in #4 ranging from 0 to chassisCapacityPciRiser-1.
6	pciRiserStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.9.1.1.3	INTEGER	RO	Shows the power status of the PCI-e Riser card (IOCD module) installed in the slot shown in #5. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown

(*1) “unknown” is shown when no PCI-e Riser card (IOCD module) is installed or no data can be obtained.

(g) moduleStatusPcieSw group

This item is not supported.

This group consists of one table: pcieSwStatusTable to show the entire PCI Express switch module information.

No	Object identifier	OID	Syntax	Access	Description
1	moduleStatusPcieSw	.1.3.6.1.4.1.116.5.39.3.10	Not-Accessible	NA	Shows the status of a PCI Express switch module.
2	pcieSwStatusTable	.1.3.6.1.4.1.116.5.39.3.10.1	Not-Accessible	NA	Shows the table of information on the PCI Express switch module status.
3	pcieSwStatusEntry	.1.3.6.1.4.1.116.5.39.3.10.1.1	Not-Accessible	NA	Shows the table entry describing the information on the PCI Express switch module status.
4	pcieSwStatusIndex	.1.3.6.1.4.1.116.5.39.3.10.1.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityPcieSw to identify the table entry.
5	pcieSwStatusSlotnum	.1.3.6.1.4.1.116.5.39.3.10.1.1.2	Integer32	RO	Shows the slot number of the PCI Express switch module corresponding to the index value shown above ranging from 0 to chassisCapacityPcieSw-1.
6	pcieSwStatusHealthStatus	.1.3.6.1.4.1.116.5.39.3.10.1.1.3	INTEGER	RO	Shows the status of the PCI Express switch module Rinstalled in the slot shown in #5. One of the following messages is shown. (*1) 1: normal 2: fail 3: unknown
7	pcieSwStatusPowerStatus	.1.3.6.1.4.1.116.5.39.3.10.1.1.4	INTEGER	RO	Shows the power status of the PCI Express switch module installed in the slot shown in #5. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: booting 5: shutdown

(*1) “unknown” is shown when no PCI Express switch module is installed or no data can be obtained.

4 partitionConfig

partitionConfig consists of the following four groups: partitionConfigCapacity and three tables such as partitionConfigTable, partitionBladeTable, and partitionPciRiserTable. Each group is described in the following table (a) to (d).

(a) partitionConfigCapacity group

No	Object identifier	OID	Syntax	Access	Description
1	partitionConfigCapacity	.1.3.6.1.4.1.116.5.39.4.1	Integer32	RO	Shows the maximum number of partitions in a server chassis. The response is always “8”.

(b) partitionConfigTable group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	partitionConfigTable	.1.3.6.1.4.1.116.5.39.4.2	Not-Accessible	NA	Shows the table of the information on a partition configuration.
2	partitionConfigEntry	.1.3.6.1.4.1.116.5.39.4.2.1	Not-Accessible	NA	Shows the table entry describing the information on the partition configuration.
3	partitionConfigIndex	.1.3.6.1.4.1.116.5.39.4.2.1.1	Integer32	RO	Shows the index value ranging from 1 to partitionConfigCapacity to identify the table entry.
4	partitionConfigPrimaryBladeNum	.1.3.6.1.4.1.116.5.39.4.2.1.2	Integer32	RO	Shows the primary blade number of the partition corresponding to the index value shown in #3 ranging from 0 to partitionConfigCapacity-1. (*1)
5	partitionConfigBladeCount	.1.3.6.1.4.1.116.5.39.4.2.1.3	Integer32	RO	Shows the number of blades that belong to the partition corresponding to the index value shown in #4. (*1)
6	partitionConfigValid	.1.3.6.1.4.1.116.5.39.4.2.1.4	INTEGER	RO	Shows whether or not the partitions shown in #4 exist. One of the following messages is shown. (*2) 1: exist 2: no-exist 3: unknown

(*1) “-1” is shown when no partition corresponding to the index value exists.

(*2) “unknown” is shown when no partition existence data can be obtained.

(*3) “Not Installed” is shown when no partition exists, no server blades corresponding to the partition installed, or no LPAR manager license given to the server blade corresponding to the partition.

(*4) “0” is shown when no partition exists, or no server blades corresponding to the partition installed.

(b) partitionConfigTable group (2/2)

No	Object identifier	OID	Syntax	Access	Description
7	partitionConfigDetailHvmLicense	.1.3.6.1.4.1.116.5.39.4.2.1.5	DisplayString	RO	Shows the detailed LPAR manager license currently given to the partition shown in #4. (*3)
8	partitionConfigMaxCurrent	.1.3.6.1.4.1.116.5.39.4.2.1.6	Integer32	RO	Shows the max current value consumed by the partition shown in #4. The value is shown 1 for 0.1A. (*4)
9	partitionConfigMaxPower	.1.3.6.1.4.1.116.5.39.4.2.1.7	Integer32	RO	Shows the rated power value of the partition shown in #4. The value is shown 1 for 1W. (*4)
10	partitionConfigTotalAmountOfDimm	.1.3.6.1.4.1.116.5.39.4.2.1.8	Integer32	RO	Shows the total DIMM amount available for the entire partition. This value is shown as 1 for 1 GB. (*1)

(*1) “-1” is shown when no partition corresponding to the index value exists.

(*2) “unknown” is shown when no partition existence data can be obtained.

(*3) “Not Installed” is shown when no partition exists, no server blades corresponding to the partition installed, or no LPAR manager license given to the server blade corresponding to the partition.

(*4) “0” is shown when no partition exists, or no server blades corresponding to the partition installed.

(c) partitionBladeTable group

No	Object identifier	OID	Syntax	Access	Description
1	partitionBladeTable	.1.3.6.1.4.1.116.5.39.4.3	Not-Accessible	NA	Shows the table of the information on the blade configuration of a partition.
2	partitionBladeEntry	.1.3.6.1.4.1.116.5.39.4.3.1	Not-Accessible	NA	Shows the table entry describing the information on the partition configuration.
3	partitionBladeIndex	.1.3.6.1.4.1.116.5.39.4.3.1.1	Integer32	RO	Shows the index value ranging from 1 to partitionConfigCapacity to identify the table entry.
4	partitionBladePartitionNum	.1.3.6.1.4.1.116.5.39.4.3.1.2	Integer32	RO	Shows the partition number corresponding to the index value shown in #3: a value from 0- to partitionConfigCapacity-1.
5	partitionBladeSlotNum1	.1.3.6.1.4.1.116.5.39.4.3.1.3	Integer32	RO	Shows the primary blade slot number of the partition corresponding to the index value shown in #4. (*1)
6	partitionBladeSlotNum2	.1.3.6.1.4.1.116.5.39.4.3.1.4	Integer32	RO	Shows the slot location of the 2nd server blade that belongs in the partition corresponding to the #4 value. (*1)
7	partitionBladeSlotNum3	.1.3.6.1.4.1.116.5.39.4.3.1.5	Integer32	RO	Shows the slot location of the 3rd server blade that belongs in the partition corresponding to the #4 value. (*1)
8	partitionBladeSlotNum4	.1.3.6.1.4.1.116.5.39.4.3.1.6	Integer32	RO	Shows the slot location of the 4th server blade that belongs in the partition corresponding to the #4 value. (*1)

(*1) "-1" is shown when no partition corresponding to the index value exists or no partition existence data can be obtained.

(d) partitionPciRiserTable group

No	Object identifier	OID	Syntax	Access	Description
1	partitionPciRiserTable	.1.3.6.1.4.1.116.5.39.4.5	Not-Accessible	NA	Shows the table of the information on the I/O board module configuration.
2	partitionPciRiserEntry	.1.3.6.1.4.1.116.5.39.4.5.1	Not-Accessible	NA	Shows the table entry describing the information on the partition configuration.
3	partitionPciRiserIndex	.1.3.6.1.4.1.116.5.39.4.5.1.1	Integer32	RO	Shows the index value ranging from 1 to partitionConfigCapacity to identify the table entry.
4	partitionPciRiserPartitionNum	.1.3.6.1.4.1.116.5.39.4.5.1.2	Integer32	RO	Shows the partition number corresponding to the index in #3. A value from 0 to partitionConfigCapacity-1
5	partitionPciRiserSlotNum1	.1.3.6.1.4.1.116.5.39.4.5.1.3	Integer32	RO	Shows the slot number of the 1st I/O board module that belongs to the partition in #4. (*1)
6	partitionPciRiserSlotNum2	.1.3.6.1.4.1.116.5.39.4.5.1.4	Integer32	RO	Shows the slot number of the 2nd I/O board module that belongs to the partition in #4. (*1)
7	partitionPciRiserSlotNum3	.1.3.6.1.4.1.116.5.39.4.5.1.5	Integer32	RO	Shows the slot number of the 3rd I/O board module that belongs to the partition in #4. (*1)
8	partitionPciRiserSlotNum4	.1.3.6.1.4.1.116.5.39.4.5.1.6	Integer32	RO	Shows the slot number of the 4th I/O board module that belongs to the partition in #4. (*1)
9	partitionPciRiserSlotNum5	.1.3.6.1.4.1.116.5.39.4.5.1.7	Integer32	RO	Shows the slot number of the 5th I/O board module that belongs to the partition in #4. (*1)
10	partitionPciRiserSlotNum6	.1.3.6.1.4.1.116.5.39.4.5.1.8	Integer32	RO	Shows the slot number of the 6th I/O board module that belongs to the partition in #4. (*1)
11	partitionPciRiserSlotNum7	.1.3.6.1.4.1.116.5.39.4.5.1.9	Integer32	RO	Shows the slot number of the 7th I/O board module that belongs to the partition in #4. (*1)
12	partitionPciRiserSlotNum8	.1.3.6.1.4.1.116.5.39.4.5.1.10	Integer32	RO	Shows the slot number of the 8th I/O board module that belongs to the partition in #4. (*1)

(*1) “-1” is shown when no partition corresponding to the index value exists, no partition existence data can be obtained.

5 partitionStatus

partitionStatus consists of one table group, partitionStatus, which describes in the following table.

(a) partitionStatusTable group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	partitionStatusTable	.1.3.6.1.4.1.116.5.39.5.1	Not-Accessible	NA	Shows the table of the information on the partition status.
2	partitionStatusEntry	.1.3.6.1.4.1.116.5.39.5.1.1	Not-Accessible	NA	Shows the table entry describing the information on the partition configuration.
3	partitionStatusIndex	.1.3.6.1.4.1.116.5.39.5.1.1.1	Integer32	RO	Shows the index value ranging from 1 to partitionConfigCapacity to identify the table entry.
4	partitionStatusPartitionNum	.1.3.6.1.4.1.116.5.39.5.1.1.2	Integer32	RO	Shows the partition number corresponding to the index value shown in #3 ranging from 0 to partitionConfigCapacity-1.
5	partitionStatusPowerStatus	.1.3.6.1.4.1.116.5.39.5.1.1.3	INTEGER	RO	Shows the power status of the partition corresponding to the partition number shown in #4. One of the following messages is shown. (*1) 1: power-off 2: power-on 3: unknown 4: pre-configure 5: booting 6:shutdonw
6	partitionStatusRunningMode	.1.3.6.1.4.1.116.5.39.5.1.1.4	INTEGER	RO	Shows the maintenance mode status of the partition corresponding to the partition number shown in #4. (*2) One of the following messages is shown. 1: normal 2: maintenance 3: unknown

(*1) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(*2) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(*3) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(a) partitionStatusTable group (2/2)

No	Object identifier	OID	Syntax	Access	Description
7	partitionStatusHvmMode	.1.3.6.1.4.1.116.5.39.5.1.1.5	INTEGER	RO	Shows the LP mode running status of the partition corresponding to the partition number shown in #4. One of the following messages is shown. (*3) 1: normal 2: hvm 3: unknown
8	partitionStatusCurrentCurrent	.1.3.6.1.4.1.116.5.39.5.1.1.6	Integer32	RO	Shows the current that currently consumed by the partition in #4. This value is shown as 1 for 1W. (*4)
9	partitionStatusCurrentPower	.1.3.6.1.4.1.116.5.39.5.1.1.7	Integer32	RO	Shows the power that currently consumed by the partition in #4. This value is shown as 1 for 1W. (*4)

(*1) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(*2) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(3*) “unknown” is shown when no partition exists or no partition existence data can be obtained.

(*4) “0” is shown when no partition exists or no server blade corresponding to the partition installed.

6 chassisStatus

(a) chassisStatusSystem group (1/3)

No	Object identifier	OID	Syntax	Access	Description
1	chassisStatusSystem	.1.3.6.1.4.1.116.5.39.6.1	Not-Accessible	NA	Shows the chassis status.
2	chassisStatusRedundancySvp	.1.3.6.1.4.1.116.5.39.6.1.1	INTEGER	RO	Shows the redundancy status of the management module. One of the following messages is shown. 1: redundancy 2: non-redundancy 3: unknown
3	chassisStatusRedundancyFan	.1.3.6.1.4.1.116.5.39.6.1.2	INTEGER	RO	Shows the redundancy status of the fan module. One of the following messages is shown. 1: redundancy 2: non-redundancy 3: unknown
4	chassisStatusRedundancyPs	.1.3.6.1.4.1.116.5.39.6.1.3	INTEGER	RO	Shows the redundancy status of the power supply module. One of the following messages is shown. 1: redundancy 2: non-redundancy 3: unknown
5	chassisStatusCurrentTemp	.1.3.6.1.4.1.116.5.39.6.1.4	Integer32	RO	Shows the inlet air temperature of the server chassis. This value is shown as 1 for 0.1°C. (*1)
6	chassisStatusCurrentCurrency	.1.3.6.1.4.1.116.5.39.6.1.5	Integer32	RO	Shows the current consumed by the server chassis using the unit of 0.1A.
7	chassisStatusCurrentPower	.1.3.6.1.4.1.116.5.39.6.1.6	Integer32	RO	Shows the power consumed by the server chassis using the unit of 0.1kW.
8	chassisStatusFanAirVolume	.1.3.6.1.4.1.116.5.39.6.1.7	Integer32	RO	Shows the air volume provided by the server chassis using the unit of 0.1m^3/min.
9	chassisStatusIntakeTemp	.1.3.6.1.4.1.116.5.39.6.1.8	INTEGER	RO	Shows the inlet air status of the server chassis. One of the following messages is shown. (*2) 1: normal 2. higher-warning 3. error-warning 4: lower-warning

(*1) “0” is shown when all server blades installed in the chassis are powered off.

(*2) “1” is shown when all server blades installed in the chassis are powered off.

(*3) This LED is always “turn-off”.

(a) chassisStatusSystem group (2/3)

No	Object identifier	OID	Syntax	Access	Description
10	chassisStatusLedNode	.1.3.6.1.4.1.116.5.39.6.1.9	INTEGER	RO	Shows the Node LED status on the front panel of the server chassis. One of the following messages is shown. 1: turn-off 2: turn-on
11	chassisStatusLedSw	.1.3.6.1.4.1.116.5.39.6.1.10	INTEGER	RO	Shows the SW LED status on the front panel of the server chassis. One of the following messages is shown. 1: off 2: on
12	chassisStatusLedPs	.1.3.6.1.4.1.116.5.39.6.1.11	INTEGER	RO	Shows the PS LED status on the front panel of the server chassis. One of the following messages is shown. 1: turn-off 2: turn-on
13	chassisStatusLedFan	.1.3.6.1.4.1.116.5.39.6.1.12	INTEGER	RO	Shows the Fan LED status on the front panel of the server chassis. One of the following messages is shown. 1: turn-off 2: turn-on
14	chassisStatusLedTemp	.1.3.6.1.4.1.116.5.39.6.1.13	INTEGER	RO	Shows the temperature LED (TEP) status on the front panel of the server chassis. One of the following messages is shown. 1: turn-off 2: turn-on
15	chassisStatusLedDev	.1.3.6.1.4.1.116.5.39.6.1.14	INTEGER	RO	Shows LED status of a device installed in the server blade on the front panel of the server chassis. One of the following messages is shown. (*3) 1: turn-off 2: turn-on
16	chassisStatusMarlogLatestInfo	.1.3.6.1.4.1.116.5.39.6.1.15	DisplayString	RO	Shows the information of the latest MAR (Maintenance Action Report) log.
17	chassisStatusMarlogInfoTable	.1.3.6.1.4.1.116.5.39.6.1.16	Not-Accessible	NA	Shows the table of information on MAR (Maintenance Action Report) logs.

(*1) “0” is shown when all server blades installed in the chassis are powered off.

(*2) “1” is shown when all server blades installed in the chassis are powered off.

(*3) This LED is always “turn-off”.

(a) chassisStatusSystem group (3/3)

No	Object identifier	OID	Syntax	Access	Description
18	chassisStatusMarlogInfoEntry	.1.3.6.1.4.1.1116.5.39.6.1.16.1	Not-Accessible	NA	Shows the table entry describing the information on MAR (Maintenance Action Report) logs.
19	chassisStatusMarlogInfoIndex	.1.3.6.1.4.1.1116.5.39.6.1.16.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMarlog to identify the table entry.
20	chassisStatusMarlogInfoData	.1.3.6.1.4.1.1116.5.39.6.1.16.1.2	DisplayString	RO	Shows the MAR (Maintenance Action Report) log information data corresponding to the index value shown in #18.

(*1) “0” is shown when all server blades installed in the chassis are powered off.

(*2) “1” is shown when all server blades installed in the chassis are powered off.

(*3) This LED is always “turn-off”.

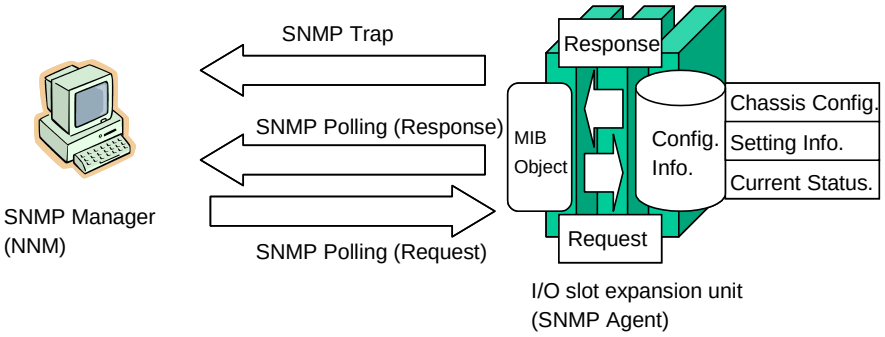
SNMP function for I/O slot expansion unit

SNMP function overview for I/O slot expansion unit

(1) Functions

No.	Function	Description
1	Polling	Allows the SNMP manager to recognize an I/O slot expansion unit as a target to monitor. When the manager requests information on each object of the I/O slot expansion unit private MIB (Management Information Base), a response corresponding to the information on the I/O slot expansion unit private MIB object is returned.
2	Trap	Sends information spontaneously to the manager according to the I/O slot expansion unit private MIB. This enables the SNMP manager to monitor faults.

The following image shows management by SNMP.



1. SNMP Polling Function

Item	Description
Support command (*1)	SNMPv1/v2c/v3 (Get, GetNext, GetBulk)
Maximum number of SNMP managers that can be notified simultaneously	4
Supported modules	I/O slot expansion unit chassis, power supply module, fan module, slot for PCI express, and port for server chassis connection

(*1) the Set command is not supported.

2. Specifications of SNMP Trap Function

Item		Description
Means of notification		SNMP (SNMPv2Trap/SNMPv3Trap)
Maximum number of SNMP managers that can be notified simultaneously		4
Event of notification		When the SEL of I/O slot expansion unit faults is issued.
Content of messaging	Binding of the first variable (Standard)	Time when the alert was sent.
	Binding of the second variable (Standard)	Chassis ID
	Binding of the third variable	Alert level
	Binding of the fourth variable	Alert message
	Binding of the fifth variable	Location where the alert occurred
	Binding of the sixth variable	Alert ID See Alert Log Message in Chapter 11.

Note: This SNMP trap function does not support the SNMP standard trap.

3. Specifications of SNMPv3

Item	Description
Authentication: Hush method	MD5/SHA-1
Encryption method	DES/AES128

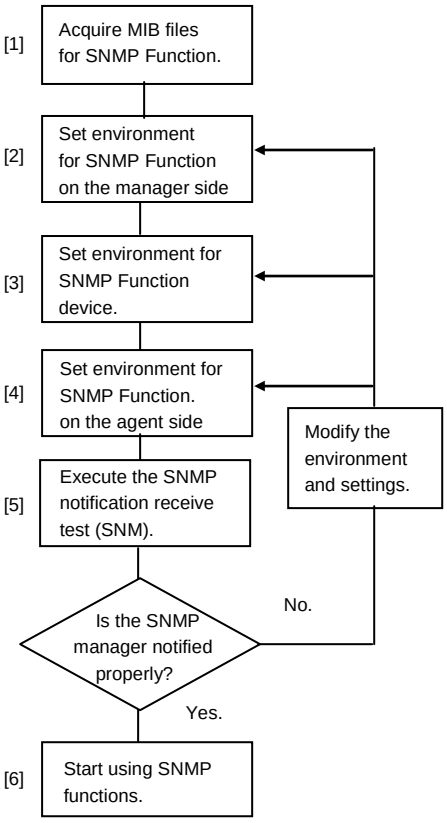
(2) Prerequisites

Prerequisites for using the SNMP function are listed in the table below.

No.	Prerequisites
1	The SNMP manager receiving SNMP traps must be compatible with SNMPv1/v2c/v3.
2	The environment must enable communications between the I/O slot expansion unit and the management server where the SNMP manager operates.

How to use the SNMP function for I/O slot expansion unit

(1) Procedure for SNMP



No.	Description
[1]	Acquire a MIB file that is required to perform the SNMP function.
[2]	Register the information in the MIB file acquired in step [1] into the SNMP manager.
[3]	Set the environment that allows SNMP trap function to perform.
[4]	Using the console, set the information required for SNMP functions, including the IP address of the destination SNMP manager and the name of a community for SNMPv1/v2c; the IP address of the destination SNMP manager, engine ID, access type, user name, and password for SNMPv3..
[5]	Using the test notification function, perform a test trap notification. If the SNMP manager fails to receive any test trap notification or receives notification of authentication error in SNMPv3Trap, review steps [2], [3], and [4] for correction.
[6]	The state is in normal operation.

(2) Acquiring MIB files for SNMP

Acquire MIB files from the SNMP agent by copying MIB files to the user directory with “SNM command” on the console of the I/O slot expansion unit.

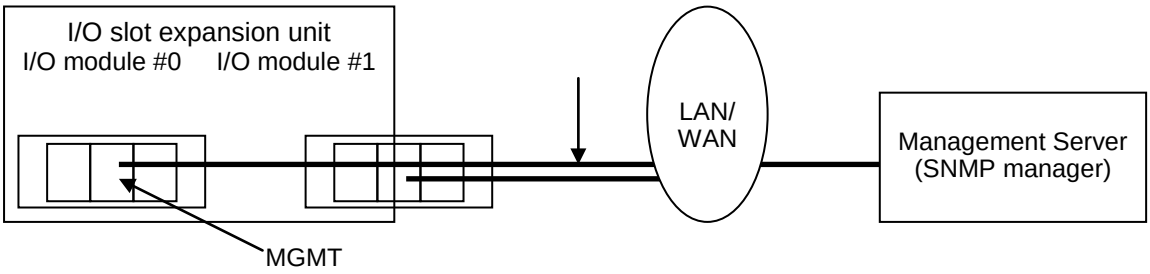
(3) Setting the information on the SNMP manager side

a. Setting the information for using the SNMP trap
Load the MIB for the I/O slot expansion unit and register the trap event to the manager by following the manual of your SNMP manager. All the trap events notified by this function are as follows:

No.	SNMP trap event name	OID	Description	Fault location
1	iodalertTrapIoxcNon-Recoverable	1.3.6.1.4.1.116.3.39.1 1.1.1.1	The I/O slot expansion unit encountered a fault at the fault level.	I/O slot expansion unit
2	iodalertTrapIoxcSerious	1.3.6.1.4.1.116.3.39.1 1.1.1.2	The I/O slot expansion unit encountered a fault at the warning level.	I/O slot expansion unit
3	iodalertTrapIoxcInformation	1.3.6.1.4.1.116.3.39.1 1.1.1.3	The I/O slot expansion unit encountered a fault at the information level.	I/O slot expansion unit
4	iodalertTrapIoxcEvent	1.3.6.1.4.1.116.3.39.1 1.1.1.4	The I/O slot expansion unit encountered an event at the event level.	I/O slot expansion unit

b. Setting the information for using the SNMP polling
Select MIB objects to acquire the information on the I/O slot expansion unit and configure the necessary settings to acquire the values by following the manual of your SNMP manager. Information obtained with the I/O slot expansion unit is shown in MIB reference.

(4) Example of environment configuration for SNMP



No.	Item	Description
1	SNMP manager	- It is necessary for a customer to obtain a management server equipped with an SNMP manager for receiving SNMP traps and processing SNMP requests. - The SNMP protocol essential for the SNMP manager to use is SNMPv1/v2c/v3.

(5) Setting the information on the SNMP agent side

Select the SNM command of the console for the I/O slot expansion unit > A. Edit agent setting and M. Edit manager setting to perform **Agent setting** and **Manager setting**, and then set the various items of information on the SNMP agent, the destination of SNMP traps, SNMP manager address, and community name.

(6) Performing SNMP tests

Select the SNM command of the console for the I/O slot expansion unit > T. SNMP trap test, and then perform **SNMP trap transmission** to perform the SNMP trap notification test.

(7) SNMP operation

Operate the SNMP function by following the information that is set with the console. When a fault occurs in the I/O slot expansion unit, obtain log files needed for fault analysis using the DL command if there is a request from maintenance personnel.

MIB reference for I/O slot expansion unit

(1) MIB tree structure

MIB supported by I/O slot expansion unit is comprised of MIB II objects and I/O slot expansion unit private MIB objects. The main tree structure is shown as follows:

```
root
|
iso(1)
  |
org(3)
  |
dod(6)
  |
internet(1)
  |
  +-mgmt(2)-+-system(1)       Device information
  |         |
  |         +-interface(2)    Interface information
  |         |
  |         +-at(3)           ARP information
  |         |
  |         +-ip(4)           IP information
  |         |
  |         +-icmp(5)         ICMP information
  |         |
  |         +-tcp(6)          TCP information
  |         |
  |         +-udp(7)          UDP information
  |         |
  |         +-snmp(11)        SNMP information
  |
  +-private(4)-private(1)-hitachi(116)-+-system(3)-HitachiComputeBlade(39)-+-bdsTrapcommon(0)
  |                                    |                                  |  (Common definition
  |                                    |                                  |   of I/O slot expansion
  |                                    |                                  |   unit private traps)
  |                                    |                                  +-iod(11)
  |                                    |                                  | (Trap definition
  |                                    |                                  |  for IOEU)
  |                                    +-systemExMib(5)–hitachiComputeBlade(39)-+-iod (11)
  |                                                                             |  (Chassis
  |                                                                             |   information)
  |                                                                             +-ioPsm (12)
  |                                                                             |  (Power module
  |                                                                             |  information)
  |                                                                             +ioFan (13)
  |                                                                             |  (Fan module
  |                                                                             |   information)
  |                                                                             +-ioPcie (14)
  |                                                                             |  (PCI Express slot.
  |                                                                             |   information)
  |                                                                             +-ioUpPort (15)
  |                                                                             |  (Server chassis
  |                                                                             |   connection port
  |                                                                             |   information)
```

(2) MIB description in the reference

This section shows the form to describe MIB in this reference, and explains the supported items to be described in the section about MIB objects.

1. Object Identifier

   The name of an MIB object identifier is shown.

2. OID (Object ID)

   OID corresponding to an MIB object identifier is shown.

3. SYNTAX

   The meaning of a syntax used in the private MIB is shown as follows:

No.	SYNTAX	Description
1	Not-Accessible	Access is not allowed.
2	Display String	A string consists of 0 to 2040 characters.
3	INTEGER	Integer value from -2147483648 to 2147483647
4	Integer32	Integer value from –2147483648 to 2147483647

4. Access

   RO: shows that MIB access is read-only.

   RW: shows that MIB access is read-write.

   NA: shows that MIB access is not-accessible.

(3) Supported standard MIB objects

Eight groups in the standard MIB, such as system, interfaces, at, ip, icmp, tcp, udp, and snmp, are supported. Objects in each group are partially supported. Supported MIB objects of each group are described in the table (a) to (h) shown below.

(a) system group

No	Object identifier	OID	Access	Description
1	sysDescr	.1.3.6.1.2.1 .1.1	NA	Describes the management equipment. This equipment has “Hitachi Compute Blade 2000 I/O slot expansion unit Ver XXXXX” as the fixed value. Ver XXXXX shows the firmware version of the I/O slot expansion unit.
2	sysObjectID	.1.3.6.1.2.1 .1.2	RO	Shows the vender OID of the management equipment. This equipment has the OID value of private.hitachi.system.hitachiComputeBlade.iod (.1.3.6.1.4.1.116.3.39.11) as the fixed value.
3	sysUpTime	.1.3.6.1.2.1 .1.3	RO	Shows the accumulated time by the 10msec after the SNMP agent boots up.
4	sysContact	.1.3.6.1.2.1 .1.4	RO (*1)	Shows the contact related to the management equipment, which is a character string set with a command.
5	sysName	.1.3.6.1.2.1 .1.5	RO (*1)	Shows the name related to the management equipment. The name is the chassis ID value.
6	sysLocation	.1.3.6.1.2.1 .1.6	RO (*1)	Shows the contact related to the management equipment, which is a character string set with a command.

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(b) interfaces group (1/2)

No	Object identifier	OID	Access	Description
1	ifNumber	.1.3.6.1.2.1.2.1	RO	Shows the number of interfaces that the management equipment has.
2	ifTable	.1.3.6.1.2.1.2.2	NA	Shows the table for setting interfaces.
3	ifEntry	.1.3.6.1.2.1.2.2.1	NA	Shows the list for setting interfaces.
4	ifIndex	.1.3.6.1.2.1.2.2.1.1	RO	Shows the number to identify each interface. The value is from 1 to ifNumber. (*1)
5	ifDescr	.1.3.6.1.2.1.2.2.1.2	RO	Shows the information on each interface. (*1)
6	ifType	.1.3.6.1.2.1.2.2.1.3	RO	Shows the type of each interface: Ethernet-csmacd (6) for this equipment. (*1)
7	ifMtu	.1.3.6.1.2.1.2.2.1.4	RO	Shows the maximum diagram size in octet that each interface can send and receive. (*1)
8	ifSpeed	.1.3.6.1.2.1.2.2.1.5	RO	Shows the current circuit speed of each interface in bit/s. (*1)
9	ifPhysAddress	.1.3.6.1.2.1.2.2.1.6	RO	Shows the physical address of each interface. (*1)
10	ifAdminStatus	.1.3.6.1.2.1.2.2.1.7	RO (*2)	Shows the desirable state of each interface. (*1) One of the following values is shown. * up (1) * down (2) * testing (3)
11	ifOperStatus	.1.3.6.1.2.1.2.2.1.8	RO	Shows the current status of each interface. (*1) One of the following values is shown. * up (1) * down (2) * testing (3)
12	ifInOctets	.1.3.6.1.2.1.2.2.1.10	RO	Shows the total number of octets that each interface has received. (*1)
13	ifInUcastPkts	.1.3.6.1.2.1.2.2.1.11	RO	Shows the number of unicast packets that each interface has received. (*1)
14	IfInNUcastPkts	.1.3.6.1.2.1.2.2.1.12	RO	Shows the number of non-unicast packets that each interface has received. (*1)
15	ifInDiscards	.1.3.6.1.2.1.2.2.1.13	RO	Shows the number of packets discarded not because of an error among incoming packets to each interface. (*1)
16	ifInErrors	.1.3.6.1.2.1.2.2.1.14	RO	Shows the number of error packets among incoming packets to each interface. (*1)
17	ifUnknown Prots	.1.3.6.1.2.1.2.2.1.15	RO	Shows the number of packets discarded due to the unsupported protocol among incoming packets to each interface. (*1)
18	ifOutOctets	.1.3.6.1.2.1.2.2.1.16	RO	Shows the total number of octets sent by each interface. (*1)

(*1) This object includes the information only on some interfaces.

(*2) This object is RW in the SNMP standard, but RO for this equipment.

(b) interfaces group (2/2)

No	Object identifier	OID	Access	Description
19	ifOutUcastPkts	.1.3.6.1.2.1.2.2.1.17	RO	Shows the number of unicast packets sent by each interface. (*1)
20	ifOutDiscards	.1.3.6.1.2.1.2.2.1.19	RO	Shows the number of packets discarded not because of an error among outgoing packets from each interface. (*1)
21	ifOutErrors	.1.3.6.1.2.1.2.2.1.20	RO	Shows the number of error packets among outgoing packets from each interface. (*1)
22	ifOutQLen	.1.3.6.1.2.1.2.2.1.21	RO	Shows the number of packets that each interface can store in the output queue. (*1)
23	ifSpecific	.1.3.6.1.2.1.2.2.1.22	RO	Shows the reference to MIB that specifies features of the interface media. It is the MIB object ID dependent on ifType. (*1)

(*1) This object includes the information only on some interfaces.
(*2) This object is RW in the SNMP standard, but RO for this equipment.

(c) at group

No	Object identifier	OID	Access	Description
1	atTable	.1.3.6.1.2.1.3.1	NA	Shows the Address Translation Table.
2	atEntry	.1.3.6.1.2.1.3.1.1	NA	Shows the entry of the Address Translation table.
3	atIfIndex	.1.3.6.1.2.1.3.1.1.1	RO	Shows the ifIndex value of the corresponding interface. (*1)
4	atPhysAddress	.1.3.6.1.2.1.3.1.1.2	RO	Shows the physical address. (*1)
5	atNetAddress	.1.3.6.1.2.1.3.1.1.3	RO	Shows the IP address corresponding to atPhysAddress. (*1)

(*1) This object includes the information only on some interfaces.

(d) ip group

No	Object identifier	OID	Access	Description
1	ipAddrTable	.1.3.6.1.2.1.4.20	NA	Shows the table related to an IP address.
2	ipAddrEntry	.1.3.6.1.2.1.4.20.1	NA	Shows the list of the table related to an IP address.
3	ipAdEntAddr	.1.3.6.1.2.1.4.20.1.1	RO	Shows an IP address. (*1)
4	ipAdEntIfIndex	.1.3.6.1.2.1.4.20.1.2	RO	Shows the index of an interface. (*1)
5	ipAdEntNetMask	.1.3.6.1.2.1.4.20.1.3	RO	Shows a Subnet mask. (*1)
6	ipAdEntBcastAddr	.1.3.6.1.2.1.4.20.1.4	RO	Shows the lowest bit value of a broadcast address. (*1)

(*1) This object includes the information only on some interfaces.

(e) icmp group (1/2)

No	Object identifier	OID	Access	Description
1	icmpInMsgs	.1.3.6.1.2.1.5.1	RO	Shows the total number of incoming ICMP messages.
2	icmpInErrors	.1.3.6.1.2.1.5.2	RO	Shows the number of incoming ICMP error messages.
3	icmpInDestUnreachs	.1.3.6.1.2.1.5.3	RO	Shows the total number of incoming “Destination Unreachable” messages.
4	icmpInTimeExcds	.1.3.6.1.2.1.5.4	RO	Shows the total number of incoming “TimeExceeded” messages.
5	icmpInParmProbs	.1.3.6.1.2.1.5.5	RO	Shows the total number of incoming “Parameter Problem” message s.
6	icmpInSrcQuenchs	.1.3.6.1.2.1.5.6	RO	Shows the total number of incoming “Source Quench” messages.
7	icmpInRedirects	.1.3.6.1.2.1.5.7	RO	Shows the total number of incoming “Redirect” messages.
8	icmpInEchos	.1.3.6.1.2.1.5.8	RO	Shows the total number of incoming “Echo Request” messages.
9	icmpInEchosReps	.1.3.6.1.2.1.5.9	RO	Shows the total number of incoming “Echo Reply” messages.
10	icmpInTimestamps	.1.3.6.1.2.1.5.10	RO	Shows the total number of incoming “Timestamp Request” messages.
11	icmpInTimestampsReps	.1.3.6.1.2.1.5.11	RO	Shows the total number of incoming “Timestamp Reply” messages.
12	icmpInAddMasks	.1.3.6.1.2.1.5.12	RO	Shows the total number of incoming “Address Mask Request” messages.
13	icmpInAddMasksReps	.1.3.6.1.2.1.5.13	RO	Shows the total number of t incoming “Address Mask Reply” messages.

(e) icmp group (2/2)

No	Object identifier	OID	Access	Description
14	icmpOutMsgs	.1.3.6.1.2.1.5.14	RO	Shows the total number of outgoing ICMP messages.
15	icmpOutErrors	.1.3.6.1.2.1.5.15	RO	Shows the total number of outgoing error ICMP messages.
16	icmpOutDestUnreachs	.1.3.6.1.2.1.5.16	RO	Shows the total number of outgoing “Destination Unreachable” messages.
17	icmpOutTimeExcds	.1.3.6.1.2.1.5.17	RO	Shows the total number of outgoing “TimeExceeded” messages.
18	icmpOutParmProbs	.1.3.6.1.2.1.5.18	RO	Shows the total number of outgoing “Parameter Problem” messages.
19	iIcmpOutSrcQuenchs	.1.3.6.1.2.1.5.19	RO	Shows the total number of outgoing “Source Quench” messages.
20	icmpOutRedirects	.1.3.6.1.2.1.5.20	RO	Shows the total number of outgoing “Redirect” messages.
21	icmpOutEchos	.1.3.6.1.2.1.5.21	RO	Shows the total number of outgoing “Echo Request” messages.
22	icmpOutEchosReps	.1.3.6.1.2.1.5.22	RO	Shows the total number of outgoing “Echo Reply” message.
23	icmpOutTimestamps	.1.3.6.1.2.1.5.23	RO	Shows the total number of outgoing “Timestamp Request” messages.
24	icmpOutTimestampsReps	.1.3.6.1.2.1.5.24	RO	Shows the total number of outgoing “Timestamp Reply” message.
25	icmpOutAddMasks	.1.3.6.1.2.1.5.25	RO	Shows the total number of outgoing “Address Mask Request” messages.
26	icmpOutAddMasksReps	.1.3.6.1.2.1.5.26	RO	Shows the total number of t outgoing “Address Mask Reply” messages.

(f) tcp group

No	Object identifier	OID	Access	Description
1	tcpConnTable	.1.3.6.1.2.1.6.13	NA	Shows the information table of TCP connection.
2	tcpConnEntry	.1.3.6.1.2.1.6.13.1	NA	Shows the information table entry of TCP connection.
3	tcpConnState	.1.3.6.1.2.1.6.13.1.1	RO (*1)	Shows the status of TCP connection. (*2) One of the following values is shown. · closed（1） · listen（2） · synSent（3） · synReceived（4） · established（5） · finWait1（6） · finWait2（7） · closeWait（8） · astAck（9） · closing（10） · timeWait（11） · deleteTCB（12）
4	tcpConnLocalAddress	.1.3.6.1.2.1.6.13.1.2	RO	Shows the local IP address of TCP connection. (*2)
5	tcpConnLocalPort	.1.3.6.1.2.1.6.13.1.3	RO	Shows the local port number of TCP connection. (*2)
6	tcpConnRemAddress	.1.3.6.1.2.1.6.13.1.4	RO	Shows the remote IP address of TCP connection. (*2)
7	tcpConnRemPort	.1.3.6.1.2.1.6.13.1.5	RO	Shows the remote port number of TCP connection. (*2)
8	tcpInErrs	.1.3.6.1.2.1.6.14	RO	Shows the number of incoming error segments.
9	tcpOutRsts	.1.3.6.1.2.1.6.15	RO	Shows the number of outgoing segments with the RST flag.

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object includes the information only on some interfaces.

(g) udp group

No	Object identifier	OID	Access	Description
1	udpConnTable	.1.3.6.1.2.1.7.5	NA	Shows the information table of UDP connection.
2	udpConnEntry	.1.3.6.1.2.1.7.5.1	NA	Shows the information table entry of UDP connection.
3	udpConnLocalAddress	.1.3.6.1.2.1.7.5.1.1	RO	Shows the local IP address of UDP connection. (*1)
4	udpConnLocalPort	.1.3.6.1.2.1.7.5.1.2	RO	Shows the local port number of UDP connection. (*1)

(*1) This object includes the information only on some interfaces.

(h) snmp group (1/2)

No	Object identifier	OID	Access	Description
1	snmpInPkts	.1.3.6.1.2.1.11.1	RO	Shows the total number of incoming SNMP messages.
2	snmpOutPkts	.1.3.6.1.2.1.11.2	RO	Shows the total number of SNMP outgoing messages.
3	snmpInBadVersions	.1.3.6.1.2.1.11.3	RO	Shows the total number of incoming unsupported version messages.
4	snmpInBadCommunityNames	.1.3.6.1.2.1.11.4	RO	Shows the total number of incoming unused community name messages.
5	snmpInBadCommunityUses	.1.3.6.1.2.1.11.5	RO	Shows the total number of incoming messages that describe the operation not allowed in the community.
6	snmpInASNParseErrs	.1.3.6.1.2.1.11.6	RO	Shows the total number of incoming “ASN.1 Error” messages.
7	snmpInTooBigs	.1.3.6.1.2.1.11.8	RO	Shows the total number of incoming PDUs whose error statuses are tooBig.
8	snmpInNoSuchNames	.1.3.6.1.2.1.11.9	RO	Shows the total number of incoming PDUs whose error statuses are noSuchName.
9	snmpInBadValues	.1.3.6.1.2.1.11.10	RO	Shows the total number of incoming PDUs whose error statuses are badValue.
10	snmpInReadOnlys	.1.3.6.1.2.1.11.11	RO	Shows the total number of incoming PDUs whose error statuses are readOnly.
11	snmpInGenErrs	.1.3.6.1.2.1.11.12	RO	Shows the total number of incoming PDUs whose error statuses are genErr.
12	snmpInTotalReqVars	.1.3.6.1.2.1.11.13	RO	Shows the total number of MIB objects that are successfully collected.
13	snmpInTotalSetVars	.1.3.6.1.2.1.11.14	RO	Shows the total number of MIB objects that are successfully set.
14	snmpInGetRequests	.1.3.6.1.2.1.11.15	RO	Shows the number of incoming “GetRequest” messages.
15	snmpInGetNexts	.1.3.6.1.2.1.11.16	RO	Shows the number of incoming “GetNext” messages.
16	snmpInSetRequests	.1.3.6.1.2.1.11.17	RO	Shows the number of incoming “SetRequest” messages.
17	snmpInGetResponses	.1.3.6.1.2.1.11.18	RO	Shows the number of incoming “GetResponce” messages.
18	snmpInTraps	.1.3.6.1.2.1.11.19	RO	Shows the number of incoming Traps.
19	snmpOutTooBigs	.1.3.6.1.2.1.11.20	RO	Shows the total number of outgoing PDUs whose error status is tooBig.
20	snmpOutNoSuchNames	.1.3.6.1.2.1.11.21	RO	Shows the total number of outgoing PDUs whose error status is noSuchName.
21	snmpOutBadValues	.1.3.6.1.2.1.11.22	RO	Shows the total number of outgoing PDUs whose error status is badValue.

(h) SNMP group (2/2)

No	Object identifier	OID	Access	Description
22	snmpOutReadOnlys	.1.3.6.1.2.1.11.23	RO	Shows the total number of outgoing PDUs whose error status is readOnly.
23	snmpOutGenErrs	.1.3.6.1.2.1.11.24	RO	Shows the total number of outgoing PDUs whose error status is genErr.
24	snmpOutGetRequests	.1.3.6.1.2.1.11.25	RO	Shows the number of outgoing “GetRequests” messages.
25	snmpOutGetNexts	.1.3.6.1.2.1.11.26	RO	Shows the number of outgoing “GetNexts” messages.
26	snmpOutSetRequests	.1.3.6.1.2.1.11.27	RO	Shows the number of outgoing “SetRequests” messages.
27	snmpOutGetResponces	.1.3.6.1.2.1.11.28	RO	Shows the number of outgoing “GetResponces” messages.
28	snmpOutTraps	.1.3.6.1.2.1.11.29	RO	Shows the number of outgoing Traps.
29	snmpEnableAuthenTraps	.1.3.6.1.2.1.11.30	RO (*1)	Shows whether or not to issue an authentication-failure Trap. · enable（1） · disable（2）
30	snmpSilentDrops	.1.3.6.1.2.1.11.31	RO	Shows the total number of SNMP incoming messages that were silently dropped because the reply size was greater than the maximum message size.
31	snmpProxyDrops	.1.3.6.1.2.1.11.32	RO	Shows the total number of SNMP incoming messages including GetRequest-PDU, GetNextRequest-PDU, GetBulkRequest-PDU, SetRequest-PDU, and InformRequest-PDU, which were silently dropped because the transmission of the message to a proxy target failed in a way that no response PDU could be returned.

(*1) This object includes the information only on some interfaces.

(4) Supported SNMPv2 MIB objects

snmpv2 group mainly describes information on SNMPv3.

This equipment supports items consisting of the following three groups: snmpFrameworkMIB, snmpUsmMIB, and snmpVacmMIB.

(a) snmpFrameworkMIB group

No	Object identifier	OID	Syntax	Description
1	snmpEngineID	.1.3.6.1.6.3.10.2.1.1	RO	Shows the engine ID value for SNMP engine management.
2	snmpEngineBoots	.1.3.6.1.6.3.10.2.1.2	RO	Shows how many times the SNMP engine (SNMP agent) has been booted after the last setting of a snmpEnginID.
3	snmpEngineTime	.1.3.6.1.6.3.10.2.1.3	RO	Shows how many seconds has passed after the last booting of the SNMP engine (SNMP agent).
4	snmpEngineMaxMessageSize	.1.3.6.1.6.3.10.1.1.4	RO	Shows the maximum size of message that the SNMP engine (SNMP agent) can send and receive. The value is fixed at 1,500 in this product.

(b) snmpUsmMIB group (1/2)

No	Object identifier	OID	Syntax	Description
1	usmStatsUnsupportedSecLevels	.1.3.6.1.6.3.15.1.1.1	RO	Shows the total number of received packets that are discarded for unsupported security levels.
2	usmStatsNotInTimeWindows	.1.3.6.1.6.3.15.1.1.2	RO	Shows the total number of received packets that are discarded for out of Window Time.
3	usmStatsUnknownUserNames	.1.3.6.1.6.3.15.1.1.3	RO	Shows the total number of received packets that are discarded for unknown users.
4	usmStatsUnknownEngineIDs	.1.3.6.1.6.3.15.1.1.4	RO	Shows the total number of received packets discarded for referring to unknown snmpEngine IDs.
5	usmStatsWrongDigests	.1.3.6.1.6.3.15.1.1.5	RO	Shows the total number of received packets discarded for excluding wrong digest values.
6	usmStatsDecryptionErrors	.1.3.6.1.6.3.15.1.1.6	RO	Shows the total number of received packets discarded for decryption errors.
7	usmUserSpinLock	.1.3.6.1.6.3.15.1.2.1	RO (*1)	Used for spin lock operation to change usmUserTable security.
8	usmUserTable	.1.3.6.1.6.3.15.1.2.2	RO	Shows the user table in Local Configuration Datastore (LCD) of the SNMP engine.
9	usmUserEntry	.1.3.6.1.6.3.15.1.1.2.1	RO	Shows the user table entry in Local Configuration Datastore (LCD) of the SNMP engine.
10	usmUserEngineID	.1.3.6.1.6.3.15.1.1.2.1.1	RO	Shows ID for managing the SNMP engine.
11	usmUserName	.1.3.6.1.6.3.15.1.1.2.1.2	RO	Readable user name: security ID on which USM depends.
12	usmUserSecurityName	.1.3.6.1.6.3.15.1.1.2.1.3	RO	Readable user name not depending on the security model: the same value as usmUserName.
13	usmUserCloneFrom	.1.3.6.1.6.3.15.1.1.2.1.4	RO (*1)	Shows a pointer to another entry from which a new entry is cloned. OID fixed at 0.0 (zerodotzero) is responded.
14	usmUserAuthProtocol	.1.3.6.1.6.3.15.1.1.2.1.5	RO	Authentication protocol of the SNMP engine shown in usmUserEngineID. One of the following values is shown: 1: sumNoAuthProtocol (No authentication) 2: usmHMACMD5AuthProtocol (MD5 authenticated) 3: usmHMACSHAAuthProtocol (SHA authenticated)

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(b) snmpUsmMIB group (2/2)

No	Object identifier	OID	Syntax	Description
15	usmUserAuthKeyChange	.1.3.6.1.6.3.15.1.1.2.1.6	RO (*1)	Object to create a snmp engine authentication key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from usmUserName of this entry. This object is fixed at ‘ ‘H.
16	usmUserOwnAuthKeyChange	.1.3.6.1.6.3.15.1.1.2.1.7	RO (*1)	Object to create a snmp engine authentication key shown in usmUserEngineID. This object is set when usmUserName is different from usmUserName of this entry. This object is fixed at ‘H‘.
17	usmUserPrivProtocol	.1.3.6.1.6.3.15.1.1.2.1.8	RO (*1)	Used by the privacy protocol of the SNMP engine shown in usmUserEngineID. One of the following values is shown: 1: usmNoPrivProtocol (No encryption) 2: usmDESPrivProtocol (DES encryption) 3: usmAesCfb128Protocol (AES encryption)
18	usmUserPrivKeyChange	.1.3.6.1.6.3.15.1.1.2.1.9	RO (*1)	Object to create an encryption key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from sumUserName of this entry.
19	usmUserOwnPrivKeyChange	.1.3.6.1.6.3.15.1.1.2.1.10	RO (*1)	Object to create an encryption key shown in usmUserEngineID. This object is set when usmUserName of a requester is different from sumUserName of this entry. This object is fixed at ‘ ‘H.
20	usmUserPublic	.1.3.6.1.6.3.15.1.1.2.1.11	RO (*1)	User authentication key: this value is created when an encryption key is changed. It can be used later to determine if the key change is enabled or not. This object is fixed at ‘ ’H.
21	usmUserStorageType	.1.3.6.1.6.3.15.1.1.2.1.12	RO (*1)	Storage type of the user entry. This value is fixed at permanent (4).
22	usmUserStatus	.1.3.6.1.6.3.15.1.1.2.1.13	RO (*1)	Shows status of the user entry. This value is fixed at activate (1).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(c) snmpVacmMIB group (1/2)

No	Object identifier	OID	Syntax	Description
1	vacmContext Table	.1.3.6.1.6.3.16 .1.5.1	NA	Shows the context table available locally.
2	vacmContext Entry	.1.3.6.1.6.3.16 .1.5.1.1	NA	Shows the context table entry available locally.
3	vacmContext Name	.1.3.6.1.6.3.16 .1.1.1.1.1	RO	Shows the readable name for a specific context in a specific SNMP entity. The empty contextName is the default context.
4	vacmSecurit yToGroupTa ble	.1.3.6.1.6.3.16 .1.2	RO	Shows the table for defining the access control policy to the operators group.
5	vacmSecurit yToGroupEn try	.1.3.6.1.6.3.16 .1.2.1	RO	Shows the table entry for defining the access control policy to the operators group.
6	vacmGroupN ame	.1.3.6.1.6.3.16 .1.2.1.2.3	RO	Shows the group name to which this entry belongs.
7	vacmSecurit yToGroupSt orageType	.1.3.6.1.6.3.16 .1.2.1.2.4	RO	Shows the method for storing this table entry, which is fixed at active(4).
8	vacmSecurit yToGroupSt atus	.1.3.6.1.6.3.16 .1.2.1.2.5	NA	Shows the method for storing this table entry, which is fixed at active (1).
9	vacmAccess Table	.1.3.6.1.6.3.16 .1.4.1	NA	Shows the table of access rights that the group has.
10	vacmAccess Entry	.1.3.6.1.6.3.16 .1.4.1.1	NA	Shows the table entry of access rights that the group has.
11	vacmAccess ContextMatc h	.1.3.6.1.6.3.16 .1.4.1.1.4	RO (*1)	Shows the method for matching contextName to vacmAccessContextPrefix. The value is fixed at exact (1).
12	vacmAccess ReadViewNa me	.1.3.6.1.6.3.16 .1.4.1.1.5	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for read access authorized by this entry.
13	vacmAccess WriteViewNa me	.1.3.6.1.6.3.16 .1.4.1.1.6	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for write access authorized by this entry.
14	vacmAccess NotifyViewN ame	.1.3.6.1.6.3.16 .1.4.1.1.7	RO (*1)	Shows vacmViewTreeFamilyViewName of MIB view for notification read access authorized by this entry.
15	vacmAccess StorageType	.1.3.6.1.6.3.16 .1.4.1.1.8	RO (*1)	Shows the method for storing this entry. The value is fixed at permanent (4).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object is RC (Read Create) in the SNMP standard, but RO for this equipment.

(c) snmpVacmMIB group (2/2)

No	Object identifier	OID	Syntax	Description
16	vacmAccess Status	.1.3.6.1.6.3.16 .1.4.1.1.9	RO (*1)	Shows the method for storing the user entry. The value is fixed at active(1).
17	vacmViewSp inLock	.1.3.6.1.6.3.16 .1.1.1	RO (*1)	Shows advisory lock, which allows cooperative SNMP command generator application to cooperate, for SET operation to create or change views. The value is fixed at 0 (zero).
18	vacmViewTr eeFamilyTab le	.1.3.6.1.6.3.16 .1.1.2	NA	Shows the local storage table for information on the sub-tree family of MIB view.
19	vacmViewTr eeFamilyEntr y	.1.3.6.1.6.3.16 .1.1.2.1	NA	Shows the local storage table entry for information on the sub-tree family of MIB view.
20	vacmViewTr eeFamilyMa sk	.1.3.6.1.6.3.16 .1.1.2.3	RO	Shows the mask value of vacmViewTreeFamilySubtree. The value is fixed at ‘ ‘ H.
21	vacmViewTr eeFamilyTyp e	.1.3.6.1.6.3.16 .1.1.2.4	RO (*1)	Shows that MIB view is included or excluded. One of the following values is displayed. 1: included 2: excluded
22	vacmViewTr eeFamilyStor ageType	.1.3.6.1.6.3.16 .1.1.2.5	RO (*1)	Shows the method for storing this entry. The value is fixed at permanent (4).
23	vacmViewTr eeFamilyStat us	.1.3.6.1.6.3.16 .1.1.2.6	RO (*2)	Shows the status of this entry. The value is fixed at active (1).

(*1) This object is RW in the SNMP standard, but RO for this equipment.

(*2) This object is RC (Read Create) in the SNMP standard, but RO for this equipment.

(5) Supported private MIB objects

1 ioChassis

ioChassis consists of the following two groups: ioChassisStatic and ioChassisDynamic. Each group is described in the following table (a) to (b).

(a) ioChassisStatic group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	ioChassisStatic	.1.3.6.1.4.1.116.5.39.11.1	Not-Accessible	NA	Shows the static information on the I/O slot expansion unit chassis.
2	ioChassisStaticCountPsm	.1.3.6.1.4.1.116.5.39.11.1.1	Integer32	RO	Shows the maximum number of slots for installing power supply modules.
3	ioChassisStaticCountFan	.1.3.6.1.4.1.116.5.39.11.1.2	Integer32	RO	Shows the maximum number of slots for installing fan modules.
4	ioChassisStaticCountPcieSlot	.1.3.6.1.4.1.116.5.39.11.1.3	Integer32	RO	Shows the maximum number of slots for installing PCI express cards.
5	ioChassisStaticCountUpPort	.1.3.6.1.4.1.116.5.39.11.1.4	Integer32	RO	Shows the maximum number of ports for connecting to server chassis.
6	ioChassisStaticInfoInfoModel	.1.3.6.1.4.1.116.5.39.11.1.5	DisplayString	RO	Shows the model name of the I/O slot expansion unit chassis.
7	ioChassisStaticInfoChassisType	.1.3.6.1.4.1.116.5.39.11.1.6	DisplayString	RO	Shows the backplane type of the I/O slot expansion unit chassis.
8	ioChassisStaticInfo ChassisId	.1.3.6.1.4.1.116.5.39.11.1.7	DisplayString	RO	Shows the chassis ID of the I/O slot expansion unit.
9	ioChassisStaticInfoSerialNo	.1.3.6.1.4.1.116.5.39.11.1.8	DisplayString	RO	Shows the serial number of the I/O slot expansion unit chassis.
10	ioChassisStaticMaxCurrent	.1.3.6.1.4.1.116.5.39.11.1.9	Integer32	RO	Shows the value of current consumed in the largest configuration of the I/O slot expansion unit chassis. Unit: 0.1A
11	ioChassisStaticMaxPower	.1.3.6.1.4.1.116.5.39.11.1.10	Integer32	RO	Shows the value of power consumed in the largest configuration of the I/O slot expansion unit chassis. Unit: 0.1kW
12	ioChassisStaticCurrentCurrent	.1.3.6.1.4.1.116.5.39.11.1.11	Integer32	RO	Shows the maximum current value consumed in the current configuration of the I/O slot expansion unit chassis. Unit: 0.1A

(a) ioChassisStatic group (2/2)

No	Object identifier	OID	Syntax	Access	Description
13	ioChassisStaticCurrentPower	.1.3.6.1.4.1.116.5.39.11.1.12	Integer32	RO	Shows the value of rated power in the current configuration of the I/O slot expansion unit chassis. Unit: 0.1kW
14	ioChassisStaticVoltage	.1.3.6.1.4.1.116.5.39.11.1.13	Integer32	RO	Shows the value of standard voltage for the I/O slot expansion unit chassis. Unit: 0.1V
15	ioChassisStaticCurrentType	.1.3.6.1.4.1.116.5 .39.11.1.14	INTEGER	RO	Shows the inlet current type of the I/O slot expansion unit chassis. One of the following values is displayed. 1: AC 2.: DC 3: unknown
16	ioChassisStaticTempHigher	.1.3.6.1.4.1.116.5.39.11.1.15	Integer32	RO	Shows the high-temperature warning threshold of inlet air for the I/O slot expansion unit chassis. Unit: 0.1°C
17	ioChassisStaticTempLower	.1.3.6.1.4.1.116.5.39.11.1.16	Integer32	RO	Shows the low-temperature warning threshold of inlet air for the I/O slot expansion unit chassis. Unit: 0.1°C
18	ioChassisStaticHeight	.1.3.6.1.4.1.116.5.39.11.1.17	Integer32	RO	Shows the height of the I/O slot expansion unit chassis. Unit: 1U
19	ioChassisStaticSize	.1.3.6.1.4.1.116.5.39.11.1.18	Integer32	RO	Shows the size of the I/O slot expansion unit chassis. Unit: 1U
20	ioChassisStaticTotalMass	.1.3.6.1.4.1.116.5.39.11.1.19	Integer32	RO	Shows the total weight of the I/O slot expansion unit chassis in the current configuration. Unit: 0.1kg
21	ioChassisStaticUnitNum	.1.3.6.1.4.1.116.5.39.11.1.20	Integer32	RO	Shows the unit numbert of the I/O slot expansion unit chassis.
22	ioChassisStaticFMver1	.1.3.6.1.4.1.116.5.39.11.1.21	DisplayString	RO	Shows the firmware version of the I/O module #0 in the I/O slot expansion unit chassis.
23	ioChassisStaticFMver2	.1.3.6.1.4.1.116.5.39.11.1.22	DisplayString	RO	Shows the firmware version of the I/O module #1 in the I/O slot expansion unit chassis.
24	ioChassisStaticCapacityMarlog	.1.3.6.1.4.1.116.5.39.11.1.23	Integer32	RO	Shows the maximum number of index for MAR (Maintenance Action Report) logs.

(b) ioChassisDynamic group (1/3)

No	Object identifier	OID	Syntax	Access	Description
1	ioChassisDynamic	.1.3.6.1.4.1.116.5.39.11.2	Not-Accessible	NA	Shows the dynamic information on the I/O slot expansion unit chassis.
2	ioChassisDynamicCurrent	.1.3.6.1.4.1.116.5.39.11.2.1	Integer32	RO	Shows the value of current consumption of the I/O slot expansion unit chassis. Unit: 0.1A
3	ioChassisDynamicPower	.1.3.6.1.4.1.116.5.39.11.2.2	Integer32	RO	Shows the value of power consumption of the I/O slot expansion unit chassis. Unit: 0.1kW
4	ioChassisDynamicFanAirVolume	.1.3.6.1.4.1.116.5.39.11.2.3	Integer32	RO	Shows the quantity of air supplied by the I/O slot expansion unit chassis. Unit: 0.1m^3/min
5	ioChassisDynamicStatusLocationLed1	.1.3.6.1.4.1.116.5.39.11.2.4	INTEGER	RO	Shows a state of Location LED #0 on the I/O slot expansion chassis. One of the following values. 1: off 2: on
6	ioChassisDynamicStatusLocationLed2	.1.3.6.1.4.1.116.5.39.11.2.5	INTEGER	RO	Shows a state of Location LED #1 on the I/O slot expansion chassis. One of the following values. 1: off 2: on
7	ioChassisDynamicPowerStatus	.1.3.6.1.4.1.116.5.39.11.2.6	INTEGER	RO	Shows a state of power supply to the I/O slot expansion chassis. One of the following values. 1: off 2: on
8	ioChassisDynamicStatusAlmLed	.1.3.6.1.4.1.116.5.39.11.2.7	INTEGER	RO	Shows a state of ALM LED on the I/O slot expansion chassis front panel. One of the following values. 1: off 2: solid orange 3: solid red
9	ioChassisDynamicTempAmbientValue1	.1.3.6.1.4.1.116.5.39.11.2.8	Integer32	RO	Shows the temperature of inlet air to the I/O module #0 in the I/O slot expansion unit chassis. Unit: 0.1°C
10	ioChassisDynamicTempAmbientValid1	.1.3.6.1.4.1.116.5.39.11.2.9	INTEGER	RO	Shows the temperature validity of inlet air to the I/O module #0 in the I/O slot expansion unit chassis. One of the following values is displayed. 1: invalid 2: valid

(b) ioChassisDynamic group (2/3)

No	Object identifier	OID	Syntax	Access	Description
11	ioChassisDynamicTempAmbientValue2	.1.3.6.1.4.1.116.5.39.11.2.10	Integer32	RO	Shows the temperature validity of inlet air to the I/O module #1 in the I/O slot expansion unit chassis.
12	ioChassisDynamicTempAmbientValid2	.1.3.6.1.4.1.116.5.39.11.2.11	INTEGER	RO	Shows the temperature validity of inlet air to the I/O module #1 in the I/O slot expansion unit chassis. One of the following values is displayed. 1: invalid 2: valid
13	ioChassisDynamicTempExhaustValue1	.1.3.6.1.4.1.116.5.39.11.2.12	Integer32	RO	Shows the temperature of outlet air from the I/O module #0 in the I/O slot expansion unit chassis.. Unit: 0.1°C
14	ioChassisDynamicTempExhaustValid1	.1.3.6.1.4.1.116.5.39.11.2.13	INTEGER	RO	Shows the temperature validity of outlet air from the I/O module #0 in the I/O slot expansion unit chassis. One of the following values is displayed. 1: invalid 2: valid
15	ioChassisDynamicTempExhaustValue2	.1.3.6.1.4.1.116.5.39.11.2.14	Integer32	RO	Shows the temperature of outlet air from the I/O module #1 in the I/O slot expansion unit chassis.. Unit: 0.1°C
16	ioChassisDynamicTempExhaustValid2	.1.3.6.1.4.1.116.5.39.11.2.15	INTEGER	RO	Shows the temperature validity of outlet air from the I/O module #1 in the I/O slot expansion unit chassis. One of the following values is displayed. 1: invalid 2: valid
17	ioChassisDynamicMarlogLatestInfo	.1.3.6.1.4.1.116.5.39.11.2.16	DisplayString	RO	Shows the information of the latest MAR (Maintenance Action Report) log.
18	ioChassisDynamicMarlogInfoTable	.1.3.6.1.4.1.116.5.39.11.2.17	Not-Accessible	NA	Shows the table of information on MAR (Maintenance Action Report) logs.
19	ioChassisDynamicMarlogInfoEntry	.1.3.6.1.4.1.116.5.39.11.2.17.1	Not-Accessible	NA	Shows the table entry describing the information on MAR (Maintenance Action Report) logs.
20	ioChassisDynamicMarlogInfoIndex	.1.3.6.1.4.1.116.5.39.11.2.17.1.1	Integer32	RO	Shows the index value ranging from 1 to chassisCapacityMarlog to identify the table entry.

(b) ioChassisDynamic group (3/3)

No	Object identifier	OID	Syntax	Access	Description
21	ioChassisDynamicMarlogInfoData	.1.3.6.1.4.1.116.5.39.11.2.17.1.2	DisplayString	RO	Shows the MAR (Maintenance Action Report) log information data corresponding to the index value shown in #20.

2 ioPsm

ioPsm consists of the following two groups: ioPsmStatic and ioPsmDynamic. Each group is described in the following table (a) to (b).

(a) ioPsmStatic group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	ioPsmStatic	.1.3.6.1.4.1.116.5.39.12.1	Not-Accessible	NA	Shows the static information on the power supply module.
2	ioPsmStaticSlotCapacity	.1.3.6.1.4.1.116.5.39.12.1.1	Integer32	RO	Shows the maximum number of slots for installing power supply modules.
3	ioPsmStaticTable	.1.3.6.1.4.1.116.5.39.12.1.2	Not-Accessible	NA	Shows the table of the static information on the power supply module.
4	ioPsmStaticEntry	.1.3.6.1.4.1.116.5.39.12.1.2.1	Integer32	RO	Shows the table entry of the static information on the power supply module.
5	ioPsmStaticIndex	.1.3.6.1.4.1.116.5.39.12.1.2.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioPsmStaticSlotCapacity
6	ioPsmStaticInstallExist	.1.3.6.1.4.1.116.5.39.12.1.2.1.2	INTEGER	RO	Shows a state of power supply modules. One of the following values is displayed. 1: nonexistent 2: existent 3: unknown
7	ioPsmStaticCurrentType	.1.3.6.1.4.1.116.5.39.12.1.2.1.3	INTEGER	RO	Shows the inlet current type of the power supply module. One of the following values is displayed. 1: AC 2: DC 3: unknown

(a) ioPsmStatic group (2/2)

No	Object identifier	OID	Syntax	Access	Description
8	ioPsmStaticVoltType	.1.3.6.1.4.1.116.5.39.12.1.2.1.4	INTEGER	RO	Shows the inlet voltage type of the power supply module. One of the following values is displayed. 1: 100 2. 200 3: unknown
9	ioPsmStaticProductSerialNo	.1.3.6.1.4.1.116.5.39.12.1.2.1.5	DisplayString	RO	Shows ProductSerialNo of the power supply module.
10	ioPsmStaticSlotnum	.1.3.6.1.4.1.116.5.39.12.1.2.1.6	Integer32	RO	Shows a slot number of the power supply module corresponding to the index value. Value: 0 to ioPsmStaticSlotCapacity-1.

(b) ioPsmDynamic group

No	Object identifier	OID	Syntax	Access	Description
1	ioPsmDynamic	.1.3.6.1.4.1.116.5.39.12.2	Not-Accessible	NA	Shows the dynamic information on the power supply module.
2	ioPsmDynamicTable	.1.3.6.1.4.1.116.5.39.12.2.1	Not-Accessible	NA	Shows the table of the dynamic information on the power supply module.
3	ioPsmDynamicEntry	.1.3.6.1.4.1.116.5.39.12.2.1.1	Not-Accessible	NA	Shows the table entry of the dynamic information on the power supply module.
4	ioPsmDynamicIndex	.1.3.6.1.4.1.116.5.39.12.2.1.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioPsmStaticSlotCapacity.
5	ioPsmDynamicPowerStatus	.1.3.6.1.4.1.116.5.39.12.2.1.1.2	INTEGER	RO	Shows a power state of the power supply module. One of the following values is displayed. 1: power off 2: power on 3: unknown
6	ioPsmDynamicHealthStatus	.1.3.6.1.4.1.116.5.39.12.2.1.1.3	INTEGER	RO	Shows a state of the power supply module. One of the following values is displayed. 1: normal 2: fault 3: unknown

3 ioFan

ioFan consists of the following two groups: ioFanStatic and ioFanDynamic. Each group is described in the following table (a) to (b).

(a) ioFanStatic group

No	Object identifier	OID	Syntax	Access	Description
1	ioFanStatic	.1.3.6.1.4.1.116.5.39.13.1	Not-Accessible	NA	Shows the static information on the fan module.
2	ioFanStaticSlotCapacity	.1.3.6.1.4.1.116.5.39.13.1.1	Integer32	RO	Shows the maximum number of slots for fan modules.
3	ioFanStaticTable	.1.3.6.1.4.1.116.5.39.13.1.2	Not-Accessible	NA	Shows the table of the static information on the fan module.
4	ioFanStaticEntry	.1.3.6.1.4.1.116.5.39.13.1.2.1	Not-Accessible	NA	Shows the table entry of the static information on the fan module.
5	ioFanStaticIndex	.1.3.6.1.4.1.116.5.39.13.1.2.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioFanStaticSlotCapacity.
6	ioFanStaticInstallExist	.1.3.6.1.4.1.116.5.39.13.1.2.1.2	INTEGER	RO	Shows a state of fan modules. One of the following values is displayed. 1: nonexistent 2: existent 3: unknown
7	ioFanStaticType	.1.3.6.1.4.1.116.5.39.13.1.2.1.3	INTEGER	RO	Shows a type of the fan module. The following value is displayed. 1: standard
8	ioFanStaticMaxRpm	.1.3.6.1.4.1.116.5.39.13.1.2.1.4	Integer32	RO	Shows the maximum number of the fan module rotations.
9	ioFanStaticMaxAirVolume	.1.3.6.1.4.1.116.5.39.13.1.2.1.5	Integer32	RO	Shows the maximum quantity of air supplied by the fan module. Unit: 0.1m^3/min
10	ioFanStaticGroup	.1.3.6.1.4.1.116.5.39.13.1.2.1.6	INTEGER	RO	Shows a group to which the fan module belongs. One of the following values is displayed. 1: group 0 2: group 1
11	ioFanStaticSlotnum	.1.3.6.1.4.1.116.5.39.13.1.2.1.7	Integer32	RO	Shows a slot number of the fan module corresponding to the index value. Value: 0 to ioFanStaticSlotCapacity-1.

(b) ioFanDyanmic group

No	Object identifier	OID	Syntax	Access	Description
1	ioFanDynamic	.1.3.6.1.4.1.116.5.39.13.2	Not-Accessible	NA	Shows the dynamic information on the fan module.
2	ioFanDynamicTable	.1.3.6.1.4.1.116.5.39.13.2.1	Not-Accessible	NA	Shows the table of the dynamic information on the fan module.
3	ioFanDynamicEntry	.1.3.6.1.4.1.116.5.39.13.2.1.1	Not-Accessible	NA	Shows the table entry of the dynamic information on the fan module.
4	ioFanDynamicIndex	.1.3.6.1.4.1.116.5.39.13.2.1.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioFanStaticSlotCapacity.
5	ioFanDynamicPowerStatus	.1.3.6.1.4.1.116.5.39.13.2.1.1.2	INTEGER	RO	Shows a power state of the fan module. One of the following values is displayed. 1: power off 2: power on 3: unknown
6	ioFanDynamicHealthStatus	.1.3.6.1.4.1.116.5.39.13.2.1.1.3	INTEGER	RO	Shows a state of the fan module. One of the following values is displayed. 1: normal 2: fault 3: unknown
7	ioFanDynamicSensorCapacity	.1.3.6.1.4.1.116.5.39.13.2.1.1.4	INTEGER	RO	Shows the number of fans per fan module.
8	ioFanDynamicValue1	.1.3.6.1.4.1.116.5.39.13.2.1.1.5	Integer32	RO	Shows the number of the fan #0 rotations.
9	ioFanDynamicValid1	.1.3.6.1.4.1.116.5.39.13.2.1.1.6	INTEGER	RO	Shows the rotation validity of the fan module #0. One of the following values is displayed. 1: invalid 2: valid
10	ioFanDynamicValue2	.1.3.6.1.4.1.116.5.39.13.2.1.1.7	Integer32	RO	Shows the number of the fan #1 rotations.
11	ioFanDynamicValid2	.1.3.6.1.4.1.116.5.39.13.2.1.1.8	INTEGER	RO	Shows the rotation validity of the fan module #1. One of the following values is displayed. 1: invalid 2: valid

4 ioPcie

ioPci consists of the following two groups: ioPciStatic and ioPciDynamic. Each group is described in the following table (a) to (b).

(a) ioPcieStatic group

No	Object identifier	OID	Syntax	Access	Description
1	ioPcieStatic	.1.3.6.1.4.1.116.5.39.14.1	Not-Accessible	NA	Shows the static information on the PCI express slot.
2	ioPcieStaticSlotCapacity	.1.3.6.1.4.1.116.5.39.14.1.1	Integer32	RO	Shows the maximum number of slots for PCI express slots.
3	ioPcieStaticTable	.1.3.6.1.4.1.116.5.39.14.1.2	Not-Accessible	NA	Shows the table of the static information on the PCI express slot.
4	ioPcieStaticEntry	.1.3.6.1.4.1.116.5.39.14.1.2.1	Not-Accessible	NA	Shows the table entry of the static information on the PCI express slot
5	ioPcieStaticIndex	.1.3.6.1.4.1.116.5.39.14.1.2.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioPciStaticSlotCapacity.
6	ioPcieStaticType	.1.3.6.1.4.1.116.5.39.14.1.2.1.2	INTEGER	RO	Shows a type of the card installed in the PCI express slot. One of the following values is displayed. 1: Gigabit Ethernet 2: Fibre-channel 4: Serial Attached SCSI 7: unknown
7	ioPcieStaticGroup	.1.3.6.1.4.1.116.5.39.14.1.2.1.3	INTEGER	RO	Shows a group to which the PCI express slot belongs. One of the following values is displayed. 1: group 0 2: group 1
8	ioPcieStaticSlotnum	.1.3.6.1.4.1.116.5.39.14.1.2.1.4	Integer32	RO	Shows a slot number of the PCI express slot corresponding to the index value. Value: 0 to ioFanStaticSlotCapacity-1.

(b) ioPcieDynamic group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	ioPcieDynamic	.1.3.6.1.4.1.116.5.39.14.2	Not-Accessible	NA	Shows the dynamic information on the PCI express slot.
2	ioPcieDynamicTable	.1.3.6.1.4.1.116.5.39.14.2.1	Not-Accessible	NA	Shows the table of the dynamic information on the PCI express slot.
3	ioPcieDynamicEntry	.1.3.6.1.4.1.116.5.39.14.2.1.1	Not-Accessible	NA	Shows the table entry of the dynamic information on the PCI express slot
4	ioPcieDynamicIndex	.1.3.6.1.4.1.116.5.39.14.2.1.1.1	INTEGER	RO	Shows the index value to identify the table entry. Value: 1 to ioPcieStaticSlotCapacity.
5	ioPcieDynamicInstallExist	.1.3.6.1.4.1.116.5.39.14.2.1.1.2	INTEGER	RO	Shows a state of PCI express slots. One of the following values is displayed. 1: nonexistent 2: existent 3: unknown
6	ioPcieDynamicPowerStatus	.1.3.6.1.4.1.116.5.39.14.2.1.1.3	Integer32	RO	Shows a power state of the PCI express slot. One of the following values is displayed. 1: power off 2: power on 3: unknown
7	ioPcieDynamicReceiverError	.1.3.6.1.4.1.116.5.39.14.2.1.1.4	Integer32	RO	Shows the number of ReceiverError counts of the PCI express slot.
8	ioPcieDynamicFcUpdateTimeoutError	.1.3.6.1.4.1.116.5.39.14.2.1.1.5	Integer32	RO	Shows the number of FcUpdateTimeoutError counts of the PCI express slot.
9	ioPcieDynamicECRCError	.1.3.6.1.4.1.116.5.39.14.2.1.1.6	Integer32	RO	Shows the number of ECRCError counts of the PCI express slot.
10	ioPcieDynamicPoisonedTLPError	.1.3.6.1.4.1.116.5.39.14.2.1.1.7	Integer32	RO	Shows the number of PoisonedTLPError counts of the PCI express slot.
11	ioPcieDynamicBadTLPError	.1.3.6.1.4.1.116.5.39.14.2.1.1.8	Integer32	RO	Shows the number of BadTLPError counts of the PCI express slot.
12	ioPcieDynamicBadDLLPError	.1.3.6.1.4.1.116.5.39.14.2.1.1.9	Integer32	RO	Shows the number of BadDLLPError counts of the PCI express slot.
13	ioPcieDynamicReplayNumRolloverError	.1.3.6.1.4.1.116.5.39.14.2.1.1.10	Integer32	RO	Shows the number of ReplayNumRolloverError counts of the PCI express slot.

(b) ioPcieDynamic group (2/2)

No	Object identifier	OID	Syntax	Access	Description
14	ioPcieDynamicReplayTimerTimeoutError	.1.3.6.1.4.1.116.5.39.14.2.1.1.11	Integer32	RO	Shows the number of ReplayTimerTimeoutError counts of the PCI express slot.
15	ioPcieDynamicRxNackDllp	.1.3.6.1.4.1.116.5.39.14.2.1.1.12	Integer32	RO	Shows the number of RxNackDllp counts of the PCI express slot.
16	ioPcieDynamicRxNgDeframingPatternEvent	.1.3.6.1.4.1.116.5.39.14.2.1.1.13	Integer32	RO	Shows the number of RxNgDeframingPatternEvent counts of the PCI express slot.
17	ioPcieDynamicRxNgDeframingPatternBufferOverflow	.1.3.6.1.4.1.116.5.39.14.2.1.1.14	Integer32	RO	Shows the number of RxNgDeframingPatternBufferOverflow counts of the PCI express slot.

5 ioUpPort

ioUpPort consists of the following two groups: ioUpPortStatic and ioUpPortDynamic. Each group is described in the following table (a) to (b).

(a) ioUpPortStatic group (1/3)

No	Object identifier	OID	Syntax	Access	Description
1	ioUpPortStatic	.1.3.6.1.4.1.116.5.39.15.1	Not-Accessible	NA	Shows the static information on the server chassis connect port.
2	ioUpPortStaticPortCapacity	.1.3.6.1.4.1.116.5.39.15.1.1	Integer32	RO	Shows the maximum number of server chassis connect ports.
3	ioUpPortStaticPortModeStatus1	.1.3.6.1.4.1.116.5.39.15.1.2	Integer32	RO	Shows an operating mode of server chassis connect ports of the I/O module #0. One of the following values is displayed. 1: 1:4 mode 2: 1:8 mode
4	ioUpPortStaticPortModeStatus2	.1.3.6.1.4.1.116.5.39.15.1.3	Integer32	RO	Shows an operating mode of server chassis connect ports of the I/O module #1. One of the following values is displayed. 1: 1:4 mode 2: 1:8 mode
5	ioUpPortStaticTable	.1.3.6.1.4.1.116.5.39.15.1.4	Not-Accessible	NA	Shows the table of the static information on the server chassis connect port.

(a) ioUpPortStatic group (2/3)

No	Object identifier	OID	Syntax	Access	Description
6	ioUpPortStaticEntry	.1.3.6.1.4.1.116.5.39.15.1.4.1	Not-Accessible	NA	Shows the table entry of the static information on the server chassis connect port.
7	ioUpPortStaticIndex	.1.3.6.1.4.1.116.5.39.15.1.4.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioUpPortStaticPortCapacity.
8	ioUpPortStaticGroup	.1.3.6.1.4.1.116.5.39.15.1.4.1.2	INTEGER	NA	Shows a group to which the server chassis connect port belongs. One of the following values is displayed. 1: group0 2: group 1
9	ioUpPortStaticBelongIod	.1.3.6.1.4.1.116.5.39.15.1.4.1.3	INTEGER	RO	Shows a number of the I/O slot expansion unit to which the server chassis connect port belongs.
10	ioUpPortStaticType	.1.3.6.1.4.1.116.5.39.15.1.4.1.4	INTEGER	RO	Shows a type of the server chassis connect port. One of the following values is displayed. 1: I/O slot expansion unit connect cable 2: sideband cable
11	ioUpPortStaticInstallExist	.1.3.6.1.4.1.116.5.39.15.1.4.1.5	INTEGER	RO	Shows the connection status of a cable connected to the server chassis connect port. One of the following values is displayed. 1: not connected 2: connected
12	ioUpPortStaticSlotnum	.1.3.6.1.4.1.116.5.39.15.1.4.1.6	Integer32	RO	Shows the number of the server chassis connect port corresponding to the index value. Value: 1 to ioUpPortStaticPortCapacity-1.
13	ioUpPortStaticBelon1Slotnum1	.1.3.6.1.4.1.116.5.39.15.1.4.1.7	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
14	ioUpPortStaticBelongSlotnum2	.1.3.6.1.4.1.116.5.39.15.1.4.1.8	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
15	ioUpPortStaticBelongSlotnum3	.1.3.6.1.4.1.116.5.39.15.1.4.1.9	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.

(a) ioUpPortStatic group (3/3)

No	Object identifier	OID	Syntax	Access	Description
16	ioUpPortStaticBelongSlotnum4	.1.3.6.1.4.1.116.5.39.15.1.4.1.10	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
17	ioUpPortStaticBelongSlotnum5	.1.3.6.1.4.1.116.5.39.15.1.4.1.11	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
18	ioUpPortStaticBelongSlotnum6	.1.3.6.1.4.1.116.5.39.15.1.4.1.12	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
19	ioUpPortStaticBelongSlotnum7	.1.3.6.1.4.1.116.5.39.15.1.4.1.13	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.
20	ioUpPortStaticBelongSlotnum8	.1.3.6.1.4.1.116.5.39.15.1.4.1.14	Integer32	RO	Shows the number of the PCI express slot belonging to the server chassis connect port.

(b) ioUpPortDynamic group (1/2)

No	Object identifier	OID	Syntax	Access	Description
1	ioUpPortDynamic	.1.3.6.1.4.1.116.5.39.15.2	Not-Accessible	NA	Shows the dynamic information on the server chassis connect port.
2	ioUpPortDynamicTable	.1.3.6.1.4.1.116.5.39.15.2.1	Not-Accessible	NA	Shows the table of the dynamic information on the server chassis connect port.
3	ioUpPortDynamicEntry	.1.3.6.1.4.1.116.5.39.15.2.1.1	Not-Accessible	NA	Shows the table entry of the dynamic information on the server chassis connect port.
4	ioUpPortDynamicIndex	.1.3.6.1.4.1.116.5.39.15.2.1.1.1	Integer32	RO	Shows the index value to identify the table entry. Value: 1 to ioStaticPortCapacity.
5	ioUpPortDynamicLink	.1.3.6.1.4.1.116.5.39.15.2.1.1.2	INTEGER	RO	Shows a link state of the server chassis connect port. One of the following values is displayed. 1: up 2: down 3: unknown
6	ioUpPortDynamicReceiverError	.1.3.6.1.4.1.116.5.39.15.2.1.1.3	Integer32	RO	Shows the number of ReceiverError counts of the server chassis connect port.

(b) ioUpPortDynamic group (2/2)

No	Object identifier	OID	Syntax	Access	Description
7	ioUpPortDynamicFcUpdateTimeoutError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.4	Integer32	RO	Shows the number of FcUpdateTimeoutError counts of the server chassis connect port.
8	ioUpPortDynamicECRCError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.5	Integer32	RO	Shows the number of ECRCError counts of the server chassis connect port.
9	ioUpPortDynamicPoisonedTLPError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.6	Integer32	RO	Shows the number of PoisonedTLPError counts of the server chassis connect port.
10	ioUpPortDynamicBadTLPError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.7	Integer32	RO	Shows the number of BadTLPError counts of the server chassis connect port.
11	ioUpPortDynamicBadDLLPError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.8	Integer32	RO	Shows the number of BadDLLPError counts of the server chassis connect port.
12	ioUpPortDynamicReplayNumRolloverError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.9	Integer32	RO	Shows the number of ReplayNumRolloverError counts of the server chassis connect port.
13	ioUpPortDynamicReplayTimerTimeoutError	.1.3.6.1.4.1.1166.5.39.15.2.1.1.10	Integer32	RO	Shows the number of ReplayTimerTimeoutError counts of the server chassis connect port.
14	ioUpPortDynamicRxNackDllp	.1.3.6.1.4.1.1166.5.39.15.2.1.1.11	Integer32	RO	Shows the number of RxNackDllp counts of the server chassis connect port.
15	ioUpPortDynamicRxNgDeframingPatternEvent	.1.3.6.1.4.1.1166.5.39.15.2.1.1.12	Integer32	RO	Shows the number of RxNgDeframingPatternEvent counts of the server chassis connect port.
16	ioUpPortDynamicRxNgDeframingPatternBufferOverflow	.1.3.6.1.4.1.1166.5.39.15.2.1.1.13	Integer32	RO	Shows the number of RxNgDeframingPatternBufferOverflow counts of the server chassis connect port.

LDAP server linkage

Overview of the LDAP server linkage

Compute Blade 2000 management modules and server blades search the LDAP directory on the LDAP server by using the Lightweight Directory Access Protocol (LDAP) to authenticate users. With this function, you can perform the following:

(1) Login to management modules and the server blades as a user registered with the LDAP directory

(2) Group authentication that allows only the account belonging to a specific group in the LDAP directory to log in

❑ Logging in as a user registered with the LDAP directory

Management modules and server blades judge whether to allow a user to log in based on the user account information registered with each module and the user account information in the LDAP directory at user authentication.

Adding user account information to the LDAP directory on the LDAP server allows all management modules and server blades using the LDAP server to use the added user account information. Besides, it is not necessary to register user account information with each module.

❑ Group authentication

During user authentication, the group information in the LDAP directory is viewed and only the user accounts belonging to the group are allowed to log in. By using the group authentication function, you can construct an LDAP server linkage environment between management modules and server blades without drastically changing the already constructed LDAP directory.



To use this function in a management module, the firmware must be version A0151 or later.

To use this function in a server blade (model E55A1), the BMC firmware must be version 03-60 or later.

To use this function for logging in to a remote console application, the remote console application must be version 04-02 or later.

Supported LDAP server

Compute Blade 2000 supports Active Directory, attached to the following Windows Server, as the LDAP server with linkage.

Supported Directory Server

Item	Name
OS	Microsoft® Windows® Server 2008 R2, Standard Microsoft® Windows® Server 2008 R2, Enterprise Microsoft® Windows® Server 2008, Standard Microsoft® Windows® Server 20082, Enterprise Microsoft® Windows® Server 2003 R2, Standard Edition Microsoft® Windows® Server 2003 R2, Standard Edition

Environmental setting for active directory

This section describes settings required when Active Directory is used as an LDAP server.

The following table shows the required setting items.

Active directory setting item

#	Setting item
1	Server certificate
2	Bind DN for the LDAP server
3	User account for logging in to management modules and to server blades
4	Group that is allowed to login to the management module and server blade

❑ Server certificate

Because all communications between Compute Blade 2000 and LDAP servers are carried out through Secure Socket Layer (SSL), the server certificate must be registered for Active Directory to be used as an LDAP server.

For details about how to register the server certificate, see the documentation of your Windows server.



There are two different server certificates. One is a self-signed certificate, and the other is a certificate certified by an external certificate authority. You can use either certificate for communication between Compute Blade 2000 and Active Directory.

❑ Bind DN for the LDAP server

To search an LDAP directory at user authentication, you must connect to an LDAP server. There are two methods for connecting to an LDAP server as below. Perform either of the following methods:

(1) Connect to an LDAP server by using an LDAP bind DN and the password.

(2) Connect to an LDAP server as an anonymous user.

Tip We recommend using an LDAP bind DN and a password.

Registering a user account to use as a bind DN

Register a user account to use as an LDAP bind DN with your Windows server. For details about how to register user accounts, see the documentation of your Windows server.

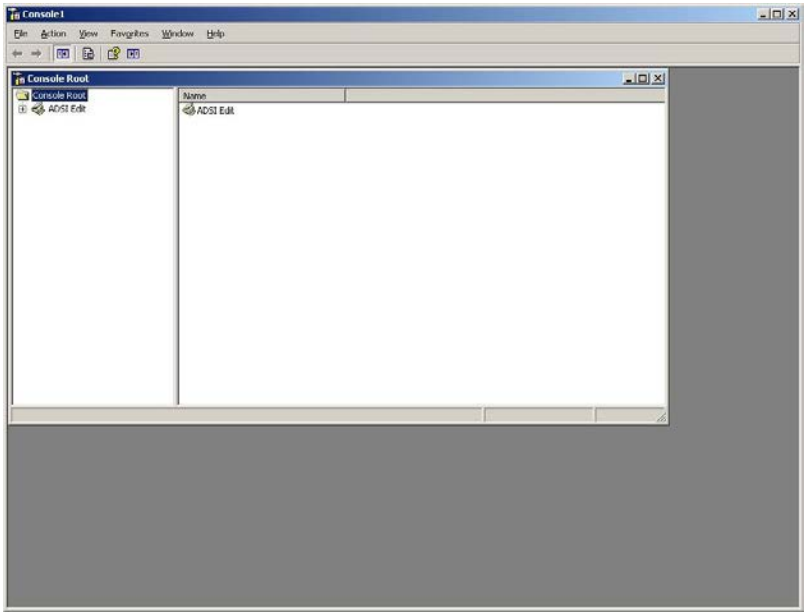
You must grant the access permission for the LDAP directory to use when authenticating users to the user account to be used as the LDAP bind DN.

Registering a user account as anonymous

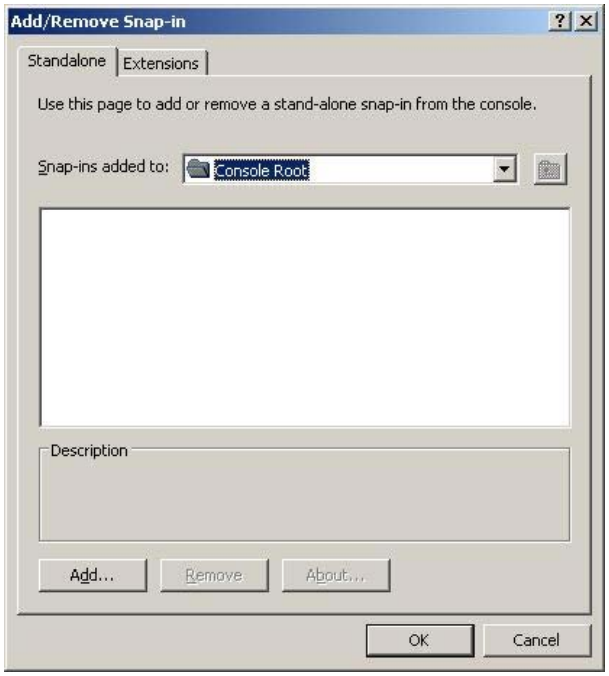
Follow the procedure below to register an anonymous user.

Tip When registering a user for LDAP connection, skip this procedure.

1 Select **Start > Run…**, type `mmc` and click **OK**.



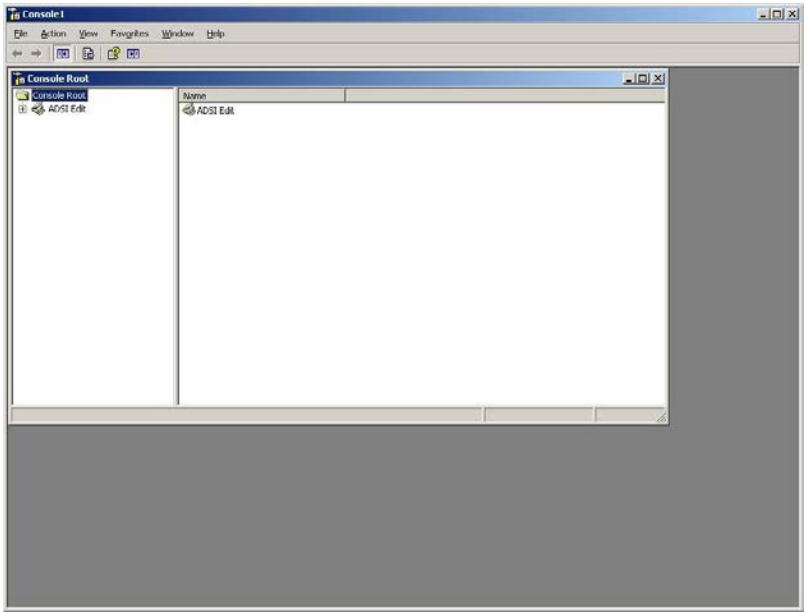
2 When the Microsoft Management Console (MMC) screen is displayed, select **Menu > File > Add/Remove Snap-in**. In the Add Standalone Snap-in screen, click the **Add…**, select `ADSI Edit` from **Available standalone snap-ins:**, click **Add**, and then click **Close**.





Tip When ADSI Edit is not available, see “Windows support tools”.

3 When “ADSI Edit” is added to the Add Standalone Snap-in screen, click **OK**. Confirm that **ADSI Edit** is added to Console Root in the MMC screen.



4 Click **ADSI Edit** in the **MMC** screen, and select **Connect to…**.

5 Select **Domain** for the domain context of Active Directory to connect, and click **OK**.



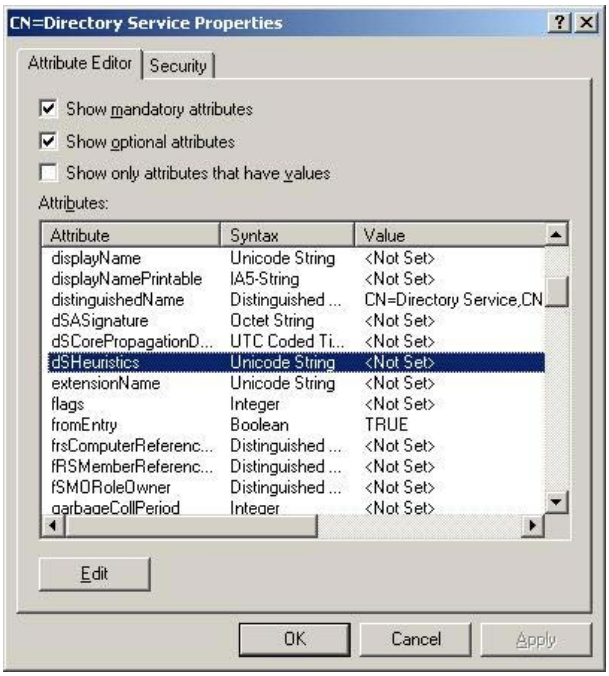
6 Right-click **ADSI Edit** again, and select **Connect to…**.

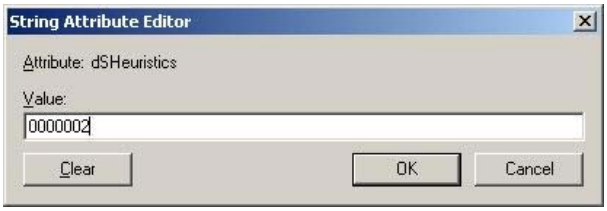
7 Select **Configuration** as Context, and click **OK**.



8 Place and right-click the mouse **on \ADSI Edit\configuration\CN=Configuration\DC=domain base\CN-Services\CN=Windows NT\CN=Directory Service,** and select **properties**.

9 Click **dSHeuristics** and then **Edit** to set a value in the **Properties** screen. When the value is **<Not Set>,** type `0000002` in the field. When a value is set, change the 7th number from the left to 2. Do not change other numbers.





10 When setting is completed, click **OK** in the properties screen to apply the setting.

The procedure above can allow you to register an anonymous user.

Then select **Management tools > Active Directory Users and Computers** to give access to an anonymous user.

❑ Registering the user account for logging in to the management module and the server blade

In **Management Tools > Active Directory Users and Computers**, register the user account for the LDAP directory. For details about how to register user accounts, see the documentation of your Windows server.

This section describes the limitations for user names and passwords to be registered and the procedure for granting role information to be used after logging in to management modules or BMC.

User name

The following characters and the number of characters are available for user names.

Number of characters	: From 1 to 32 characters
Available characters for the head of a name	: [A-Z] [a-z]
Available characters for from the second to the end of a name	[A-Z] [a-z] [0-9] , "-" (hyphen), "_" (underscore), "." (period)

Password

The following characters and the number of characters are available for passwords.

Number of characters	: From 1 to 32 characters
Available characters	: Printable characters in ASCII (0x20-0x7e)



The complexity of passwords depends on the security policy of your Windows server.

Granting role information

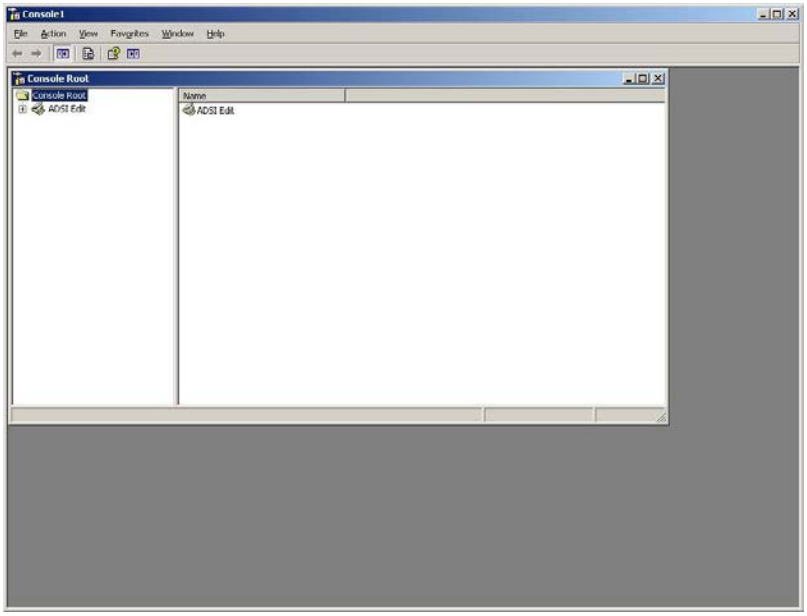
By granting role information to a user account registered with the LDAP directory, you can set the range of operations to be performed after the login.



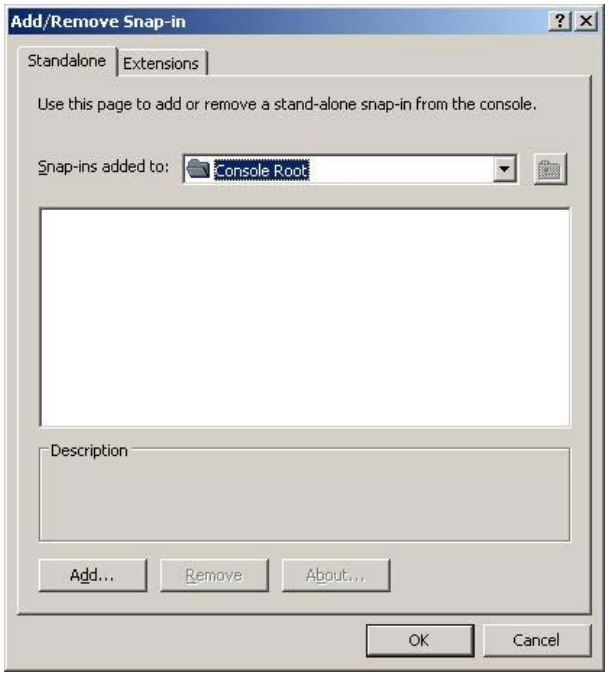
If you do not grant role information, operations you can perform after the login are minimized.

Follow the procedure below to assign role information.

1 Select **Start > Run…**, type `mmc` and click **OK**.



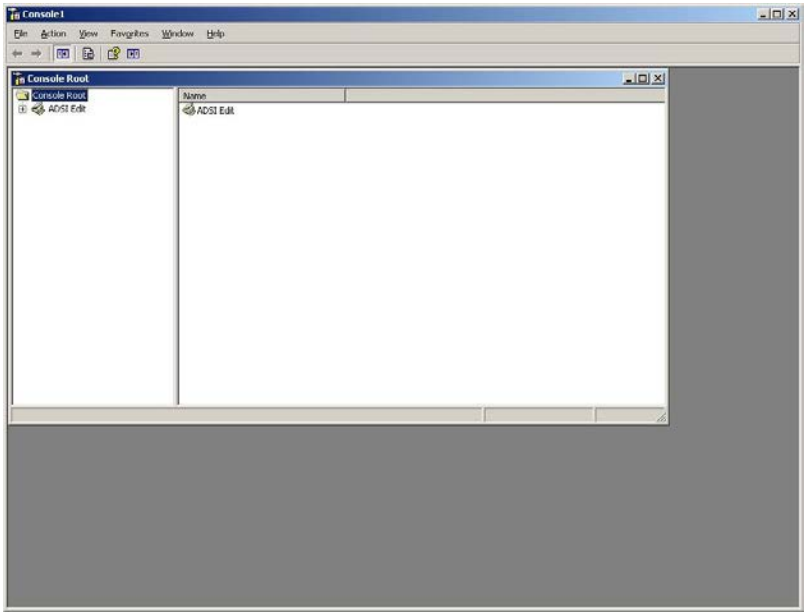
2 When the Microsoft Management Console (MMC) screen is displayed, select **Menu > File > Add/Remove Snap-in**. In the **Add Standalone Snap-in** screen, click **Add…**, select **ADSI Edit** from **Available standalone snap-ins:**, click **Add**, and then click **Close**.





Tip When ADSI Edit is not available, see Windows support tools.

3 When “ADSI Edit” is added to the Add Standalone Snap-in screen, click **OK**. Confirm that **ADSI Edit** is added to **Console Root** in the MMC screen.



4 Click **ADSI Edit** in the MMC screen, and select **Connect to…**.

5 Select **Domain** for the domain context of Active Directory to connect, and click **OK**.



6 Open the ADSI Edit tree, and right-click a user account to give roles on the LDAP directory to open **Properties**.

7 A list of attributes assigned to the user account is displayed.



8 Select an attribute with “Unicode String” for Syntax and with “<Not Set>” for Value, and click **Edit**.

9 Set roles for server blades with the following character string.

ServerBladeRole=XXXXXXXX

X: “0” or “1”
XXXXXXXX: each X from the head to the end corresponds to a following role in the numerical order.

1 Login
2 Administrator
3 Server Operation
4 User Account Management
5 Service Settings
6 Remote Console
7 Remote Media
8 SMASH CLIP

10 Set roles for management modules with the following character string.

“Management ModuleRole=role_name”

role_name: used role names defined to the management module

11 After setting roles, click **OK**.

12 When the screen returns to Properties, click **OK**.

The procedure above completes the role setting for users to log in to the management module and BMC.



When typing roles for BMC and the management module consecutively, divide them with a blank space.

Setting example:
ServerBladeRole=10101010 ManagementModuleRole=Administrator

❑ Registering groups

Register the group to use for group authentication.



If you do not use group authentication, this setting is not required.

Open **Management Tools > Active Directory Users and Computers**, create a group you allow login to server blades and a group you allow login to management modules in the LDAP directory. After you create the groups, register user accounts you allow login with each group.

For details about how to create groups and how to register user accounts with groups, see the documentation of your Windows server.



You can use a single group for logging in to server blades and management modules.

❑ Windows support tools

Windows Support Tools is a package software program that contains "ADSI (Active Directory Service Interface) Edit" for operating objects registered with Active Directory, and "ldp" for performing Active Directory operations through LDAP.

This section describes how to check whether this package software is installed



When Windows Server 2008 or later versions are equipped with this package, skip this procedure.

Select **Control Panel** and open **Add and Remove Programs**. The list of installed programs is displayed.

When “Windows Support Tools” is displayed in the list, “ADSI Edit” and “ldp” are available. If not, install “Windows Support Tools” from the install media.

Setting management modules and server blades

This section describes necessary settings for connecting management modules to LDAP servers.

Tip For details about server blade settings, see the "LDAP Setup" of the Web console for server blades.

❑ Setting user authentication

Enable the function for connecting to LDAP of “LDAP Server Linkage Setup” for the system web console. By enabling this function, the system searches the LDAP directory on the LDAP server at user authentication, and tries to authenticate users.

Tip

- If the LDAP connection function is enabled, you can log in to management modules and BMC by using the user account you already set
- If you register a user account name you already set for management modules and BMC with the LDAP directory, the system authenticates users by using the user account information set for management module and BMC.

❑ Registering LDAP servers

A maximum of three LDAP servers can be registered. If you register multiple LDAP servers, the system tries to connect to the LDAP servers in the order they were registered. The system searches the LDAP directory on the server of which connection was established first, and tries to authenticate users.

If the system fails to connect to all the registered LDAP servers, user authentication using the LDAP servers also fails.

Tip Even if the system fails to connect to all registered LDAP servers, it can authenticate users by using a user account registered with a management module and BMC correctly.

❑ Setting the LDAP server connection

Port number

Specify the port number to use for connecting to the LDAP server. Normally, the 636 port is used, however, depending on your environment, you might have to use another port. Check your network environment before you specify a port.

❑ Bind DN and bind password

Set the method for connecting the LDAP server at user authentication.

You must set the method according to the settings you specified during user registration for LDAP connection.

❑ Setting for searching the LDAP directory

Base DN

Specify the DN for the root directory of the LDAP directory to be searched. The directories under the specified root directory are to be searched at user authentication.

Attribute indicating login IDs

Specify the attribute of each entry in the LDAP directory to be compared with the user ID specified at user authentication.

For Active Directory, the attribute name “sAMAccountName” is used for searching login IDs usually.

Attribute indicating roles

If you grant a role to the user account for logging in to a management module and BMC during the operation described in Granting role information, specify the attribute used for granting the role.



If you did not grant a role, you do not need to perform this operation.

Setting group authentication



If you do not specify group settings during the operation described in "Registering Groups", you do not need to perform this operation.

Attribute indicating groups

Specify the attribute in which the list of user accounts whose login is to be allowed is stored.

For Active Directory, the list of user accounts is normally stored in the attribute name “member”.

DN whose login is allowed

Specify the group DN created in Registering groups.

A maximum of five groups can be specified. User accounts of which login you want to allow must belong to one of the specified groups.

Power efficiency

This section describes the energy-saving features of the Compute Blade 2000.

Compute Blade 2000 is equipped with the following energy-saving features to reduce power consumption and initial costs:

- Power monitoring
- Power capping
- Demand Base Switching (DBS)
- Optimum Control on Power Supply Module
- Restriction on maximum power consumption

Power monitoring

Power usage by the server blades and server chassis is displayed in graph format on the management module's system web console. The server administrator can easily see how much power is being consumed by the server.

The power usage windows provide a Current Data view and Trend Data view. The Current Data view shows information about the current power usage of the server blades and server chassis. The Trend Data view shows historical information about power usage by the server chassis as a 24-hour graph or in table format.

❑ Current data view

In the Current Data view, you can view the following power usage data for the server chassis and server blades.

- Server chassis

Item	Description
Maximum power supply **W**	Total DC power supplied by all Power Supply Modules
Current power supply **W**	Total DC power supplied by the active Power Supply Modules. The display changes when optimized Power Supply Module control is enabled.
Power rating **W**	Maximum DC power consumed by the server chassis
Current power consumption **W**	Current DC power consumed by the server chassis
Chassis power consumption (AC) **W**	Current AC power consumed by the server chassis
Mean power consumption **W**	Mean DC power consumed by the server chassis during the three minutes prior to the time the current was measured
Minimum power consumption **W**	Minimum DC power consumed by the server chassis during the three minutes prior to the time the current was measured
Maximum power consumption **W**	Maximum DC power consumed by the server chassis during the three minutes prior to the time the current was measured

- Server blade

Item	Description
Current power consumption **W**	Current power consumed by the server blade
Mean power consumption **W**	Mean power consumed by the server blade during the three minutes prior to the time the current was measured
Minimum power consumption **W**	Minimum power consumed by the server blade during the three minutes prior to the time the current was measured
Maximum power consumption **W**	Maximum power consumed by the server blade during the three minutes prior to the time the current was measured
Power rating **W**	Maximum power consumed by the server blade
CPU frequency **MHz**	Current operating frequency of the CPU. When DBS is enabled, the CPU frequency shown by the OS may be less than the displayed value. When Turbo Mode is enabled, the CPU frequency shown by the OS may be greater than the displayed value.
Maximum CPU frequency **MHz**	Maximum operating frequency of the CPU. When Turbo Mode is enabled, the CPU frequency shown by the OS may be greater than the displayed value.

- Power supply module

Item	Description
Maximum power supply **W**	Maximum DC power that can be supplied by the Power Supply Module
Current power consumption **W**	Current power supplied by the Power Supply Module

- Management module

Item	Description
Power rating **W**	Maximum power consumed by the Management Module

- Switch Module

Item	Description
Power rating **W**	Maximum power consumed by the Switch Module

For details about how to check power usage on the Management Module's system Web console, see "Server Chassis Management" in Chapter 6. To check power usage in command mode, see "PS Command" in Chapter 6.

❑ Trend data view

In the Trend Data view, you can view power usage data for the server chassis and server blades in graph or table format. The data covers the 24 hours of the previous day (from 00:00 to 23:59) or the 24 hours prior to the time the current was measured. The Management Module collects power usage data at 3-minute intervals.

You can view this information in two ways: (1) Graph display, or (2) Table display. To view server chassis power usage data, see "Power Status Trend View (Chassis)". For more information, see Chapter 6. To view server blade power usage data, see "Power Status Trend View (Partition)". For more information, see Chapter 6. To view the information in command mode, see "DL Command". For more information, see Chapter 11.

Power capping

By using the power capping feature, processor performance can be automatically adjusted so that the server blade's power consumption never exceeds a limit value set by the server administrator. This allows applications to run at optimal performance per watt*, reducing excess heat generation and lowering power infrastructure costs.

Using the Management Module's system Web console, the server administrator can set a limit value or "cap" on the power consumption of a selected server blade. The set power cap must be between the minimum and maximum power consumption values displayed on the console.

Power capping has two control modes: Static control and dynamic control.

In static control mode, appropriate ACPI processor performance states (P-states) are set for the server blade's CPU in line with the specified power capping value so that the server blade's maximum power consumption is kept within a set limit. In contrast, in dynamic control mode, CPU performance is lowered only when power consumption comes close to the power capping value, keeping the server blade's mean power consumption within a set limit. High performance server blades support only dynamic control.

*Indicator of performance per consumed power

❑ Supported OS

The Compute Blade 2000's power capping feature has been verified to work in static control mode with the following operating systems. Dynamic control mode is independent of the OS and works with any operating system.

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

❑ Notes on settings

To use power capping, you must enter settings on the EFI Setup screen and on the Management Module's system Web console. Once entered, do not change the settings while power capping is enabled.

(1) Setting on the EFI setup screen

On the EFI Setup screen, enable the CPU's EIST functionality. For details, see "EFI Setup Screen". On the Advanced menu, select "CPU Configuration". On the displayed sub-menu, select "EIST" and set "Enabled".

(2) Settings on the management module's system web console

Set up the power capping feature on the "Power Control Settings List View" of the Management Module's system Web console.

#	Setup Item	Required Setting for Power Capping	Default
1	Power capping enable/disable	Enabled	Disabled
2	Power cap	Any value. The specifiable range will differ for each server blade configuration.	Not set
3	Control mode (*1)	Select "Static" for static control mode. Select "Dynamic" for dynamic control mode.	Static
4	Exception processing	Set the server blade's behavior when the power consumption within a defined period exceeds a user-specified value. 1. Log a fault (SEL). -> Warning 2. Log a fault (SEL) and set the CPU duty cycle to 12.5%. -> Warning & CPU duty cycle 12.5%	Warning & CPU duty cycle 12.5%

(*1) When you select static control mode for high performance server blades, a warning to show “not supported”.

For details about how to set the power capping feature, see "Power Control Settings List View" in Chapter 6. Alternatively, for the procedure in command mode, see "PSV Command" in Chapter 6.



Power capping is set on a partition basis.

- When a server blade defined in a partition is replaced, the power capping settings are inherited by the replacement server blade.
- Power capping settings are not transferred from the active partition to the standby partition in an N+M cold standby configuration. If you want the power capping settings to be inherited by the standby partition when switched in, you must enter the same settings on both the active and standby partitions.

DBS (Demand Base Switching)

DBS (Demand Base Switching) is a function that controls ACPI processor performance states (P-states) based on CPU usage. CPU voltage and frequency vary in line with the set P-states. DBS optimizes voltage and frequency according to CPU usage, minimizing the CPU's power consumption.

By enabling the DBS functionality, the CPU's frequency, as verifiable in the OS, can be seen as lower than the rated frequency, depending on the set DBS values and CPU workload.

❑ Setting procedure

To use DBS, you must enter settings on the BMC's server blade Web console and in the OS.

(1) Setting on the EFI setup screen

On the EFI Setup screen, enable the CPU's Enhanced Intel SpeedStep Technology (EIST) functionality. For details, see "EFI Setup Screen". On the Advanced menu, select "CPU Configuration". On the displayed sub-menu, select "EIST" and set "Enabled".

(2) Settings in the OS (Windows Server 2003)

The following describes how to set up DBS in Windows Server 2003.

From the Control Panel, click "Power Options". On the "Power Schemes" page, change the "Power schemes" settings. Those relating to DBS are as follows. DBS is enabled by setting "Server Balanced Processor Power and Performance power scheme" (item 2).

#	Setup Item	Description
1	Always on	Sets the performance state to the highest level, and disables DBS. This is the default setting.
2	Server Balanced Processor Power and Performance power scheme	Enables DBS, and changes the performance state dynamically according to the CPU load.

(3) Setting in the OS (Windows Server 2008)

The following describes how to set up DBS in Windows Server 2008.

From the Control Panel, click "Power Options". On the "Select a power plan" page, change the power plan settings. DBS is enabled by setting "Balanced" (item 1).

#	Setup Item	Description
1	Balanced	Enables DBS, and changes the performance state dynamically according to the CPU load. This is the default setting.
2	Power saver	Sets the performance state to the lowest level.
3	High performance	Sets the performance state to the highest level, and disables DBS.

Optimized power supply module control

Optimized Power Supply Module control is functionality that controls the number of active Power Supply Modules (modules with DC output ON) installed in the Compute Blade 2000 according to the number of active server blades. The Compute Blade 2000 Power Supply Modules convert AC power to DC power. The conversion efficiency differs according to how much DC power is output. Generally speaking, the greater the output DC power, the higher conversion efficiency is obtained.

When optimized control is used, the Management Module determines the ON/OFF status of the DC output of each Power Supply Module so that a minimum number of Power Supply Modules supply the DC power required to run the server blades. The server blades' power requirements are determined from the pre-defined server blade configuration (CPU or memory configuration).



When redundant power supplies cannot be maintained, DC output is not turned off.

❑ Setting procedure

To use optimized Power Supply Module control, you must enter settings on the "Power Control Settings List View" of the Management Module's system Web console. Alternatively, enter the required settings in command mode, using the "PSM Command". Note that optimized control is disabled by default.

Control of maximum power consumption

Control of maximum power consumption is functionality that keeps the power consumption of the server chassis as a whole within a user-specified value by limiting the number of server blades that are active in the server chassis. This allows the server chassis to be safely installed and operated even in an infrastructure with limited power capacity.

The number of active server blades is determined from the power requirements of each pre-defined server blade configuration (CPU or memory configuration).

❑ Setting procedure

To use control of maximum power consumption, you must enter settings on the "Power Control Settings List View" of the Management Module's system Web console. Alternatively, enter the required settings in command mode, using the "PSV Command". Note that power consumption control is disabled by default.

Dictionary updating

This section describes the procedure for updating the dictionary with management modules and I/O slot expansion units.

Tip

The dictionary means the data that defines meanings of events created in Compute Blade and actions for those events, and the shared data used between devices.

Note

- Do not downgrade the current dictionary to any earlier version.
- Locate the currently installed dictionary version in “Firmware Management View” in the system Web console, “FV Command” or “FW Command” in the system console, Chapter 6, or “FW Command” in the I/O slot expansion unit console in Chapter 10.
- Check your dictionary version with the dictionary file name as follows:

  Naming rules: dict.xxxxx.update
  xxxxx: Dictionary version

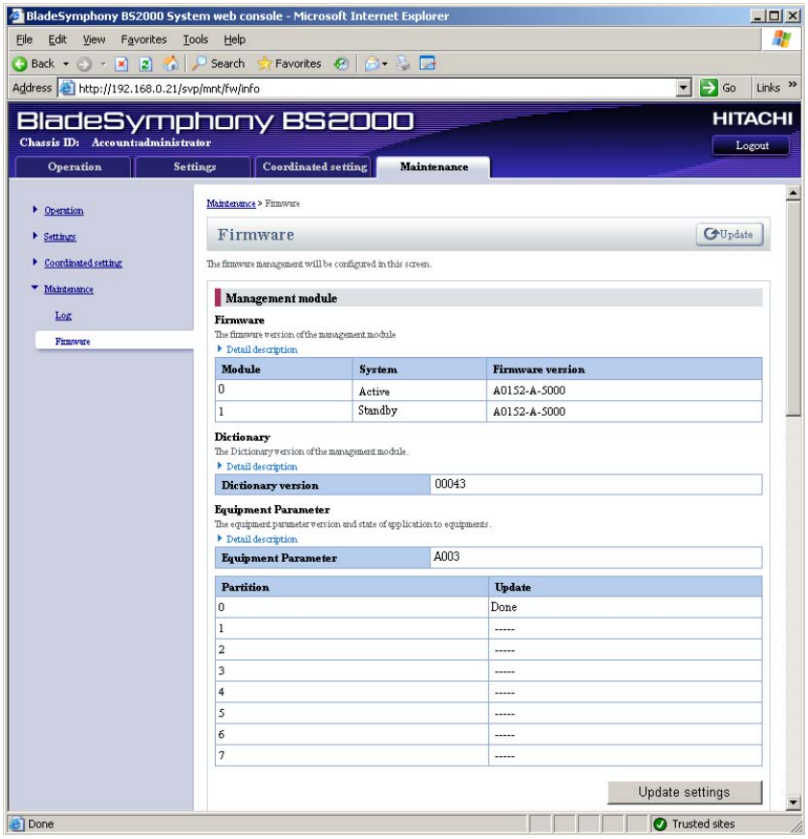
The procedure with the system Web console is shown below. With the system console, see “FW Command” in Chapter 6. With the I/O slot expansion unit console, see “FW Command” in Chapter 10.

Updating dictionary

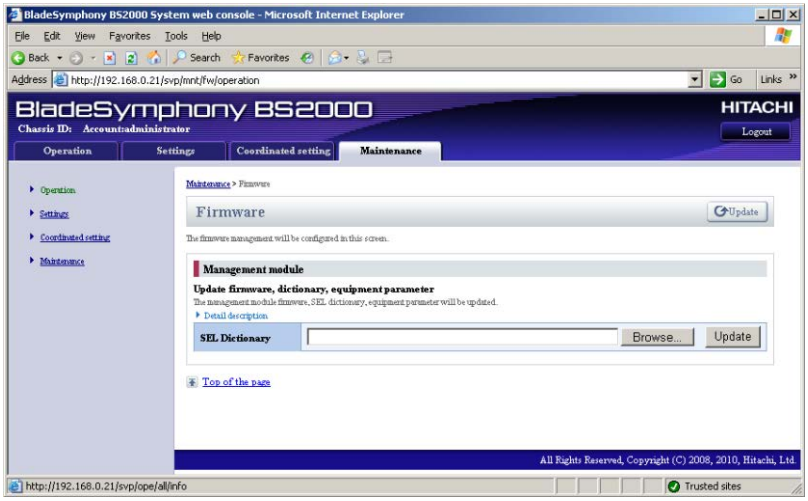
1 Log in to the system Web console as Administrator.

2 Select **Maintenance > Firmware** in the menu on the left of the screen.

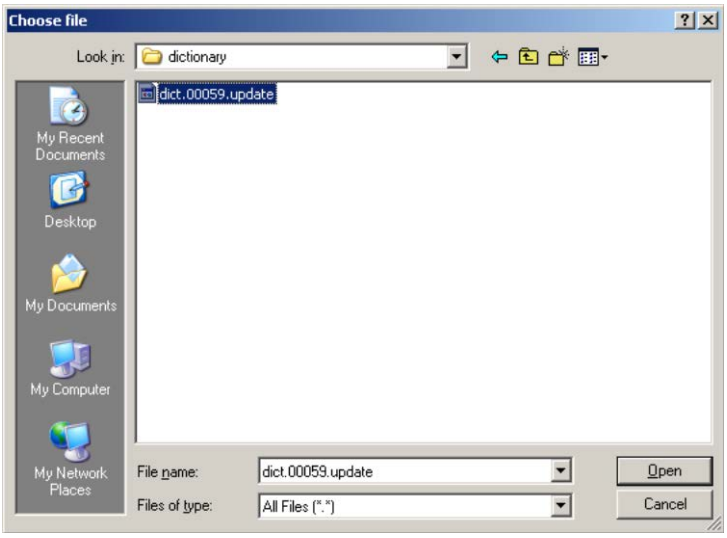
3 In the Firmware screen, click **Update settings**.



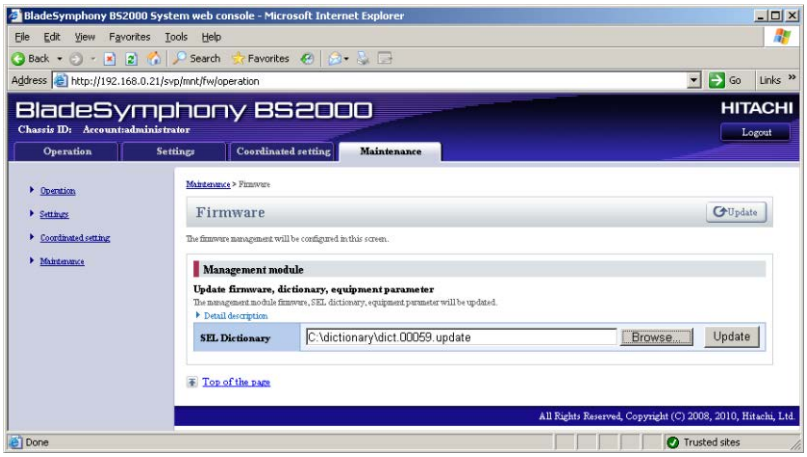
4 Click **Browse...**.



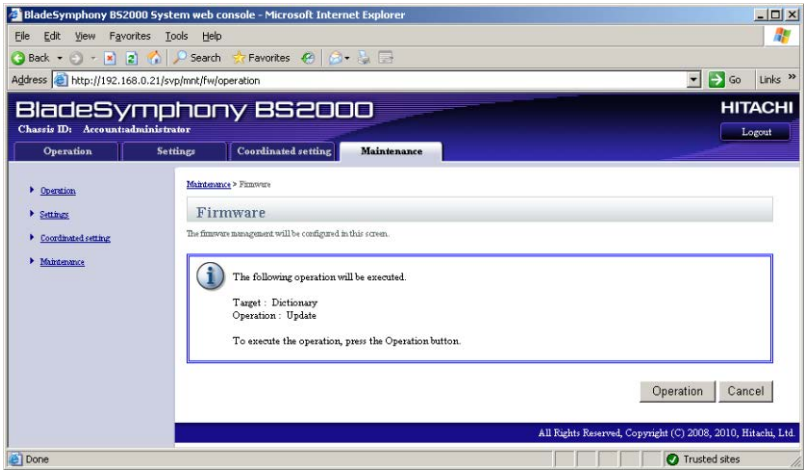
5 In the Choose file window, select a dictionary file and click **Open**.



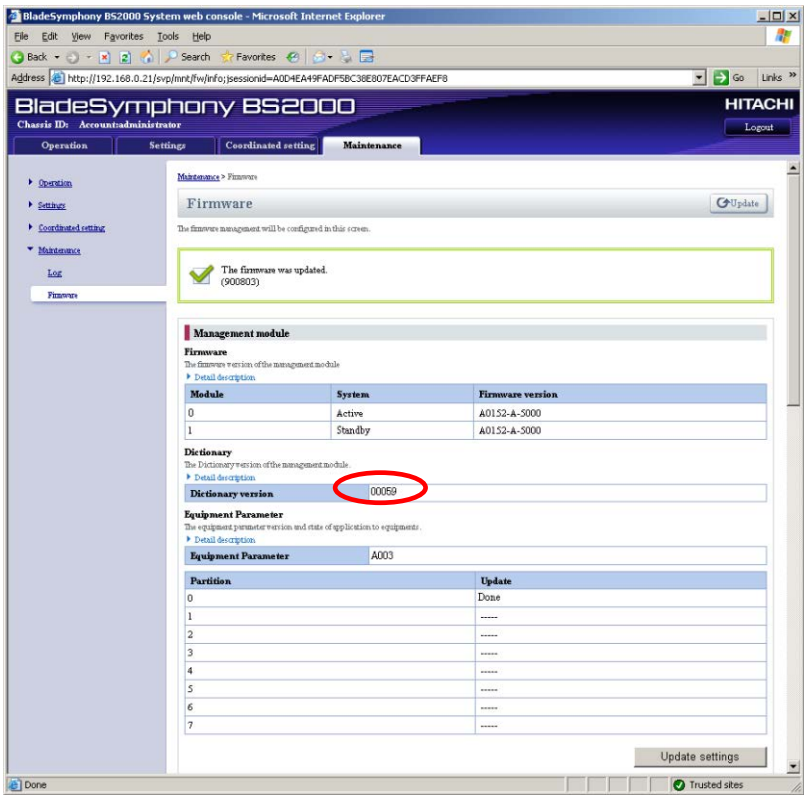
6 Confirm that the file you selected is displayed in the dictionary field, and click **Update**.



7 In the confirmation screen, click **Operation**. Dictionary update starts.



8 When the dictionary update is completed, the screen returns to **Firmware**. Confirm that your dictionary version has been updated.



Operation log

Operation log overview

❑ Operation log

The operation log function records logs for operations to the system unit. The following list shows those logs, including some logs for operations to management modules and server blades. Management module operation logs are downloaded from the system Web console, and sever blade operation logs from the server blade Web console.



- When a management module is changed not in the non-redundant configuration, the management module operation logs recorded so far will be lost.
- When a server blade is changed, the server blade operation logs will be lost.
- This function is available with management firmware version A0182 or later.
- When using this operation log function withX55 A1/X55A2 model, you need to install BMC firmware version 03-91 or later.
- When using this operation log function with X57A1 model, you need to install BMC firmware version 04-51 or later
- Operation log messages can be changed depending on the firmware version.

❑ Specifications of operation log

The following table describes specifications of operation logs.

No.	Item	Description	
		Server blade operation logs	Management module operation logs
1	Recording	Operation events are classified into four categories described in the list later, and three results including Success, Failure, and Occurrence are recorded.	
2	Coverage	The system start and stop; authentication; change in the settings; maintenance operation (See Operation log messages for details.)	
3	Number of logs	Up to 2,048 logs per partition The oldest log is overwritten when the number of logs reaches the upper limit in each partition.	Operations available with the partition privilege: up to 2,048 logs per partition Operations other than the above: up to 2,048 logs Overwrites the oldest log when the number of logs reaches the upper limit in each partition.

No.	Item	Description	
		Server blade operation logs	Management module operation logs
4	Download	Downloads logs from the Log tab on the server blade Web console. See Standard Server Blade Settings (X55A1/X55A2 Models) > Logs Tab in Chapter 5 for how to download logs with the server blade Web console.	Downloads logs from the Log Management View of the system Web console. See System Web Console > Log Management in Chapter 6 for how to download logs with the system Web console.
5	Restrictions on download	None	Restrictions depend on the account privilege used in login: Partition privilege: Can download only from permitted partitions. Chassis privilege: can download form all partitions or the server chassis including all partitions.
6	Number of logs to be downloaded	Up to 2,048 logs	Partition selected: Up to 2,048 logs Server chassis selected: Up to 18,432 logs: 2,048 x 8 partitions and 2,048 for logs of other than partitions.
7	Download file format	Comma-separated values (CSV) file: a comma "," is used as a separator.	
8	Download file name	operation log_<model name>_<product code>.csv <model name>_<product code> are identical to those of the server blade with which you have downloaded logs.	opr-YYYYMMDD-hhmmss.csv YYYYMMDD-hhmmss shows the time when you have downloaded logs. YYYY: A.D.; MM: month; D: day; hh: hour; mm: minute; ss: second

❑ Operation log format

The following table describes the download format for operation logs. Management modules and server blades use the same format for their operation logs.

No.	Item ( ): header	Number of letters	Description	Remarks
1	Sequence number (seq_no)	1 to 10	A sequence number to specify a log in the management module is provided from 1 to 9999999999. If beyond 9999999999, it returns to 1 (one).	-
2	Day/time (date)	29	A day and time zone when and where a log is recorded. YYYY-MM-DDThh:mi:ss.SSS±h2:s2 YYYY: A.D.; MM: month; DD: day; T: fixed	-

No.	Item ( ): header	Number of letters	Description	Remarks
			(separator); hh: hour; mi: minute; ss: second; SSS: millisecond (000 fixed); h2: UTC offset (hour)*; m2: UTC offset (minute)* *: time zone is recorded as UTC offset.	
3	Partition number (par_no)	1	- Server blade: A partition number where an operation event is generated. - Management module: Partition number 0 to 7 for partitions available with the partition privilege Partition number 8 for operations other than the above.	Logs only for operations with the partition privilege out of the management module operation logs are provided to users with the partition privilege. Thus, logs are allocated to and stored in each partition with a specific number.
4	Component name (compid)	7 to 17	The name of a component where you operated - Server blade operation logs: Server Blade - Management module operation logs: Management Module	-
5	Operation place (place)	15 to 40	Host name of a component where you operated - Server blade operation logs: an IP address of the server blade Management module operation logs: an IP address of the management module	-
6	Operation category (categ)	7 to 19	A category name for each operation	See the Category of Operation Event below.
7	Operation result	7 to 10	An operation result: Success; Failure; Occurrence	See the Operation Event Result below.
8	Operation type (subjtype)	10 to 14	- Operation by a user: User Operation - Operation by a system process: System Process	-
9	Operator (subject)	1 to 32	- Operation by a user: the login name - Operation by a system process: the process identifier	
10	Session ID (sessionid)	3 to 32	Information to identify 2 or more users when they	N/A is shown when no login is detected such as

No.	Item ( ): header	Number of letters	Description	Remarks
			log in with the same account.	a system process.
11	Message ID (msgid)4	4	message ID in hexadecimal	-
12	Message (message)	1 to 240	Message to an operation	-

Each item is recorded in a variable length record.

A header is added to the first line at the format change. See the dump examples of operation logs shown below for output contents to headers.

Items are separated by commas ",". A linefeed, such as CR (Carriage Return) or LF (LineFeed) is added to the end of each line.

No.12 Message is recorded with double quotation marks enclosed.

Category of operation event

No.	Category	Operation event
1	StartStop	Start and stop
2	Authentication	Identification and authentication
3	ConfigurationAccess	Configuration access
4	Maintenance	Maintenance

Result of operation event

No.	Result	Operation event
1	Success	The operation event is successful.
2	Failure	The operation event failed.
3	Occurrence	The operation event occurred without success or failure.

The following shows the dump examples of operation logs

```
seq_no,date,par_no,compid,place,categ,result,subjtype,subject,sessionid,msgid,message
1,2011-05-22T06:33:18.000+09:00,0,Management module,192.168.0.1,StartStop,Success,User
Operation,maintenance,FFFFFFFF,8000,"On Partition0, requested operation. Channel:System
Console Method:Power on"
2,2011-05-22T06:33:18.000+09:00,0,Management module,192.168.0.1,StartStop,Success,User
Operation,maintenance,FFFFFFFF,8000,"On Partition0, requested operation. Channel:System
Console Method:Shutdown"
3,2011-05-22T06:33:18.000+09:00,1,Management module,192.168.0.1,StartStop,Success,User
Operation,maintenance,FFFFFFFF,8000,"On Partition1, requested operation. Channel:System
Console Method:Power on"
4,2011-05-22T06:33:18.000+09:00,1,Management module,192.168.0.1,StartStop,Success,User
Operation,maintenance,FFFFFFFF,8000,"On Partition1, requested operation. Channel:System
Console Method:Shutdown"
5,2011-05-22T06:33:18.000+09:00,2,Management module,192.168.0.1,StartStop,Success,User
Operation,maintenance,FFFFFFFF,8000,"On Partition2, requested operation. Channel:System
Console Method:Power on"
```

Operation log messages

Management module operation logs

ID	Operation event type	Event logged (*1)	Message
0800	Start Stop	PC command requested operation on the partition.	On Partition%1$s, requested operation. Channel:%2$s Method:%3$s
0801		PC command failed to request operation on the partition.	On Partition%1$s, failed to requested operation. Channel:%2$s Method:%3$s
0802		MMC command requested operation on the management module	On Management module%1$s, requested operation. Channel:%2$s Method:%3$s
0803		MMC command failed to request operation on the management module	On Management module%1$s, failed to requested operation. Channel:%2$s Method:%3$s
0804		SDN command requested shutdown of the system	On Server chassis, requested shutdown. Channel:%1$s
0805		SDN command failed to request shutdown of the system	On Server chassis, failed to requested shutdown. Channel:%1$s
0806		SWC command requested operation on the switch module	On Switch module%1$s, requested operation. Channel:%2$s Method:%3$s
0807		SWC command failed to request operation on the switch module	On Switch module%1$s, failed to requested operation. Channel:%2$s Method:%3$s
1800	Authentication	logged in to the system console	Logged in to the System Console. Username:%1$s Session ID:%2$s Source IP address:%3$s
1801		Failed to log in to the system console	Failed to login to the System Console. Username:%1$s Source IP address:%2$s Cause:%3$s
1802		Logged out of the system console.	Logged out from the System Console. Username:%1$s Session ID:%2$s Source IP address:%3$s Cause:%4$s
1803		Logged in to the system Web console	Logged in to the System Web Console. Username:%1$s Session ID:%2$s Source IP address:%3$s
1804		Failed to log in to the system Web console	Failed to login to the System Web Console. Username:%1$s Source IP address:%2$s Cause:%3$s
1805		Logged out of the system Web console	Logged out from the System Web Console. Username:%1$s Session ID:%2$s Source IP address:%3$s Cause:%4$s
1806		Failed to log in to the system console or system Web console	Failed to login to the Console. Cause:%1$s

ID	Operation event type	Event logged (*1)	Message
3800	Configuration Access	PR command changed partition settings	On Partition%1$s, setting is changed. Channel:%2$s Category:%3$s Detail:%4$s Value:%5$s
3801		PR command changed partition configurations	On Partition%1$s, setting is changed. Channel:%2$s Category:%3$s Partition:%4$s Blades:%5$s
3803		PSM command changed power supply module settings	On Power supply module, setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
3804		PSM command changed power supply module settings	On Power supply module%1$s, setting is changed. Channel:%2$s Category:%3$s Detail:%4$s Value:%5$s
3806		LC command changed management module LAN settings	Management LAN setting is changed. Channel:%1$s Category:%2$s Value:%3$s
3807		LC command changed partition LAN settings	On Partition%1$s, LAN setting is changed. Channel:%2$s Category:%3$s Value:%4$s
3808		LC command changed switch module LAN settings	On Switch module%1$s, LAN setting is changed. Channel:%2$s Category:%3$s Value:%4$s
3809		LC command changed switch module LAN settings	On Switch module%1$s, LAN setting is changed. (ApplyManaegment module setting) Channel:%2$s
380E		LC command changed VLAN settings	VLAN setting is changed.(Move port) Channel:%1$s Target:%2$s Partition:%3$s Switch module:%4$s VLAN ID:%5$s
380F		LC command created a VLAN	VLAN is created on management LAN port. Channel:%1$s VLAN ID:%2$s Ext port:%3$s
3810		LC command removed a VLAN	VLAN is removed on management LAN port. Channel:%1$s VLAN ID:%2$s
3814		SD command changed date and time settings	Date and time is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
3818		SO command created an account	An account is created. Channel:%1$s ID:%2$s Status:%3$s Role:%4$s
3819		SO command removed an account	An account is removed. Channel:%1$s ID:%2$s
381C		SO command created a role	A role is created. Channel:%1$s Role name:%2$s P01234567:%3$s SW012345:%4$s Net:%5$s Chassis:%6$s Account:%7$s
381D		SO command removed a role	A role is removed. Channel:%1$s Role:%2$s
381F		WWN command initialized an additional WWN	Additional WWN is initialized. Channel:%1$s Partition:%2$s Blade:%3$s
3820		WWN command	Additional WWN is changed.

ID	Operation event type	Event logged (*1)	Message
	Configuration Access	changed additional WWN settings	Channel:%1$s Partition:%2$s Blade:%3$s
3821		DC command requested restoration to the factory settings	Reset management module to factory setting. Channel:%1$s Category:%2$s
3822		DC command requested sever blade Web console settings or restoration to the factory settings	Reset partition%1$s to factory setting. Channel:%2$s Category:%3$s
3826		BSM command changed SC/BSM connection settings	SC/BSM connection setting is changed. Channel:%1$s Server#:%2$s Category:%3$s Value:%4$s
3827		BSM command changed SC/BSM connection settings	SC/BSM connection setting is changed.(detail setting) Channel:%1$s Server#:%2$s Category:%3$s Value:%4$s
3828		BSM command removed a SC/BSM connection setting	SC/BSM connection setting is removed. Channel:%1$s Server#:%2$s
3829		BSM command changed SC/BSM connection settings	SC/BSM connection setting is changed.(command port#) Channel:%1$s Value:%2$s
382A		BSM command sent SC/BSM test alert	On Partition%1$s, SC/BSM send test alert(N+M cold standby) Channel:%2$s Category:%3$s
382B		MI command changed e-mail settings	E-mail setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
382C		MI command changed e-mail settings	E-mail setting is changed. Channel:%1$s Address:%2$s Detail:%3$s Value:%4$s
382D		MI command removed e-mail settings	E-mail setting is removed. Channel:%1$s Address:%2$s
382E		SNM command changed SNMP settings	SNMP setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
382F		SNM command deleted SNMP settings	SNMP setting is removed Channel:%1$s Category:%2$s Number:%3$s
3830		SEC command changed service settings	%1$s service setting is changed. Channel:%2$s Category:%3$s Value:%4$s
3832		CER command created an SSH host key pair	SSH host key pair is created. Channel:%1$s
3834		CER command backed up an SSH host key pair	SSH host key pair is removed. Channel:%1$s File:%2$s
3836		CER command restored an SSH host key pair	SSH host key pair is restored. Channel:%1$s File:%2$s
3838		CER command created an SSH host key pair and self signed certificate	SSL private key and self signed certificate are created. Channel:%1$s
383A		CER command created	SSL private key and certificated signing

ID	Operation event type	Event logged (*1)	Message
		CSR	request (CSR) are created. Channel:%1$s
383C		CER command imported a certificate	Certificate is imported. Channel:%1$s File:%2$s Certificate file type:%3$s
383E		CER command copied a certificate	Certificate is copied. Channel:%1$s File:%2$s Certificate file type:%3$s
3840		CER command backed up a certificate	Certificate is backed up. Channel:%1$s File:%2$s
3842		CER command restored a certificate	Certificate is restored. Channel:%1$s File:%2$s
3844		UBR command backed up management module settings	Management module setting is backed up. Channel:%1$s File:%2$s
3845		UBR command restored management module settings	Management module setting is restored. Channel:%1$s File:%2$s
3847		UBR command backed up server blade settings	On Partition%1$s, setting(%2$s) is backed up. Channel:%3$s File:%4$s
3849		UBR command restored server blade settings	On Partition%1$s, setting(%2$s) is restored. Channel:%3$s File#:%4$s
384B		LDAP command changed LDAP settings	LDAP setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
384C		LDAP command changed LDAP settings	LDAP setting is changed. Channel:%1$s Category:%2$s Detail:%3$
384E		UBR command restored server blade settings	On Partition%1$s, setting (&2$s) is restored. Channel:%3$s Category:%4$s Blade:%5$s Slot:%6$s Slot on IOEU:%7$s
384F		UBR command removed server blade settings file	On Partition%1$s, setting (&2$s) is removed. Channel:%3$s Category:%4$s Blade:%5$s Slot:%6$s Slot on IOEU:%7$s
3850		PSV command changed power saving settings	Power saving setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
3851		PSV command changed power saving settings	On Partition%1$s, Power saving setting is changed. Channel:%2$s Category:%3$s Detail:%4$s Value:%5$s
3860		N+M cold standby changed partition information settings	On Partition%1$s, N+M cold standby partition information setting is changed. Channel:%2$s
3900	Configuration Access	HCSM command changed HCSM service settings	HCSM cooperation setting is changed. Channel:%1$s Category:%2$s Detail:%3$s Value:%4$s
3901		HCSM command added HCSM server settings	HCSM manager setting is created. Channel:%1$s IP address:%2$s Alert port:%3$s Alert level%4$s Retry interval:%5$s Retry duration:%6$s
3902		HCSM command	HCSM manager setting is changed.

ID	Operation event type	Event logged (*1)	Message
	Configuration Access	changed HCSM server settings	Channel:%1$s IP address:%2$s Category:%3$s Before:%4$s After:%5$s
3903		HCSM command changed HCSM server settings	HCSM manager setting is changed. Channel:%1$s IP address:%2$s Detail:%3$s Value:%4$s
3904		HCSM command deleted HCSM server settings	HCSM manager setting is removed. Channel:%1$s IP address:%2$s
3905		HCSM command disconnected HCSM server session	HCSM server is disconnected. Channel:%1$s IP address:%3$s
3913		Changing Syslog transfer settings	Syslog transfer setting is changed. Channel:%1$s Detail:%2$s Value:%3$s
3917		Backing up the fibre channel settings (For mezzanine card and I/O board)	On Partition%1$s, setting(%2$s) is backed up. Channel:%3$s Category:%4$s Blade:%5$s Slot:%6$s File:%7$s
3918		Backing up the fibre channel settings (For I/O board on an I/O slot expansion unit)	On Partition%1$s, setting(%2$s) is backed up. Channel:%3$s Category:I/O adapter on IOEU Blade:%4$s Slot:%5$s Slot on IOEU:%6$s File:%7$s
385E		MAC command initialized additional MAC address settings	Additional MAC is initialized. Channel:%1$s Partition:%2$s Blade:%3$s
385F		MAC command changed additional MAC address settings	Additional MAC is changed. Channel:%1$s Partition:%2$s Blade:%3$s

Note (*1) This item shows system console command names, and logs are collected by the same function of the system Web console.

Server blade operation logs

ID	Operation event type	Event logged	Message
0001	Start Stop	Powered on the server blade	Requested a power-on of the server blade. Method:xxx
0002		Powered off the server blade	Requested a power-off of the server blade. Method:xxx xxx
0003		Reset the server blade	Requested a reset of the server blade. Method:xxx
0004		Issued an NMI signal	Issued an NMI signal of the server blade. Method:xxx
0005		Pressed the power button	Pressed the power button of the server blade.
0007		Pressed the reset button	Pressed the reset button of the server blade.
000C		Restarted BMC	Requested a restart of BMC. Method:xxx
0012		BMC started successfully	BMC started successfully.
0013		BMC failed to start	BMC failed to start.
0014		The server blade is being powered on	The server blade is powered on.
0015		The server blade is being powered off	The server blade is powered off.
0017		Requested OS shutdown	Requested an OS shutdown of the server blade. Method:xxx
0018		EFI started successfully	EFI started successfully.
1001	Authentication	Logged in to the remote console	Logged in to the remote console. Username:xxx Source IP address:xxx User authentication method:xxx
1002		Logged out from the remote console	Logged out from the remote console. Username:xxx Source IP address:xxx Cause:xxx
1003		Failed to login to the remote console	Failed to login to the remote console. Username:xxx Source IP address:xxx Cause:xxx
1004		Started using the remote FD	Started using the remote FD. Username:xxx Source IP address:xxx
1005		Stopped using the remote FD	Stopped using the remote FD. Username:xxx Source IP address:xxx Cause:xxx
1006		Started using the remote CD/DVD	Started using the remote CD/DVD. Username:xxx Source IP address:xxx
1007		Stopped using the remote CD/DVD	Stopped using the remote CD/DVD. Username:xxx Source IP address:xxx Cause:xxx
1008		Logged in to the server blade web console	Logged in to the server blade web console. Username:xxx Source IP address:xxx User authentication method:xxx

ID	Operation event type	Event logged	Message
1009		Logged out from the server blade web console	Logged out from the server blade web console. Username:xxx Source IP address:xxx Cause:xxx
100A		Failed to login to the server blade web console	Failed to login to the server blade web console. Username:xxx Source IP address:xxx Cause:xxx
100B		Logged in to the OS console	Logged in to the OS console(xxx). Username:xxx Source IP address:xxx User authentication method:xxx
100C		Logged out from the OS console	Logged out from the OS console(xxx). Username:xxx Source IP address:xxx Cause:xxx
100D		Failed to login to the OS console	Failed to login to the OS console(xxx). Username:xxx Source IP address:xxx Cause:xxx
100E		Failed to start using the remote FD	Failed to start using the remote FD. Source IP address:xxx Cause:xxx
100F		Failed to start using the remote CD/DVD	Failed to start using the remote CD/DVD. Source IP address:xxx Cause:xxx
3001	Configuration Access	Initialized user accounts	Requested an initialization of the user accounts. Method:xxx
3002		Changed BMC IP address	Requested a change of BMC IP address. IP address after change:xxx Method:xxx
3003		Changed username	Requested a change of username xxx. Username after change:xxx Role:xxx Method:xxx
3004		Changed user account information	Requested a change of user account information for xxx. Item changed:xxx xxx Method:xxx
3005		Changed SSH server settings	Requested a change of SSH server settings. Authentication method:xxx Method:xxx
3006		Changed LDAP settings	Requested a change of LDAP settings. User authentication method:xxx Method:xxx
3007		Changed OS console(SSH) settings	Requested a change of OS console(SSH) settings. Service:xxx Method:xxx
3008		Changed Remote KVM settings	Requested a change of Remote KVM settings. Port number:xxx Method:xxx
3009		Created a self-signed certificate	Requested a creation of a self-signed certificate. Method:xxx
300A		Created a CSR	Requested a creation of a CSR. Method:xxx
300B		Imported a server certificate	Requested an import of a server certificate. Method:xxx
300C		Downloaded the server certificate	Requested a download of the server certificate. Method:xxx

ID	Operation event type	Event logged	Message
300D		Changed DNS client settings	Requested a change of DNS client settings. xxx:xxx Method:xxx
300E		Changed time synchronization method	Requested a change of time synchronization method. Method:xxx Method:xxx
300F		Changed localtime	Requested a change of localtime. Localtime:xxx Method:xxx
3010		Changed NTP settings	Requested a change of NTP settings. NTP server 1:xxx NTP server 2:xxx Method:xxx
3011		Changed timezone settings	Requested a change of timezone settings. Timezone:xxx Method:xxx
3012		Changed daylight savings time settings	Requested a change of daylight savings time settings. Daylight savings time:xxx Start:xxx End:xxx Method:xxx
3013		Changed reduction settings	Requested a change of reduction settings. Method:xxx
3014		Changed capacity on-demand settings	Requested a change of capacity on-demand settings. Method:xxx
3015		Changed EFI settings	Requested a change of EFI settings. Method:xxx
3016		Changed LP settings	Requested a change of LPAR manager settings. Method:xxx
3017		Changed language settings	Requested a change of language settings. Method:xxx
3018		Changed asset information	Requested a change of asset information. Method:xxx
3019		Changed mouse mode of remote console	Requested a change of mouse mode of remote console. Method:xxx
301A		Backed up server management settings	Requested a backup of server management settings. Method:xxx
301B		Restored server management settings	Requested a restore of server management settings. Method:xxx
301C		Backed up system settings	Requested a backup of system settings. Method:xxx
301D		Restored system settings	Requested a restore of system settings. Method:xxx
301E		Changed IP address restriction settings (Permitted IP Address 1-4)	Requested a change of IP address restriction settings. Item:xxx Before:xxx After xxx Method:xxx
301F		Downloaded operation logs	Requested a download of operation logs. Method:xxx
3020		Cleared operation logs	Requested a clear of operation logs. Method:xxx
3021		Downloaded logs corrected by BMC	Requested a download of logs corrected by BMC. Method:xxx
3022		Requested change in WSMAN service settings	Requested a change of WSMAN service settings. Service:xxx wsmans port number:xxx Method:xxx

ID	Operation event type	Event logged	Message
3023	Configuration Access	Requested change in user name for IPMI Over LAN	Requested a change of IPMI Over LAN username xxx. Username after change: xxx Status: xxx Privilege Level: xxx Method: xxx
3024		Requested change in user account information on IPMI Over LAN	Requested a change of IPMI Over LAN user account information for xxx. Item changed: xxx xxx xxx Method: xxx
3025		Requested changing Security strength to High	Requested a transition to Security strength High. Method:xxx
3026		Requested changing Security strength to Default	Requested a transition to Security strength Default. Method:xxx
3027		Requested changing OS console (Telnet) settings	Requested a change of OS console(Telnet) settings. Service:xxx Method: xxx
3028		Requested changing remote console service settings	Requested a change of Remote console service settings. Service:xxx SSL/TLS communication: xxx SSLv3: xxx TLSv1.0: xxx TLSv1.1: xxx TLSv1.2: xxx Method: xxx
3029		Requested changing remote CD/DVD connection port	Requested a change of Remote CD/DVD settings. Port number:xxx Method: xxx
302A		Requested changing remote FD connection port	Requested a change of Remote FD settings. Port number:xxx Method: xxx
302B		Requested changing Web console (HTTP) settings	Requested a change of Web console(HTTP) settings. Service:xxx Method: xxx
302C		Requested changing Web console (HTTPS) settings	Requested a change of Web console service settings. SSLv3:xxx TLSv1.0: xxx TLSv1.1: xxx TLSv1.2: xxx Method: xxx
302D		Requested changing IPMI over LAN service settings	Requested a change of IPMI over LAN service settings. Service:xxx IPMI over LAN v1.5: xxx Method: xxx
302E		Requested changing Cipher Suite Privilege Levels	Requested a change of Cipher Suite Privilege Levels. xxx Method: xxx
302F		Requested changing Syslog transfer	Requested a change of Syslog transfer settings. Syslog transfer:xxx Syslog Server: xxx Port Number: xxx Method: xxx
3030		Requested sending Syslog transfer test message	Requested a Send syslog transfer test message. Method:xxx
8001	Maintenance	Transition from maintenance mode to normal mode	Requested a transition from maintenance mode to normal mode. Method:xxx
8002		Transition from normal mode to maintenance mode	Requested a transition from normal mode to maintenance mode. Method:xxx

ID	Operation event type	Event logged	Message
8003		Requested an update of EFI firmware	Requested an update of EFI firmware. Method:xxx
8004		EFI firmware was updated	EFI firmware was updated. New EFI firmware:xxx Method:xxx
8005		Requested an update of BMC firmware	Requested an update of BMC firmware. Method:xxx
8006		BMC firmware was updated	BMC firmware was updated. New BMC firmware:xxx Method:xxx
8007		Requested an update of FPGA	Requested an update of FPGA. Method:xxx
8008		FPGA was updated	FPGA was updated. New FPGA:xxx Method:xxx
8009		Switched BMC firmware bank	Requested a switching of BMC firmware bank. Bank to be used:xxx Method:xxx
800A		Switched EFI firmware bank	Requested a switching of EFI firmware bank. Bank to be used:xxx Method:xxx
800B		Requested hardware memory dump	Requested a hardware memory dump. Method:xxx
800C		Canceled PCI Express deconfiguration	Requested a cancellation of PCI Express deconfiguration. Method:xxx



If download is blocked by the browser security protection function when you download a file from the system Web console such as ID: 3844 and 3917, the operation log is recorded. See “Client Settings”, System Web Console in Chapter 6 for client browser settings.

Syslog Transfer

This section describes the Syslog transfer function for management modules and BMC.

Overview

Compute Blade 2000 management modules and BMC can transfer events of user operation, hereinafter referred to as Audit event, to a syslog server. You can integrate and manage Audit events in management modules and BMC using the syslog server.



- Audit events at user operation with stopping a management module, such as shutdown, restart, and switching, may not be sent depending on the timing.
- When you shut down, restart, or switch a management module immediately after performing some operation, or when the management module fails immediately after your operation, the audit event may not be sent depending on the timing.
- Syslog transfer is performed in cleartext. Encrypted communication is not supported.
- Port number 514 is fixed for use in Syslog transfer. The port number cannot be changed.
- Only Audit events can be sent to the syslog server. Events as alert trigger for SC/BSM or HCSM are not sent to the syslog server.
- Audit events in a management module are sent to the syslog server from the management module. Audit events in BMC are sent to the syslog server from BMC. You need to configure settings for transfer to the syslog server in management modules and in BMC respectively.
- Syslog transfer for BMC is supported only by standard server blade: X55R3/X55S3/X55R4 models and high-performance server blade: X57 A2 model.

Audit events to transfer

Audit events are transferred when the events occur as operation logs. See Operation log for details.

Log format

The following format is used for logs transferred to the syslog server.

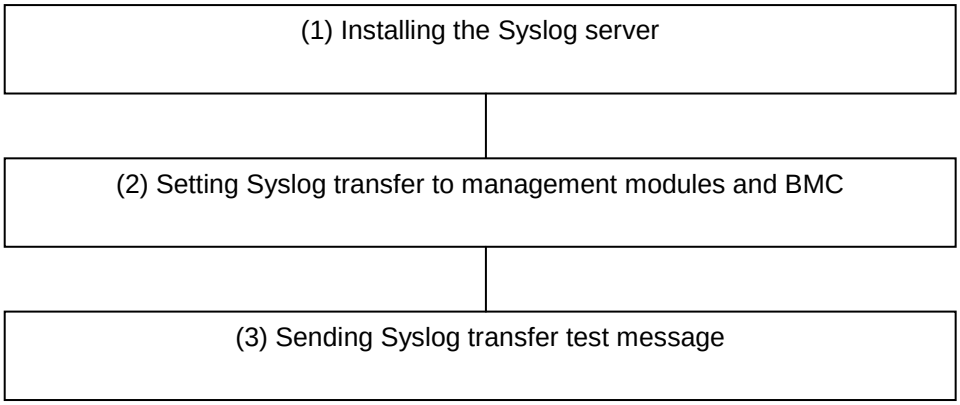
[date] [IP address for SVP or BMC] mm: auditevent,[log message]

An operation log is in [log message]. See Operation for the format and messages.

“user” is displayed as facility for logs transferred to the syslog server. For severity, “notice” is displayed as the result in the operation log when an operation fails, and “info” is displayed when the operation result is other than failure.

Using Syslog transfer

The following flowchart shows the procedure for using Syslog transfer.



1. Installing the Syslog server

   Install a syslog server to transfer Audit events.

2. Setting Syslog transfer to management modules and BMC

   Configure the following settings for the management module and BMC. For management modules, see “ST Command” in Chapter 6; for server blades (BMC), see “Syslog Transfer” in Chapter 5

- Enabling/disabling Syslog transfer

  Enable or disable Syslog transfer. To send Audit events with Syslog transfer, enable it.

- Sending or not sending Audit events (only for management modules)

  Enable or disable Syslog transfer whether or not to send Audit events. To send them using Syslog transfer, enable it.

- Syslog server for destination

  Set an IP address or host name for the syslog server for destination. Use FQDN to set the host name.



- The port number used for Syslog transfer cannot be changed.
- Only one syslog server can be specified as destination.

3. Sending Syslog transfer test message

   When you log into the management module system console or system Web console, “Logged in to the System Console.” or “Logged in to the System Web Console.” is sent. For BMC, “Requested a Send syslog transfer test message.” is sent when you log into the server blade Web console and send the Syslog transfer test message on the Syslog transfer screen. Check if the message is sent or not. When the message is sent, Syslog transfer setting is correct.

Notes on Windows

This section contains notes about operating Windows. See Compute Blade 2000 Software Guide for more information.

Memory dump in no system response

Memory dump is required to track down the cause of errors when the system does not respond and the task stops. Memory dump is a file where data of failure on the physical memory is saved on the hard disk and is used for tracking the status of the system with no response and applications.

Set the memory dump to be collected for finding the cause of the error, no system response. For Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 R2, set and check as follows.

❑ NMI dump registry

Set the registry key on the registry editor.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl

Name: NMICrashDump

Type: REG_DWORD

Value: 1

❑ Virtual memory (pagefile.sys)

Set the virtual memory following the steps below.



The procedure shown below is an example, and may not be available with some environments. See the following Website for further details.

http://support.microsoft.com/kb/969028/en-us

1. Click **Start**, right-click **Computer**, and click **Properties**.
2. Click **Advanced system settings**.
3. Click **Advanced** tab under the **System** page.
4. Click **Settings** under the **Performance** area.
5. Click the **Advanced** tab.
6. Click **Change** under **Virtual memory**.
7. Select a drive to set “pagefile.sys”, and check that the value of Initial size and Maximum size is the physical memory + 400 MB or over.
8. Click **OK** to close **System**, and restart Windows.

❑ Location space for the memory dump file

Check that the location space for the memory dump file, MEMORY.DMP, is the physical memory + 400 MB or over.

Tip

- See “Memory Dump Collection” in Chapter 14 for how to collect memory dump.
- This setting is not necessary for Windows Server 2012 or later.

Complete memory dump

Complete memory dump collects memory dump including user mode information. Thus, it can more probably find the cause in failure analysis than other memory dump files.

Complete memory dump, however, requires more space on the location where the memory dump file is stored depending on the physical memory installed. Complete memory dump is recommendable if enough space is secured for the file destination.

Complete memory dump requires the following setting as well as settings shown in Memory dump in no system response.

❑ Complete memory dump registry

Set the registry key on the registry editor.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl

Name: CrashDumpEnabled

Type: REG_DWORD

Value: 1

Note

The setting above is required only for Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003 R2.

❑ Procedure for complete memory dump

Follow the steps below to set Complete memory dump.

1. Click **Start**, right-click **Computer**, and click **Properties**.
2. Click **Advanced system settings**.
3. Click the **Advanced** tab under the **System** page.
4. Click **Settings** under the **Startup and Recovery**.
5. Select **Complete memory dump** under the **Writing debugging information** area.
6. Click **OK** to close **Startup and Recovery**.
7. Click **OK** to close **System Properties**, and restart Windows.

Useful settings for Red Hat Enterprise Linux

Using parameters to stop the system at hardware failure

❑ Potential problems and the solution

At hardware failure, Compute Blade issues an interrupt, which is called NMI (*1), to stop the system during the hardware recovery process. Red Hat Enterprise Linux, however, has a setting by default not to stop a system when NMI is issued. As a result, unexpected behavior may occur because the system keeps running at hardware failure.

A solution to this problem is to set parameters for Red Hat Enterprise Linux to stop the system when NMI is issued. This can prevent unexpected behavior at hardware failure. It is highly recommended that you should set these parameters.

In the environment with Linux Tough Dump, a highly reliable tool for collecting dumps, the setting stops the system when NMI is issued. Thus, you do not need to change the setting.

(*1) NMI (Non-Maskable Interrupt): hardware interruption that cannot be prevented by software.



Red Hat Enterprise Linux has some functions to utilize NMI, such as monitoring CPU hang ups, profiling kernel, and stopping a system instantly at receiving NMI, although some functions are not supported by some OS versions. You can use one of them as a dedicated function. When the instant stop at NMI is enabled, CPU watchdog and kernel profile are not available.

❑ System that requires the setting change

Systems that satisfy the following two conditions require the setting change.

1. Linux Tough Dump is not applied.
2. The following OS is used:

   Red Hat Enterprise Linux 5.3 (x86, AMD/Intel 64)

❑ How to change the settings

1. Change “/boot/grub/grub.conf”.

Set a kernel parameter “nmi_watchdog=0” .

Before the setting change

```
title Red Hat Enterprise Linux Server (2.6.18-128.el5)
      root (hd0,0)
      kernel /vmlinuz-2.6.18-128.el5 ro root=/dev/VolGroup00/LogVol00 nodmraid
      initrd /initrd-2.6.18-128.el5.img
```

After the setting change

```
title Red Hat Enterprise Linux Server (2.6.18-128.el5)
      root (hd0,0)
      kernel /vmlinuz-2.6.18-128.el5 ro root=/dev/VolGroup00/LogVol00 nodmraid
nmi_watchdog=0
     initrd /initrd-2.6.18-128.el5.img
```

2. Change “/etc/sysctl.conf” file.

Add the following parameter to the last line of the “/etc/sysctl.conf” file. When the parameter already has been set, change the value as shown below.

```
kernel.unknown_nmi_panic = 0
kernel.panic_on_unrecovered_nmi = 1
```

3. Reboot the OS.

Type the following command to reboot the OS.

```
# reboot
```

4. Check whether the new setting is reflected.

Execute the following command to check the parameter. (Italic characters show command results.)

```
# cat /proc/cmdline
ro root=/dev/VolGroup00/LogVol00 nodmraid nmi_watchdog=0
# sysctl -a | grep “unknown_nmi_panic =”
kernel.unknown_nmi_panic = 0
# sysctl -a | grep “panic_on_unrecovered_nmi =”
kernel.panic_on_unrecovered_nmi = 1
```

❑ How to deal with hardware failure

When hardware fails, the error LED on the system equipment turns on. Monitor the error LED, and consult our maintenance personnel when you find the error LED lights solid.

If the following message is displayed, hardware may fail. Check the error LED on the system equipment.

```
Kernel panic - not syncing: NMI: Not continuing
```

System time delay with Red Hat Enterprise Linux 5 (x86)

❑ Potential Problems and the Solution

Red Hat Enterprise Linux 5 (hereinafter referred to as RHEL5) may have the system time delay (*1), even if rarely, by a few hours per day in operation. The system continues to delay at the same rate from the boot to reboot. Even if you use the time adjustment with NTP, the system time delays because the adjustment cannot work properly.

Moreover, when this delay occurs, CPU clock frequencies that the OS recognizes are higher than the actual clock frequencies.

This may seriously affect your business by not starting processes and batch jobs at the scheduled time.

To avoid this problem, disable the item “Legacy USB Support“ in the BIOS setting if your system satisfies conditions described later in Conditions for Time Delay.

If this countermeasure cannot be applied, be sure to execute the procedures shown in “How to Deal With the Time Delay”. For how to apply the countermeasure and how to deal with the time delay, refer to each item described later.

(*1) This system time delay cannot be automatically corrected.

❑ Conditions for time delay

When the following conditions are all satisfied, the system time may delay at a specific timing.

1. OS is RHEL5 (x86).

   AMD/Intel 64 architecture is not the case.

2. Item “Legacy USB Support” is Enabled in the BIOS setting.
3. Not in the LPAR manager environment.

This phenomenon can occur in all models that support RHEL5 (x86).

For condition 2, check the item “Legacy USB Support” in the BIOS setup menu. For how to operate the BIOS setup menu, see Chapter 5 “Server Blade Setup”.

❑ How to avoid time delay

■ Preventive measure

Change settings of “Legacy USB Support” in the BIOS setup menu from Enabled to Disabled.

Route to target: Advanced > USB Configuration > Legacy USB Support

■ Notes on changing settings

Do not change other items in the BIOS setup.

See Chapter 5 “Server Blade Setup” for how to operate the BIOS setup menu. If you do not apply the preventive measure above, execute the procedures in How to deal with the time delay.

Disabled setting in the item “Legacy USB Support” has the following restrictions:

1. Booting from USB devices including USB CD-ROM and USB FD is not available.
2. Keyboard operation is not available in the GRUB menu at the OS boot.
3. Do not implement the process in the LPAR manager environment. If you do, LPAR manager cannot be booted.

The restrictions above are effective when the remote KVM function is used.

Thus, temporarily enable the Legacy USB Support in the BIOS setup when executing the tasks described in restrictions above.

Once the OS is booted, you can use USB devices including USB CD-ROM and USB FD regardless of the Legacy USB Support setting. Keyboard operation in the BIOS setup menu and Boot menu is available regardless of the setting.

❑ How to deal with the time delay

If you are not using the preventive measure, be sure to execute the procedure shown below every time and immediately after the system has booted.

The following is an example of how to check the frequency recognized by the OS at the boot when an actual CPU clock frequency is 3000 MHz (3.00 GHz).

1. Check the actual CPU clock frequency.

   Use /proc/cpuinfo to check the actual CPU clock frequency.

   # grep “model name”/proc/cpuinfo

   model name : Intel® Xeon® CPU E5450 @3.00 GHz

   …..

2. Check the CPU clock frequency

   Use /var/log/dmesg to check the CPU clock frequency.

   # grep “MHz processor”/var/log/dmesg

   Detected 3000.264 MHz processor. ← correctly recognized.

   # grep “MHz processor”/var/log/dmesg

   Detected 3122.376 MHz processor. ← incorrectly recognized (due to this problem).

With NTP, when delayed difference between frequencies is less than 0.05%, the difference will not cause the system time to delay. For example, when an actual clock frequency of CPU is 3000 MHz and the delayed difference is less than 3001.5 MHz, NTP adjusts the system time.

If the system time delay is troublesome without NTP, use NTP.

3. To correct the system time when clock frequencies are incorrectly recognized:

   The followings show the steps with and without NTP.

   With NTP to adjust time

   Reboot the system following the steps below:

   a. Stop running applications.
   b. Reboot the system.
   c. Check if the CPU clock frequencies are correctly recognized using step 2 described above after the reboot.
   d. Confirm that the system clock is correct.

   With NTP to adjust time, the system time is adjusted at the system reboot.

   Without NTP to adjust time

   Reboot the system following the steps below:

   a. Stop running applications.
   b. Adjust the time using the following command.

      Example: to set time to 15:00 7th August, 2009

      # date –s “08/07 15:00 2009”

   c. Reboot the system.
   d. Check if the CPU clock frequencies are correctly recognized using step 2 described above after the reboot.
   e. Confirm that the system clock is correct.

System problems by error in detecting frequency of APIC timer at OS boot

Frequency of the APIC timer may be detected incorrectly at OS boot, which may cause the following results.

- OS hangs up during the boot to fail to boot.
- Processing like nanosleep system calls pause execution for a short time, which lowers the application performance.
- Commands for collecting information, such as “sar” and vmstat”, which are used to measure loading on the system, output incorrect results.

These problems are caused by an error in detecting frequency of the kernel APCI timer at the OS boot.

When USB Legacy emulation interrupt occurs in frequency detection, the detection process is delayed. Thus, the frequency may be different from the actual value. However, since frequency detection is executed at OS boot, this phenomenon cannot occur during the system operation.

If your system satisfies the following conditions, apply measures to avoid this problem to be described later.

❑ Conditions for incorrect frequency detection

When the following conditions are all satisfied, this might occur at a specific timing.

1. OS is one of the following:
   - Red Hat Enterprise Linux 5.4 (x86, AMD/Intel64)
   - Red Hat Enterprise Linux 5.4 Advanced Platform (x86, AMD/Intel64)
   - Red Hat Enterprise Linux 5.3 (x86, AMD/Intel64)
   - Red Hat Enterprise Linux 5.3 Advanced Platform (x86, AMD/Intel64)
2. The kernel version is less than 2.6.18-164.2.1.el5.
3. Legacy USB Support is enabled in the system BIOS setting.
4. Not in the LPAR manager environment,

❑ Preventive measure

Change settings of “Legacy USB Support” in the BIOS setup menu from Enabled to Disabled.

```
Route to target: Advanced > USB Configuration > Legacy USB Support
```

This can be avoided occurring by disabling Legacy USB Support to prevent the interrupt of USB Legacy emulation when frequency is being detected.

When you have disabled Legacy USB Support, the following restrictions are applied.

❑ Restriction

When disabling Legacy USB Support, you cannot use USB devices until the USB driver is loaded from the GRUB menu during OS boot.

1. Booting from USB devices such as a USB CD-ROM and USB FDD is not available.

2. Operating the keyboard is not available in the GRUB menu during OS boot.

3. This preventive measure cannot be used in the LPAR manager environment. If used, LP manager can not boot.

Since functions of the remote console and remote KVM by the remote console option are recognized as USB devices, these restrictions apply to them.

If you use them, temporarily enable Legacy USB.

Once the OS boots up, you can use USB devices such as a USB CD-ROM and USB FDD regardless of Legacy USB Support settings. You can also use the keyboard in the setup menu and Boot menu.

❑ How to check frequencies

Compare the following values, which are output in “/proc/interrupts”, to check whether or not the APIC timer can detect correct frequency.

(1) Number of the global timer interrupts: total amount of each CPU

(2) Number of the local timer interrupts for CPU0

When frequencies of the APIC timer are detected correctly, values of (1) and (2) are almost the same. If detected incorrectly, values of (1) and (2) are extremely different.

How to check whether or not a detected frequency is correct is described by showing correct and incorrect examples:

If frequencies of the APIC timer are detected incorrectly, stop the system immediately and apply the preventive measure.

- Correctly detected

```
# grep -e CPU -e timer -e LOC /proc/interrupts

           CPU0       CPU1       CPU2       CPU3
  0:   52343376   52341770   52317862   52335150   IO-APIC-edge timer
LOC: 209325542 209325558 209318927 209318950
```

  - (1) 209338158 = 52343376 + 52341770 + 52317862 + 52335150
  - (2) 209325542

- Incorrectly detected

```
# grep -e CPU -e timer -e LOC /proc/interrupts

          CPU0       CPU1       CPU2       CPU3
  0: 22188646   22187456   22187286   22185276   IO-APIC-edge timer
LOC: 44361775   44366256   44361703   44366179
```

  - (1) 88748664 = 22188646 + 22187456 + 22187286 + 22185276
  - (2) 44361775

Hardware memory dump

Hardware Memory Dump is a system-embedded functionality to get memory dump. It is supported by X57A1, X55A1 (*) and X55A2 models of Compute Blade 2000 server blades.

(*) EFI version 03-xx/04-xx needs to be installed on the X55A1 model to use the Hardware Memory Dump.

If Hardware Memory Dump is enabled and properly configured, you can get memory dump even in case that memory dump operation by kdump, which is a dump functionality provided by the OS, fails.

We recommend that you configure Hardware Memory Dump in addition to the OS dump functionality so that you can get memory dump in more situations.

See "Hardware Memory Dump" in "Chapter 5: Server Blade Setup" for the instructions to use Hardware Memory Dump.

See the Red Hat, Inc. website for details of kdump.

Hot-plug module with PCIe error isolation mode enabled

❑ Applying a hot-plug module

When the PCIe error isolation mode is enabled with Linux, the OS will keep running if the device is isolated and not available at a PCIe failure. If the hot-plug module “acpiphp” has not been loaded then, the device remains on the OS, causing inconsistency between current states of the device and the OS.

Apply the hot-plug module to avoid the trouble described above.

❑ Target system requirements

The following requirements apply to a target system.

- The OS is one of those below:
  - Red Hat Enterprise Linux 5.4 (x86, AMD/Intel 64)
  - Red Hat Enterprise Linux 5.4 Advanced Platform (x86, AMD/Intel 64)
- PCIe Error Isolation is enabled in PCI Error Handling Mode.

❑ How to change settings

1 Create acpiphp.modules.

Perform the following command:

```
# vi /etc/sysconfig/modules/acpiphp.modules
```

The following shows the edited content.

```
#/bin/bash
/sbin/modprobe acpiphp
```

Save the edited content, and configure the privilege using the OS chmod command.

```
# chmod 755 /etc/sysconfig/modules/acpiphp.modules
```

Confirm that the OS privilege is set as shown below.

```
# ls -l /etc/sysconfig/modules/acpiphp.modules
-rwxr-xr-x 1 root root 35 mm dd hh:mm
/etc/sysconfig/modules/acpiphp.modules
```

2 Load the acpiphp module.

Perform acpiphp.modules created in Step 1.

```
# /etc/sysconfig/modules/acpiphp.modules
```

Check if the acpiphp module has been loaded. This step is required once when the acpiphp.modules are created. Next time, acpiphp will be automatically loaded at the OS boot.

```
# /sbin/lsmod | grep acpiphp
acpiphp 58713 0
```

TCP checksum offload

With TCP (Transmission Checksum Protocol) enabled, which checks TCP packets in a LAN controller, failure in the LAN controller may cause packet data to be destroyed.

Target device drivers:

- e1000 e driver
- igb driver

TCP checksum offload is set by specifying parameters of tx (in transmission) and rx (in reception) to the argument of the ethtool command. The following describes values of tx/rx parameters and the format.

values: off (disabled) or on (enabled)

Disable TCP checksum offload in both transmission and reception using the ethtool command. Add the ethtool command to `/sbin/ifup-pre-local` as shown below, and restart the OS. The settings will be automatically specified at the OS restart.

Example: When disabling two LAN controllers, add the following line to `/sbin/ifup-pre-local` assuming that Linux recognizes each of them as network devices eth0 and eth1.

```
if [ "${1}" == "ifcfg-eth0" ]; then
/sbin/ethtool -K eth0 rx off
/sbin/ethtool -K eth0 tx off
fi
if [ "${1}" == "ifcfg-eth1" ]; then
/sbin/ethtool -K eth1 rx off
/sbin/ethtool -K eth1 tx off
fi
```

If the `/sbin/ifup-pre-local` file does not exist, create a new one with the file privilege 755 and add the setting above. If the file exists, add the setting above to the file. Then restart the OS or restart the network device to enable the setting.

To enable TCP checksum offload, use the procedure by replacing values of tx/rx parameters “off” with “on”.

Additional setting for Kdump configuration with 1-TB main memory

You need to execute the following procedure for Kdump configuration with 1-TB main memory before getting Kdump. If not, getting Kdump may fail.

Target OS: Red Hat Enterprise Linux 5

1. You need to add a setting to the /etc/sysconfig/kdump file. Execute the following command to output kernel boot option for obtaining information.

   ```
   # cat /proc/cmdline
   ```

   Example for output:

   ```
   ro root=/dev/vgroot/ hashdist=1 mem= mem=1024G
   ```

2. Add the kernel boot option without `mem= mem=1024G` output in Step 1 to KDUMP_COMMANDLINE parameter to edit /etc/sysconfig/kdump,

   Example for edited KDUMP_COMMANDLINE parameter

   KDUMP_COMMANDLINE=”`ro root=/dev/vgroot/ hashdist=1`”

3. Restart the system for `/etc/sysconfig/kdump` to take effect.



- For the system with many I/O adapters, getting Kdump may fail even if this setting is added. If so, change memory size for Kdump kernel from 128 MB by default to 256 MB, 512 MB… and retry it.
- If the kernel boot option has been changed after a character string is added to KDUMP_COMMANDLINE, make sure to execute the procedure above.

CPU planned degradation with 4-blade SMP (X57A1/X57A2 models)



When a system is configured with 4-blade SMP using high-performance server blades and many I/O boards are installed in the system, using CPU planned degradation may cause an OS to fail to boot.

Useful settings for VMware

This section describes useful advice about using Vmware.

Using parameters to stop the system at hardware failure

At hardware failure, an interrupt called NMI (*1) is issued to the OS to stop the system during the hardware recovery process. If Vmware ESX/Vmware ESXi (*2) is used, however, the default settings do not stop a system when NMI is issued. As a result, unexpected behavior may occur because the system keeps running at hardware failure.

(*1) NMI (Non-Maskable Interrupt): hardware interruption that cannot be masked by software.

(*2) VMware version is displayed such as VMware ESX, VMware ESX Server, and VMware ESX Server 3i.

Vmware ESX 4.0/Vmware ESXi 4.0 or later versions are provided with parameters to stop the system when NMI is issued. Enable the setting by following the procedure below. This can prevent unexpected behavior at hardware failure. It is highly recommended that you should set these parameters.

Vmware ESX Server 3.5 is also provided with parameters. Enable the setting by following the procedure below. If the enabled parameter does not work, it is recommended that you should upgrade ESX 3.5 to ESX 4.0.

❑ Target OS

- VMware ESX Server 3.5 Update 4
- VMware ESX Server 4.0 (including Update 1)
- VMware ESXi Server 4.0 (including Update 1)

❑ Setting procedure

Procedures are different depending on a VMware version. Thus, configure the setting for your environment.

VMware ESX 4.0/VMware ESXi 4.0

Setting Procedure

1 Log in VMware ESX or vCenter Server as a user with root or Administrator.

2 In the inventory panel, select the host, and click the **Configuration** tab.

3 Under Software, click **Advanced Settings**.

4 In the left pane of the Advanced Settings box, click **VMkernel**.

5 In the right pane, find **VMkernel.Boot.nmiAction** and ensure that it is set to **2**.

6 Click **OK**.

7 Reboot the host.

Checking the result

Follow the procedure below to check if the setting is properly configured.

1 Log in VMware ESX or vCenter Server as a user with root or Administrator.

2 Click the **Configuration** tab and then **Advanced** in the Software group.

3 Click **VMkernel > Boot** from the category. In the Setting Values shown on the right, confirm that the value of **VMkernel.nmiAction is 2**, changed from 3, and click **OK**.

VMware ESX server 3.5

Follow the procedure described below to enable the parameter.



When you perform an operation that adds a heavy load to the CPU, the enabled parameter may not stop the system when NMI is issued.

Thus, it is highly recommended that you should upgrade ESX 3.5 to ESX 4.0.

Setting Procedure

1 Log in the service console as a user with root.

2 Add the following parameters to the last line of the “/etc/sysctl.conf” file**.**

```
kernel.unknown_nmi_panic=1
kernel.panic=1
```

3 Reboot WMware ESX.

❑ Checking the hardware failure

When hardware is in failure, the error LED of the system lights solid.

If ERROR LED lights solid, contact your reseller.

If the following message is displayed on the service console screen of VMware ESX, hardware can fail. Check if the error LED lights on the system.

- VMware ESX 4.0/VMwqare ESXi 4.0

```
NMI_Lint1IntAction+xxxx stack : xxxxxxxxxx
Lint1 interrupt on pcpu x <- (“x” stands for a alphanumerical character.)
```

- VMware ESX 3.5

```
Kernel panic : Attempted to kill the idle task !
```

PCI error handling mode

This section describes PCI Error Handling Mode supported by Compute Blade 2000.

The following three PCI error handling modes are supported by Compute Blade 2000. See Chapter 5: Server Blade Setup for the setting procedure.

Mode	Description
PCIe Error Isolation (Default)	EFI isolates PCI express unrecoverable errors, such as disconnection of a connection cable for the I/O slot expansion unit. Since features of the isolated PCI express due to failure cannot recover, the system can maintain features and keep operating by switching to a redundant path with NIC teaming or MPIO of FC-HBA. With some serious failures, however, notifying NMI prompts OS to reboot the same way as Legacy. When PCI express unrecoverable errors occur, the OS operation stops for about 500 minutes because EFI collects failure information. Take this OS down time at the failure into account when you design a system.
Legacy	PCI express error is not isolated by EFI. When unrecoverable PCI express failure occurs, notifying NMI prompts OS to reboot.
OS AER	OS executes Advanced Error Reporting (AER). You can set this mode only when using OS (*1) that supports AER.

(*1) No OS is available for this feature as of March 2010.



- When the EFI firmware versions "01-xx/02-xx" on standard server blade (X55A1 model), it works as Legacy mode without regard to the preset value of PCI Error Handling Mode.
- Other functions are supported with EFI firmware versions "03-xx/04-xx" or later.

PCI error handling mode available for OS/virtual environment

Which PCI error handling mode can be configured depends on the type of OS/virtual environment. Some OS/virtual environments, where multiple modes can be set, have optimal modes based on the hardware configuration. Thus configure modes for your environment.

OS/Virtual environment	EFI/BMC	Selectable Mode	Description
Microsoft® Windows Server®2008 Microsoft® Windows Server®2003 R2	-	Legacy	Supports only Legacy mode.
Microsoft® Windows Server®2008 R2	Standard server blades with EFI: 03-42/04-42 or earlier BMC: 03-77 or earlier High-performance server blades with EFI: 03-16/04-16 or earlier BMC: 04-32 or earlier	Legacy	Supports only Legacy mode.
	Standard server blades with EFI: 03-43/04-43 or later BMC : 03-78 or later High-performance server blades with EFI: 03-17/04-17 or later BMC: 04-33 or later	PCIe Error Isolation/Legacy	With Hyper-V, supports only Legacy mode. Without Hyper-V, supports PCIe Error Isolation and Legacy mode. When all I/O devices, including HBA and NIC, are configured with redundancy, PCIe Error Isolation mode is recommended. With other than that, make sure to select Legacy mode.
Red Hat Enterprise Linux5.3	-	Legacy	Supports only Legacy mode.
Red Hat Enterprise Linux5.4 Red Hat Enterprise Linux5.6	Standard server blades with EFI: 03-42/04-42 or earlier BMC: 03-77 or earlier High-performance server blades with EFI: 03-16/04-16 or earlier BMC: 04-32 or earlier	Legacy	Supports only Legacy mode.
Red Hat Enterprise Linux5.4 Red Hat Enterprise Linux5.6	Standard server blades with EFI: 03-43/04-43 or later BMC : 03-78 or later High-performance server blades with EFI: 03-17/04-17 or	PCIe Error Isolation/ Legacy	Supports only Legacy mode. Supports PCIe Error Isolation and Legacy mode. When all I/O devices, including HBA and NIC, are configured with redundancy, PCIe Error Isolation mode is recommended. With other than that, make sure to select

OS/Virtual environment	EFI/BMC	Selectable Mode	Description
	later BMC: 04-33 or later		Legacy mode.
VMware ESX	-	Legacy	Supports only Legacy mode.
LP	Standard server blades with EFI: 03-42/04-42 or earlier BMC: 03-77 or earlier High-performance server blades with EFI: 03-16/04-16 or earlier BMC: 04-32 or earlier	Legacy	Supports only Legacy mode.
	Standard server blades with EFI: 03-43/04-43 or later BMC : 03-78 or later High-performance server blades with EFI: 03-17/04-17 or later BMC: 04-33 or later	PCIe Error Isolation/ Legacy	Supports PCIe Error Isolation and Legacy mode. When all I/O devices, including HBA and NIC, are configured with redundancy, PCIe Error Isolation mode is recommended. With other than that, make sure to select Legacy mode.

❑ Restrictions on PCIe error isolation mode

Note the following restrictions on PCIe error isolation modes.

- Onboard NICs do not support the PCIe error isolation mode. Make sure to disable the PCIe error isolation setting of the onboard NIC when using the PCIe error isolation mode with a standard server blade with EFI 03-43/04-43 or later and BMC 03-78 or later; a high-performance server blade with EFI 03-17/04-17 or later and BMC 04-33 or later.
- See PCIe devices supporting error isolation mode for PCIe devices available for the PCIe error isolation mode.
- When using the PCIe error isolation mode with Red Hat Enterprise Linux, make sure to apply hot-plug modules. See Hot-plug module with PCIe error isolation mode enabled for details.
- When the PCIe error isolation mode is used with Red Hat Enterprise Linux, the following message may appear at a PCI Express failure, which is no problem.

  ixgbe: ethX: ixgbe_reset: Hardware Error: -15

  (Note: ethX is for a LAN device name such as eth0 and eth1.)

❑ Note on redundant system configuration

The PCIe error isolation mode avoids rebooting the system when certain failures occur in a PCI express. Then, with N+M cold standby or HA cluster software, switching between active and standby may not be performed. With redundant system configuration, set the PCI error handling mode to Legacy. When setting the PCI error handling mode to PCIE Error Isolation, confirm that redundancy is configured on each expansion board and expansion card, and then enable the PCIe error isolating setting for them.

Devices supporting PCIe error isolation mode

❑ PCIe devices supporting error isolation mode

Isolation-mode-capable device		Model code	OS/Virtual environment	
			Windows Server 2008 R2	RedHat Enterprise Linux 5.4/5.6
I/O adapter	1 Gbps Ethernet x2	GVX-CN2N1G1X1 GVX-CN2D1G1X1	✓	✓
	1 Gbps Ethernet x4	GVX-CN2N1G2X1 GVX-CN2D1G2X1	✓	✓
	10 Gbps Ethernet x2	GVX-CN2NXG2X1 GVX-CN2DXG2X1	✓	✓
	8 Gbps Fibre-channel x1, Hitachi	GVX-CC2N8G1X1 GVX-CC2D8G1X1	✓	✓
	8 Gbps Fibre-channel x2, Hitachi	GVX-CC2N8G2X1 GVX-CC2D8G2X1	✓	✓
	8 Gbps Fibre-channel x2, Emulex	GVX-CC2N8G3X1 GVX-CC2D8G3X1	✓	-
	4 Gbps Fibre-channel x2, Hitachi	GVX-CC2N4G1X1	-	-
Mezzanine card	1 Gbps Ethernet x4	GVX-CN2M1G1X1	✓	✓
	8 Gbps Fibre-channel x2, Hitachi	GVX-CC2M8G1X1	✓	✓
	8 Gbps Fibre-channel x4, Hitachi	GVX-CC2M8G2X1	✓	✓
	8 Gbps Fibre-channel x2, Emulex	GVX-CC2M8G3X1	✓	-

When using the PCIe error isolation mode with the system in which a not-capable-PCIe-error-isolation device is installed, disable the PCIe error isolation setting for **Mezzanine** for a mezzanine card; **PCIe Slot** for an I/O adapter referring to “EFI Setup” in Chapter 5.

❑ Software version supporting PCIe error isolation mode

When using the PCIe error isolation mode, make sure to use the following software versions.

- Windows Server 2008 R2

Item	Model name	Version
OS	hotfix	KB2511500
Driver	10 Gbps Ethernet, 1 Gbps Ethernet : Intel Pro(R) PROSet	15.8.1 or later
	8 Gbps Fibre-channel, Hitachi	4.2.6.790 or later
	8 Gbps Fibre-channel, Emulex	7.2.20.006 or later
Redundancy software *1	Hitachi Dynamic Link Manager	6.5.1-00 or later
Management software	ServerConductor/Blade Server Manager	08-90 or later
	ServerConductor/Agent	08-90 or later
	ServerConductor/Deployment Manager	08-90 or later

- Red Hat Enterprise Linux 5.4

Item	Model name	Version
OS	kernel	2.6.18-164.15.1 or later
Driver	10 Gbps Ethernet x2 (ixgbe)	2.0.75.7-h1 or later
	1 Gbps Ethernet (igb)	1.3.19.3-h8 or later
	8 Gbps Fibre-channel, Hitachi (hfcldd)	x86: 1.5.16.1218 or later x64: 4.5.16.1218 or later
Redundancy software *1	Hitachi Dynamic Link Manager	6.5.1-00 or later
Management software	ServerConductor/Blade Server Manager	08-90 or later
	ServerConductor/Agent	08-90 or later
	ServerConductor/Deployment Manager	08-90 or later

- Red Hat Enterprise Linux 5.6

Item	Model name	Version
Driver	10 Gbps Ethernet x2 (ixgbe)	3.2.9-h2-NAPI or later
	1 Gbps Ethernet (igb)	2.4.11-h4 or later
	8 Gbps Fibre-channel, Hitachi (hfcldd)	x86: 1.5.16.1218 or later x64: 4.5.16.1218 or later
Management software	ServerConductor/Blade Server Manager	08-90 or later
	ServerConductor/Agent	08-90 or later
	ServerConductor/Deployment Manager	08-90 or later

*1 Redundancy software equipped with an OS
Redundancy software equipped with an OS has the risk in reliability of the entire system. It includes longer time required for analyzing failures due to less traceability of failure information and for providing the update patch.When using the redundancy software, take the time required for figuring out the cause of the failure and for recovering with the update patches when configuring the system.

❑ How to check PCI express error isolation

1 Log into the management module system console.

2 Perform DL command to display system event logs for the target partition.

The following message "PCI Express Error Isolation Started." is displayed, the PCI Express error has been isolated.

```
2011-01-17 21:57:46 P0 Info 024A 02 0100 04 1530 07A80310 PCI Express
Error Isolation Started.
```

For using the DL command, see Chapter 6: Management Module Settings > System Console Command Reference > DL Command.

SMASH for server blades

This section describes SMASH (Systems Management Architecture for Server Hardware) supported by X57A2, X55R3, and X55S3 server blades.



- SMASH functions are supported with the following BMC firmware version.
  BMC: 05-50 or later, or 07-01 or later with a standard server blade, X55R3 or X55S3, or X55R4 model
  BMC: 06-01 or later with a high-performance server blade, X57A2 model

SMASH overview

Systems Management Architecture for Server Hardware (SMASH) is a standard management tool for server hardware provided by Distributed Management Task Force (DMTF). You can use SMASH to perform operations including powering on or off a server blade and refer to FRU information. X57A2, X55R3, X55S3, and X55R4 server blade models can use SMASH with SMASH- CLP (Command Line Protocol) and WS-MAN (Web Services Management). See the DMTF Web site shown below for details about SMASH and WS-MAN.

http://dmtf.org/

SMASH features

The following items are available for SMASH with Compute Blade 2000.

SMASH Operations

#	Operation
1	Shows server blade status.
2	Powers on the server blade.
3	Powers off the server blade.
4	Performs server blade hardware reset.
5	Shows processor status.
6	Shows memory status.
7	Shows power supply module status.
8	Shows fan module status.
9	Shows sensor information.
10	Shows FRU information.
11	Switches boot devices.
12	Shows account information.
13	Restarts BMC.

SMASH can perform many types of operations defined by CIM (Common Information Model) profiles. X57A2, X55R3, and X55S3, and X55R4 server blade models support CIM profiles shown in the table below. See DMTF Web site for details about CIM profiles.

http://dmtf.org/standards/profiles

CIPM profiles

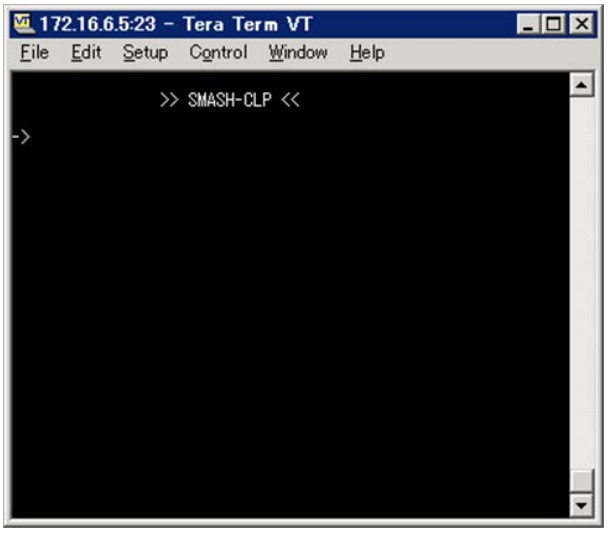
#	DSP	CIM profile	Organization	Version
1	DSP1004	Base Server	DMTF	1.0.0 or later
2	DSP1006	SMASH Collection	DMTF	1.0.0 or later
3	DSP1007	SM CLP Admin Domain	DMTF	1.0.0 or later
4	DSP1009	Sensors	DMTF	1.0.0 or later
5	DSP1011	Physical Asset	DMTF	1.0.0 or later
6	DSP1012	Boot Control	DMTF	1.0.0 or later
7	DSP1013	Fan	DMTF	1.0.0 or later
8	DSP1015	Power Supply	DMTF	1.0.0 or later
9	DSP1018	Service Processor	DMTF	1.0.0 or later
10	DSP1022	CPU	DMTF	1.0.0 or later
11	DSP1026	System Memory	DMTF	1.0.0 or later
12	DSP1033	Profile Registration	DMTF	1.0.0 or later
13	DSP1034	Simple Identity Management	DMTF	1.0.0 or later

Connection to SMASH-CLP

SMASH-CLP (Command Line Protocol) is available using terminal software on a console terminal connected via Telnet or SSH. Steps for connection are as follows.

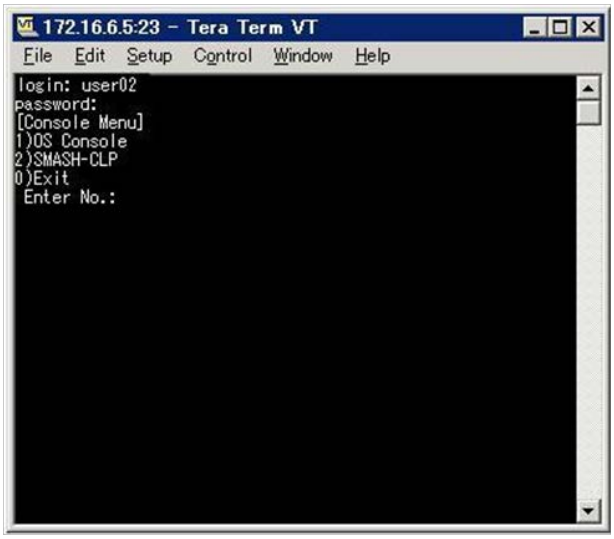
1 Start the terminal software on a console terminal, and connect to a server blade, on which you use SMASH-CLP, via Telnet or SSH. See Chapter 6 > LC Command > P: partition network setting for the server blade IP address.

2 Type a user name and password in connection via Telnet or SSH to connect to SMASH-CLP. See Chapter 5 > Initial Settings with Server Blade Web Console > User Account Configuration for how to set a user name and password.





- When using SMASH-CLP, check if there is SMASH-CLP role in the user account. If not, you are connected to the OS console. If your user account includes both roles: Remote Console and SMASH-CLP, the following screen is displayed for selection.
- See Chapter 5 > Initial Settings with Server Blade Web Console > User Account Configuration for details about roles. See Server Blade Operation for details about OS console.



❑ Using SMASH-CLP

With SMASH-CLP, you can operate “target” shown in a hierarchical structure using “verb”. Type the following string in the SMASH-CLP command line to operate an item shown in the table: SMASH Operations.

<verb> [<options>] [<target>] [<properties>]

See the table: verb available for options for verbs available for SMASH-CLP. See the table: targets for operations for targets corresponding to items shown in SMASH Operations. To view details for verb options, type the following.

```
help <verb>
```

To view target properties, move to a target layer to view its properties and type the following.

```
show -display properties
```

You can view verbs and properties for a target to operate using “show”.

verb available for options

verb	Options	Description
cd	-default, -examine, -help, -output, -version	Moves among layers.
show	-all, -default, -display, -examine, -help, -level, -output, -version	Shows properties and verbs for a target.
exit	-help, -output, -version	Finishes SMASH-CLP.
help	-examine, -help, -output, -version	Shows help for a target.
version	-examine, -help, -output, -version	Shows a version for a target.
set	-examine, -help, -output, -version	Sets properties for a target.
start	-examine, -force, -help, -output, -version	Requests the target to start.
stop	-examine, -force, -help, -output, -state, -version, -wait	Requests the target to stop.
reset	-examine, -help, -output, -version	Requests the target to reset.

targets for operations

target	Operation corresponding to the target
/admin1/system1	Shows server blade status. Powers on the server blade. Powers off the server blade. Performs server blade hardware reset.
/admin1/system1/cpu<N> /admin1/system1/capabilities1/cpucap<N> /admin1/hdwr1/mainchassis1/card<N>/chip<N>	Shows processor status.(*)
/admin1/system1/memory1 /admin1/hdwr1/mainchassis1/card<N>/pmem<N>	Shows memory status.
/admin1/system1/pwrsupply<N>	Shows power supply module status.
/admin1/system1/fan<N>	Shows fan module status.
/admin1/system1/sensors1/sensor<N> /admin1/system1/sensors1/currentsensor<N> /admin1/system1/sensors1/tachsensor<N> /admin1/system1/sensors1/tempsensor<N> /admin1/system1/sensors1/voltsensor<N>	Shows sensor information.
/admin1/hdwr1/mainchassis1	Shows FRU information.
/admin1/system1/settings1/bootcfgsetting1	Switches boot devices.
/admin1/system1/sp1/account<N>	Shows account information.
/admin1/system1/sp1	Restarts BMC.

Note*: This includes an item showing information at the last EFI boot.

An example of using SMASH-CLP is shown below.

To show the server blade status:

```
cd /admin1/system1
show
```

To power on the server blade:

```
start /admin1/system1
```

To power off the server blade:

```
stop /admin1/system1
```

To perform hardware reset on the server blade:

```
reset /admin1/system1
```

To switch to PXE boot:

```
cd /admin1/system1/settings1/bootcfgsetting1

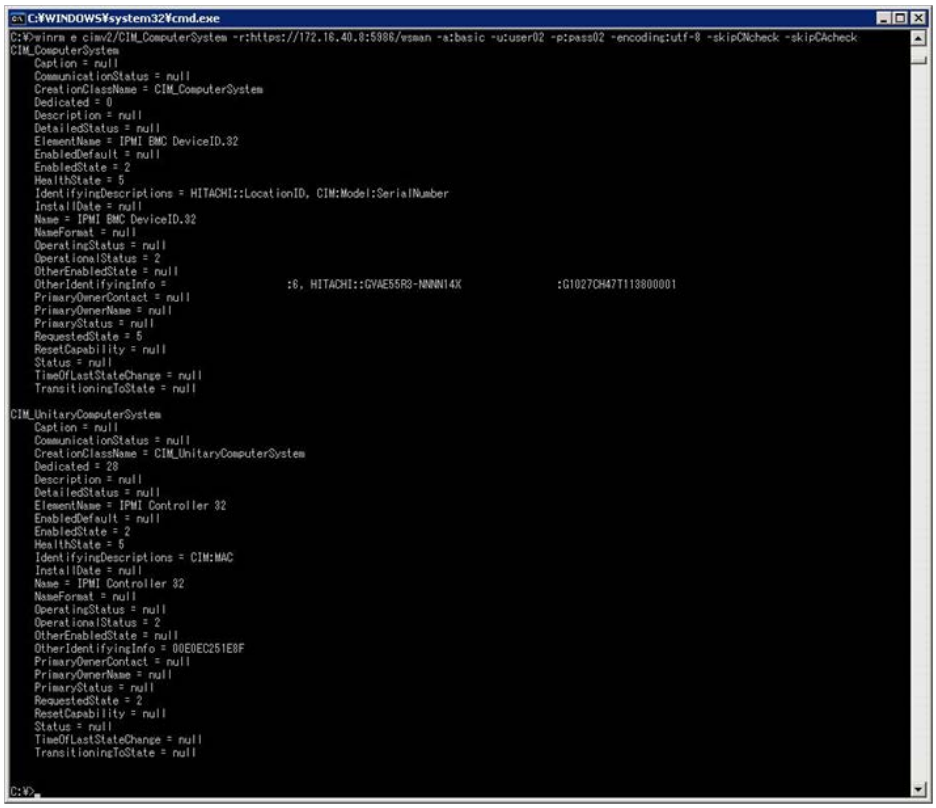
set bootorder=/admin1/system1/settings1/bootcfgsetting1/bootsrcsetting3
```



To cancel PXE boot, specify bootsrcsetting4 instead of bootsrcsetting3.

Connection to SMASH using WS-MAN

Windows Remote Management (WinRM), in which WS-MAN protocol has been implemented, is used for connection to SMASH. The following figure shows an example of connection to SMASH using WinRM.





- Use WinRM 2.0 or later. Behavior with WnRM 1.1 is not supported. You can download Windows management framework including WinRM 2.0 from Microsoft Web site.
- When using WinRM, make sure that WS-MAN service is enabled. See Chapter 5: Server Blade Setup > Server Settings Tab > Service Settings for details about WS-MAN service.
- When using WinRM, make sure that SMASH-CLP is included in the user account roles. See Chapter 5: Server Blade Setup > Initial Settings with Server Blade Web Console > User Account Configuration for details about WinRM.

❑ Using WinRM

To perform operations shown in the table OPERATION below, type the following command line at the command prompt on the console terminal with WinRM installed or in Windows PowerShell.

Winrm <OPERATION> <RESOURCE_URI> [-SWITCH:VALUE][@{KEY=VALUE}]

See tables, OPERATION, RESOURCE URI, and –SWITCH:VALUE, for operations available for WinRM. See Help in WinRM for details about WinRM.

OPERATION

OPERATION	Description
g(et)	Gets management information.
s(et)	Sets management information.
e(numerate)	Enumerates all instances of management resources.
i(nvoke)	Invokes a method to management resources.
id(entify)	Identifies if WS-MAN is executed on the server blade connected.

RESOURCE_URI

RESOURCE	Description
cimv2/CIM_ComputerSystem	Shows server blade status.
	Powers on the server blade.
	Powers off the server blade.
	Performs server blade hard reset.
cimv2/CIM_Processor	Shows processor status.(*)
cimv2/CIM_Chip	
cimv2/CIM_ProcessorCapabilities	
cimv2/CIM_Memory	Shows memory status.
cimv2/CIM_PhysicalMemory	
cimv2/CIM_PowerSupply	Shows power module status.
cimv2/CIM_Fan	Shows fan module status.
cimv2/CIM_Sensor	Shows Sensors.
cimv2/CIM_NumericSensor	
cimv2/CIM_Chassis	Shows FRU information.
cimv2/CIM_BootConfigSetting	Switches boot devices.
cimv2/CIM_Account	Shows account information.
cimv2/CIM_UnitaryComputerSystem	Restarts BMC.

Note*: This includes an item showing information at the last EFI boot.

–SWITCH:VALUE

–SWITCH	VALUE	Description
-r(emote)	[TRANSPORT]	Sets HTTPS to the URI scheme.
	HOST	Specifies a format: DNS name, NetBIOS name, or IP address.
	[PORT]	Uses a port number set for wsmans.(*)
	[PREFIX]	By default, wsman is set.
-u(sername)	USERNAME	Specifies the user name of a server blade connected.
-p(assword)	PASSWORD	Specifies the user password of a server bladed connected.
-a(uthentification)	VALUE	Authentication mechanism used for server connection - None - Basic - Digest - Negotiate
-encoding	VALUE	Specifies an encoding for communication with a server blade connected.
-file	VALUE	Specifies an XML file read from a file when s(et), c(reate), and i(nvoke) operations are executed.
-skipCAcheck	-	Specifies that the server certification does not need a signature of a trusted route certification authority. You need to use this option only with a trusted computer.
-skipCNcheck	-	Specifies that a common name for a server certification does not need to be the same name as the server host name. You need to use this option only with a trusted computer.

Note*: See Chapter 5: Server Blade Setup > Server Settings Tab > Service Settings for details about the port number (wsmasn).

An example of using WinRM is shown below.

To show the server blade status:

```
C:\>winrm e cimv2/CIM_ComputerSystem -
r:https://172.16.0.2:5986/wsman -a:basic -u:user02 -p:pass02 -
encoding:utf-8
```



When an error message indicating that the envelope is too large is displayed, type the following command to avoid trouble.

```
C:\>winrm s winrm/config @{MaxEnvelopeSizekb="4096"}
```

To power on the server blade:

```
C:\> winrm i RequestStateChange
"cimv2/CIM_ComputerSystem?CreationClassName=CIM_ComputerSystem+Name=
IPMI BMC DeviceID.32" @{RequestedState="2"} -
r:https://172.16.0.2:5986/wsman -a:basic -u:user02 -p:pass02 -
encoding:utf-8
```

To power off the server blade:

```
C:\> winrm i RequestStateChange
"cimv2/CIM_ComputerSystem?CreationClassName=CIM_ComputerSystem+Name=
IPMI BMC DeviceID.32" @{RequestedState="3"} -
r:https://172.16.0.2:5986/wsman -a:basic -u:user02 -p:pass02 -
encoding:utf-8
```

To perform hardware reset on the server blade:

```
C:\>winrm i ChangeBootOrder
cimv2/CIM_BootConfigSetting?InstanceID=BootConfigSetting1 -
r:https://172.16.0.2:5986/wsman -a:basic -u:user02 -p:pass02 -
encoding:utf-8 -file:input-ChangeBootOrder.xml1
```

To switch to PXE boot:

```
C:\>winrm i ChangeBootOrder
cimv2/CIM_BootConfigSetting?InstanceID=BootConfigSetting1 -
r:https://172.16.0.2:5986/wsman -a:basic -u:user02 -p:pass02 -
encoding:utf-8 -file:input-ChangeBootOrder.xml
```

See the following figure for ChangeBootOrder.xml specified with –file.

ChangeBootOrder.xml

```
<n1:ChangeBootOrder_INPUT
        xmlns:n1="http://schemas.dmtf.com/wbem/wscim/1/cim-
schema/2/CIM_BootConfigSetting"
        xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
        xmlns:wsman="http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd">
  <n1:source>
    <wsa:ReferenceParameters>
<wsman:ResourceURI>http://schemas.dmtf.com/wbem/wscim/1/cim-
schema/2/CIM_BootSourceSetting</wsman:ResourceURI>
        <wsman:SelectorSet>
          <wsman:Selector
Name="InstanceID">BootSourceSetting1</wsman:Selector>
        </wsman:SelectorSet>
      </wsa:ReferenceParameters>
  </n1:source>
</n1:ChangeBootOrder_INPUT>
```



To cancel PXE boot, change InstanceIDs to BootSourceSetting0 instead of BootSourceSetting1.

IPMI commands list

The following items are supported IPMI commands with Compute Blade 2000.



- This function is supported with the following BMC firmware version.
  BMC: 05-18 or later, or 07-01 or later with a standard server blade, X55R3, X55S3, and X55R4 model
  BMC: 04-72 or later, or 06-01 or later with a high-performance server blade, X57A1 and X57A2 model

Supported IPMI Commands

Command	NetFn	CMD	Remark
IPM Device "Global" Commands			
Get Device ID	App(06h,07h)	01h	
Get ACPI Power State	App(06h,07h)	07h	
BMC Watchdog Timer Commands			
Reset Watchdog Timer	App(06h,07h)	22h	
Set Watchdog Timer	App(06h,07h)	24h	
Get Watchdog Timer	App(06h,07h)	25h	
BMC Device and Messaging Commands			
Get System GUID	App(06h,07h)	37h	
Get Channel Authentication Capabilities	App(06h,07h)	38h	
Set Session Privilege Level	App(06h,07h)	3Bh	
Close Session	App(06h,07h)	3Ch	
Get Session Info	App(06h,07h)	3Dh	
Set Channel Access	App(06h,07h)	40h	
Get Channel Access	App(06h,07h)	41h	
Set User Access	App(06h,07h)	43h	
Get User Access	App(06h,07h)	44h	
Set User Name	App(06h,07h)	45h	
Get User Name	App(06h,07h)	46h	
Set User Password	App(06h,07h)	47h	
Activate Payload	App(06h,07h)	48h	
Deactivate Payload	App(06h,07h)	49h	
Get Payload Activation Status	App(06h,07h)	4Ah	
Get Payload Instance Info	App(06h,07h)	4Bh	
Set User Payload Access	App(06h,07h)	4Ch	
Get User Payload Access	App(06h,07h)	4Dh	
Get Channel Cipher Suites	App(06h,07h)	54h	
Chassis Device Commands			
Get Chassis Capabilities	Chassis(00h,01h)	00h	
Get Chassis Status	Chassis(00h,01h)	01h	

Command	NetFn	CMD	Remark
Chassis Control	Chassis(00h,01h)	02h	
Chassis Identify	Chassis(00h,01h)	04h	
Set System Boot Options	Chassis(00h,01h)	08h	*1
Get System Boot Options	Chassis(00h,01h)	09h	
Sensor Device Commands			
Get Sensor Threshold	Sensor/Event(04h,05h)	27h	
Get Sensor Reading	Sensor/Event(04h,05h)	2Dh	
FRU Device Commands			
Get FRU Inventory Area Info	Storage(0Ah,0Bh)	10h	
Read FRU Data	Storage(0Ah,0Bh)	11h	
SDR Device Commands			
Get SDR Repository Info	Storage(0Ah,0Bh)	20h	
Reserve SDR Repository	Storage(0Ah,0Bh)	22h	
Get SDR	Storage(0Ah,0Bh)	23h	
SEL Device Commands			
Get SEL Info	Storage(0Ah,0Bh)	40h	
Reserve SEL	Storage(0Ah,0Bh)	42h	
Get SEL Entry	Storage(0Ah,0Bh)	43h	
Clear SEL	Storage(0Ah,0Bh)	47h	
Get SEL Time	Storage(0Ah,0Bh)	48h	
Set SEL Time	Storage(0Ah,0Bh)	49h	
LAN Device Commands			
Set LAN Configuration Parameters	Transport(0Ch,0Dh)	01h	*2
Get LAN Configuration Parameters	Transport(0Ch,0Dh)	02h	
Serial/Modem Device Commands			
Set SOL Configuration Parameters	Transport(0Ch,0Dh)	21h	*3
Get SOL Configuration Parameters	Transport(0Ch,0Dh)	22h	
DCMI Command			
Get Asset Tag	DCGRP(2Ch,2Dh)	06h	
Set Asset Tag	DCGRP(2Ch,2Dh)	08h	

*1: Only Boot Device Selector is supported. Selectable Options are "No override" and "Force PXE".

*2: Configurable parameters are "IPv4 Header Parameters" and "RMCP+ Messaging Cipher Suite Privilege Levels".

*3: Configurable parameters are "SOL Enable", "SOL Authentication", "Character Accumulate Interval", "Character Send Threshold" and "SOL Retry".

Security of management interfaces

This section describes security functions of management interfaces.

Network communication by the system equipment

The system equipment has the following interfaces.

- Management module

Function	Protocol
System console	telnet
	ssh
System Web console	HTTP
	HTTPS
File transfer	ftp
	Sftp
SNMP*	SNMP (v1/v2c)
	SNMP (v3)
Email notification	SMTP
	SMTP (StartTLS)
LDAP	LDAPS
HCSM	HTTPS (command) and Hitachi original protocol (alert)
SC/BSM	Hitachi original protocol
Remote maintenance	Hitachi original protocol

*: For the function with System Center Operations Manager Management Pack (SCOM MP), SNMP is used.

- Server blade (BMC)

Function	Protocol for use
OS console	telnet
	ssh
Web	HTTP
	HTTPS
IPMI over LAN	IPMI v1.5
	IPMI v2.0
Remote console (Reclient for Windows)	Hitachi original protocol
Remote console (Java application)	Hitachi original protocol
LDAP	LDAPS
SMASH-CLP	telnet
	ssh
WS-MAN	HTTPS

Security strength

You can increase security strength on the management network for the system equipment. Security strength levels include Default and High. The system has shipped with the setting: Default.

The setting value: High increases the security strength on the management network for the system equipment.

- When encrypted data communication is available, you cannot send data in unencrypted form.
- For encrypted data communication, encryption algorithm with high security is used.

Relationship between security strength and functions

The following table describes the relationship between security strength levels and system functions.

- Management module

Function	Protocol	Security strength level	
		Default	High
System console	telnet	Available	Not available (*1)
	ssh	Available (SSHv2)	Available (SSHv2)
System Web console	HTTP	Available (*2)	Not available (*1)(*2)
	HTTPS	Available (SSL3.0, TLS1.0/1.1/1.2) (*2)(*4)	Available (TLS 1.2) (*2)(*4)
File transfer	ftp	Available	Not available (*1)
	sftp	Available (SSHv2)	Available (SSHv2)
SNMP	SNMP (v1/v2c)	Available	Not available (Not responds to the manager's request; not issues trap.)
	SNMP (v3)	Available	Available
Email notification	SMTP	Available	Not available (Not issues e-mail.)
	SMTP (StartTLS)	Available (SSL3.0, TLS1.0/1.1/1.2)	Available (TLS 1.2)
LDAP	LDAPS	Available (SSL3.0, TLS1.0/1.1/1.2)	Available (TLS 1.2)
HCSM	HTTPS and Hitachi original protocol	Available (SSL3.0, TLS1.0/1.1/1.2) (*5)	Available (TLS 1.2) (*5)
SC/BSM	Hitachi original protocol	Available (You can prevent communication by BSM command to close the port. See BSM command in Chapter 6 for details.)	Available (You can prevent communication by BSM command to close the port. See BSM command in Chapter 6 for details.)
Remote maintenance (*3)	Hitachi original protocol	Available	Available

(*1) The port used for the protocol is closed.
(*2) HTTP/HTPS are exclusively used.
(*3) Only maintenance personnel can use this function.
(*4) Your browser needs to support the SSL/TLS version.
(*5) Your application needs to support the SSL/TLS version.

■ Server blade (BMC)

Function	Protocol	Security strength level	
		Default	Default
OS console	telnet	Available	Not available (*1)
	ssh	Available (SSHv2)	Available (SSHv2) (*2)
Web	HTTP	Available	Not available (*1)
	HTTPS	Available (SSL3.0, TLS1.0/1.1/1.2)	Available (TLS 1.2) (*3)
IPMI over LAN	IPMI v1.5	Available	Not available (*4)
	IPMI v2.0	Available	Available (*5)
Remote console (Reclient for Windows)	Hitachi original protocol	Available (unencrypted form)	Not available
Remote console (Java application)	Hitachi original protocol	Available (unencrypted form/SSL3.0, TLS1.0/1.1/1.2)	Available (TLS 1.2) (*3)
LDAP	LDAPS	Available (SSL3.0, TLS1.0/1.1/1.2)	Available (TLS 1.2)
SMASH-CLP	telnet	Available	Not available (*1)
	ssh	Available (SSHv2)	Available (*2)
WS-MAN	HTTPS	Available (SSL3.0, TLS1.0/1.1/1.2)	Available (*3)

(*1) The port used for the protocol is closed.

(*2) For password authentication, use RSA: the first-described public-key cryptosystem for connection. Digital signature algorithm (DSA), host key algorithm cannot be used for authentication.

(*3) Certificate with less than 2048 bits cannot be used for connection. Change the value back to Default, register a certificate with 2048 bits or more, and then change security strength to High.

(*4) Connection is rejected at IPMI v1.5 LAN Session Startup.

(*5) Available only when CipherSuite ID is “3” and both UserName and Password are filled out.

User setting for security strength

You can configure the following settings using the management command console and server blade Web console. See SC Command in Chapter 6 and Initial Settings with Server Blade Web Console in Chapter 5.

Function	Device and function	
	Management module	Server blade
Change in security strength: Default or High	Command console of the management module (*1)(*2)	Command console of the management module (*1)(*3)(*5)
Specify supported versions of SSL/TLS	Command console of the management module (*4)	Server blade Web console (*4)

(*1) Security levels can be changed only when the following conditions are satisfied.
- All server blades have been initialized and powered off.
- All management modules have been initialized.

(*2) When a security level is changed, all management modules are restarted. When the primary management module has been initialized, the new value takes effect.

(*3) When a security level is changed, BMC for the server blade is restarted, and then the new value takes effect.

(*4) The setting is dynamically updated.

(*5) The setting can take effect only when the server blade BMC supports the security strength setting.

❑ Notes

- When security strength for a management module is changed, the management module is automatically restarted.
- When security strength for a server blade is changed, BMC is automatically restarted.
- Security strength for management modules and server blades is included in Backup and restore setting. See UBR Command in Chapter 6 for details.
- Security strength setting on a server blade is not included in the information taken over at N+M cold standby failover. When configuring N+M cold standby, configure the same security strength to the active and standby partitions.
- Function with SCOM MP is not available when a security level is High.

Functions depending on the security strength

■ SSL/TLS

Encryption suite	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	✓	-	-	-
SSL_RSA_WITH_RC4_128_MD5	-	-	-	-
SSL_RSA_WITH_RC4_128_SHA	✓	-	-	-
TLS_RSA_WITH_AES_128_CBC_SHA	✓	-	✓	✓
TLS_RSA_WITH_AES_256_CBC_SHA	-	-	✓	✓
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	✓	-	-	-
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	✓	-	-	-
SSL_RSA_WITH_3DES_EDE_CBC_SHA	✓	-	-	-
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	✓	-	-	-
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	✓	-	-	-
SSL_RSA_WITH_DES_CBC_SHA	-	-	-	-
SSL_DHE_RSA_WITH_DES_CBC_SHA	-	-	-	-
SSL_DHE_DSS_WITH_DES_CBC_SHA	-	-	-	-
SSL_RSA_EXPORT_WITH_RC4_40_MD5	-	-	-	-
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	-	-	-	-
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	-	-	-	-
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	-	-	-	-
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	✓	✓	-	-
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	-	-	-	-
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	✓	✓	-	-
TLS_RSA_WITH_AES_128_CBC_SHA256	✓	✓	✓	✓
TLS_RSA_WITH_AES_256_CBC_SHA256	-	-	✓	✓

Encryption suite	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	-	-	-	-
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	✓	✓	-	-
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	✓	✓	-	-
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	✓	-	-	-
TLS_RSA_WITH_3DES_EDE_CBC_SHA	-	-	✓	-
TLS_RSA_WITH_RC4_128_MD5	-	-	✓	-
TLS_RSA_WITH_RC4_128_SHA	-	-	✓	-
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	✓	-	-	-
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	✓	-	-	-
TLS_ECDHE_RSA_WITH_RC4_128_SHA	✓	-	-	-
TLS_ECDH_RSA_WITH_RC4_128_SHA	✓	-	-	-

Server certificate (Public key algorithm)	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
RSA1024 authentication	✓	-	✓	-
RSA1024 configuration	✓	✓	✓	-
RSA2048 authentication	✓	✓	✓	✓
RSA2048 configuration	✓	✓	✓	✓
RSA4096 authentication	-	-	-	-
RSA4096 configuration	-	-	-	-
DSA1024 authentication	✓	-	✓	-
DSA1024 configuration	✓	✓	✓	-

Server certificate (Signature algorithm)	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
SHA1 authentication	✓	✓	✓	✓
SHA1 configuration	✓	-	✓	-
SHA256 authentication	✓	✓	✓	✓
SHA256 configuration	-	✓	✓	✓

■ SSH

Host key algorithm		Management module		Server blade	
		Security strength		Security strength	
		Default	High	Default	High
Password authentication	RSA1024 authentication	-	-	-	-
	RSA1024 configuration	-	-	-	-
	RSA2048 authentication	✓	✓	✓	✓
	RSA2048 configuration	✓	✓	✓	✓
	RSA4096 authentication	-	-	-	-
	RSA4096 configuration	-	-	-	-
	DSA1024 authentication	-	-	✓	-
	DSA1024 configuration	-	-	✓	-
Public key algorithm	RSA1024 authentication	✓	✓	✓	✓
	RSA2048 authentication	-	-	-	-
	RSA2048 authentication	✓	✓	✓	✓
	RSA4096 authentication	-	-	-	-
	RSA4096 authentication	✓	✓	✓	✓
	DSA1024 authentication	-	-	-	-
	DSA1024 authentication	✓	✓	✓	✓
	RSA1024 authentication	-	-	-	-

Key exchange algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
diffie-hellman-group1-sha1	✓	✓	✓	✓
diffie-hellman-group14-sha1	✓	✓	✓	✓
diffie-hellman-group-exchange-sha1	✓	✓	✓	✓
diffie-hellman-group-exchange-sha256	✓	✓	✓	✓

Encryption algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
3des	-	-	-	-
3des-cbc	✓	✓	✓	✓
aes128-cbc	✓	✓	✓	✓
aes192-cbc	✓	✓	✓	✓
aes256-cbc	✓	✓	✓	✓
aes128-ctr	✓	✓	✓	✓
aes192-ctr	✓	✓	✓	✓
aes256-ctr	✓	✓	✓	✓
blowfish-cbc	✓	-	✓	-
cast128-cbc	✓	-	✓	-

Encryption algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
arcfour	✓	-	✓	-
arcfour128	✓	-	✓	-
arcfour256	✓	-	✓	-
rijndael-cbc@lysator.liu.se	✓	-	✓	-

Message authentication algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
hmac-md5	✓	-	✓	-
hmac-sha1	✓	✓	✓	✓
hmac-ripemd160	✓	-	✓	-
hmac-ripemd160@openssh.com	✓	-	✓	-
umac-64@openssh.com	✓	-	✓	-
hmac-sha1-96	✓	✓	✓	✓
hmac-md5-96	✓	-	✓	-
hmac-sha2-256	✓	✓	✓	✓
hmac-sha2-512	✓	✓	✓	✓

- SNMP v3

Encryption algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
None	✓	-	SNMP not supported	
DES	✓	-		
AES128	✓	✓		

Authentication algorithm	Management module		Server blade	
	Security strength		Security strength	
	Default	High	Default	High
None	✓	-	SNMP not supported	
MD5	✓	-		
SHA1	✓	✓		

14

When you need help

This chapter describes how to troubleshoot problems you may encounter while operating the system equipment.

Troubleshooting 1812
How to display the server blade screen 1818
Memory dump collection 1819
Error at server blade startup.....1825

Troubleshooting

The following summarizes problems that prevent the Compute Blade 2000 system and peripheral devices from working properly, and describes what action to take in each case. If the described action does not resolve the problem, contact your sales or service representative.

Server blade problems

The table below lists the problems that may cause a server blade to malfunction and describes what action to take.

No.	Location of Problem	Nature of Problem	Checklist and Action
1-1	Power supplies. LEDs, etc.	The power cannot be turned on. Nothing appears on the monitor. No LEDs are illuminated.	Are the power cables properly connected? Is the power light emitting diode (LED) on the Power Supply Module illuminated green? Is the server blade inserted all the way into the slot? Check the system status using the service processor (SVP) command "MC". If there is no improvement, contact your sales or service representative.
1-2	Screen display	The server blade powers up, but nothing appears on the monitor.	Is the monitor plugged in to the power outlet? Is the monitor’s power switch turned on? Is the cable securely connected? Does replacing the monitor fix the problem? If there is no improvement, contact your sales or service representative.
1-3	Screen display	The screen display is abnormal or garbled.	Is the monitor's brightness and contrast controls set correctly? Is the cable securely connected? Does replacing the monitor fix the problem? Is the correct video driver installed in the OS? Unlit pixels may occasionally be encountered when using a liquid crystal display (LCD) monitor, but this is not a fault. If there is no improvement, contact your sales or service representative.
1-4	Screen display	Images are distorted.	Are there any precision instruments in use anywhere near the Compute Blade 2000? Was the Compute Blade 2000 chassis or monitor moved while the system was in use? The earth's magnetic field may affect the images and colors shown on the monitor. Turn off the power, wait at least 30 minutes, and then try again. Are the Compute Blade 2000 chassis and monitor installed too close together? Separate the Compute Blade 2000 chassis and monitor, or increase the screen refresh rate. Does replacing the monitor fix the problem? If there is no improvement, contact your sales or service representative.

No.	Location of Problem	Nature of Problem	Checklist and Action
1-5	Screen display	The screen display is illegible or distorted.	Does the screen refresh rate exceed the monitor specifications? Does replacing the monitor fix the problem? If there is no improvement, contact your sales or service representative.
1-6	Screen display	A blue screen appears and nothing happens.	Try restarting. If restarting does not solve the problem, re-install the OS. If there is no improvement, contact your sales or service representative.
1-7	--	An error message appears when the BIOS starts.	See Error at server blade startup, and take corrective action.
1-8	Keyboard	Nothing can be entered from the keyboard.	Is the cable securely connected? Does removing and then re-connecting the cable make any difference? If the problem is unresolved, contact your sales or service representative.
1-9	Mouse	The mouse does not work properly.	Is the cable securely connected? Does removing and then re-connecting the cable make any difference? If the problem is unresolved, contact your sales or service representative.
1-10	Memory	The displayed memory is less than the actual installed memory.	Contact your sales or service representative.
1-11	Hard disk drive	The hard disk drive does not work properly.	Check the file system, referring to the manual for your operating system. If the problem is unresolved, contact your sales or service representative.
1-12	USB device (floppy disk drive)	The floppy disk drive does not work.	Make sure your OS supports USB-connected floppy disk drives. Is the cable connected correctly between the server blade and floppy disk drive? Does replacing the floppy disk drive make any difference? If the problem is unresolved, contact your sales or service representative.
1-13	USB device (DVD-ROM drive)	The DVD-ROM drive does not work.	Make sure your OS supports Universal Serial Bus (USB)-connected DVD-ROM drives. Is the cable connected correctly between the server blade and digital versatile disc (DVD)-Read Only Memory (ROM) drive? Does replacing the DVD-ROM drive make any difference? If the problem is unresolved, contact your sales or service representative.
1-14	--	The management software does not recognize the server blade.	Does restarting the management server make any difference? Does removing and re-inserting the Management Module resolve the problem? If there is no improvement, contact your sales or service representative.

No.	Location of Problem	Nature of Problem	Checklist and Action
1-15	--	An error message appears after the operating system has booted up.	Try to resolve the problem by referring to the manual for your operating system and the online Help.
1-16	--	The operating system hangs.	Restart the system.
1-17	--	The server blade emits an odor.	Contact your sales or service representative.
1-18	--	The server blade makes a strange noise.	Contact your sales or service representative.
1-19	Remote console application (Java application)	When you use JRE7 or JRE7u1 and try to start the remote console, the remote console does not start with a message shown like “Downloading the application”.	Solution 1: Update Java Runtime Environment (JRE) to 7u2 or later. Solution 2: Click “x” button instead of “Cancel” to close the message window like “Downloading the application” shown at remote console startup.
1-20	Remote console application (Java application)	When Internet Explorer 8 is used, the login window to remote console starts twice.	This may be caused by the problem related to Internet Explorer 8 shown in the following website. http://support.microsoft.com/kb/973082 SmartScreen filter: Deactivate SmartScreen filter.
1-21	-	The system does not respond.	The cause is not specified. Call maintenance personnel or consult your reseller. See Memory dump collection.

Fan module problems

The following summarizes problems that prevent the Fan Module from working properly and describes what action to take in each case.

No.	Location of Problem	Nature of Problem	Checklist and Action
2-1	Fan Module	The fan does not turn.	Is the Fan Module inserted correctly into the chassis? Is the system powered on? Is there any debris inside the system's Fan Module? If the problem is unresolved, contact your sales or service representative.
2-2	Fan Module	The management software does not recognize the Fan Module.	Is the Fan Module inserted correctly into the chassis? Restart the management server, remove and re-insert the Management Module, and then check again. If the problem is unresolved, contact your sales or service representative.
2-3	Fan Module	The fan makes a strange noise.	Is something touching the fan? If there is no apparent problem, contact your sales or service representative.
2-4	Fan Module	The fan emits an odor.	Contact your sales or service representative.
2-5	Fan Module	The LEDs on the Fan Module are not illuminated.	Is the Fan Module inserted correctly into the chassis? Is the system powered on? If the problem is unresolved, contact your sales or service representative.

Management module problems

The following summarizes problems that prevent the Management Module from working properly and describes what action to take in each case.

No.	Location of Problem	Nature of Problem	Checklist and Action
3-1	Power supply	The power cannot be switched on.	Are the power cables properly connected? Is the power LED on the Power Supply Module illuminated green? Is the Management Module inserted all the way into the chassis? If there is no improvement, contact your sales or service representative.
3-2	LED	The red error LED is illuminated.	Does removing the Management Module from the chassis and then re-inserting it make any difference? If there is no improvement, contact your sales or service representative.
3-3	--	The management software does not recognize the Management Module.	Does removing the Management Module from the chassis and then re-inserting it make any difference? If there is no improvement, contact your sales or service representative.
3-4	Serial port	The serial port is completely inoperative. The prompt does not appear when the terminal is connected to the Management Module via the serial port.	Is the serial cable connected to the connector? Are the communication parameters set appropriately in the communication software (9600 bps, 1 stop bit)? Are you using an RS-232C cross cable? Does removing the Management Module from the chassis and then re-inserting it make any difference? If the problem is unresolved, contact your sales or service representative.
3-5	Serial port	The display is garbled when the serial port is used.	Are the communication parameters set appropriately in the communication software (9600 bps, 1-stop bit)? Try removing and then re-inserting the Management Module, keeping the communication software's terminal window open. If the problem is unresolved, contact your sales or service representative.
3-6	--	Unable to connect to the Management Module via Telnet.	Is the Management Module's IP address correct? Is there a response when you ping the Management Module's IP address? If a router is present, are the router settings correct? Does it make any difference when the Telnet terminal is connected directly to the Management Module and not through a network device? If the problem is unresolved, contact your sales or service representative.
3-7	--	The Management Module makes a strange noise.	Contact your sales or service representative.

No.	Location of Problem	Nature of Problem	Checklist and Action
3-8	--	The Management Module emits an odor.	Contact your sales or service representative.

Power supply module problems

The following summarizes problems that prevent the Power Supply Modules from working properly and describes what action to take in each case.

No.	Location of Problem	Nature of Problem	Checklist and Action
4-1	LED	The green power LED is not illuminated when the power is on.	Is the power cable connected? Is power being supplied to the AC input terminal? If there is no apparent problem, contact your sales or service representative.
4-2	--	The Power Supply Module emits an odor.	Contact your sales or service representative.
4-3	--	The Power Supply Module makes a strange noise.	Contact your sales or service representative.

How to display the server blade screen

This section describes how to display the screen of a server blade.

To view the screen, display it remotely.

To remotely display the screen

You can remotely display the server blade system’s screen with a PC or server and not the server blades.

For the procedures, see ”Connect the Remote Console” in Chapter 3.

Memory dump collection

This section describes how to collect memory dump.



Memory dump is required to track down the cause of the error when the system does not respond and the task stops. You need to set the memory dump to be collected before operating the system.

Memory dump for Windows

This subsection describes how to collect memory dump for Windows.



See “Memory Dump in No System Response” and “Complete Memory Dump” in Chapter 13 for memory dump settings.

❑ Triggering memory dump

When the blue screen appears in STOP error, memory dump is automatically collected. When the system hangs up, issuing non-maskable interrupt (NMI) allows the memory dump to be collected.

To issue NMI, select **NMI** from **Power and Reset** menu of Remote console application, or click **Server Operation tab > Power and LEDs** and click **NMI**. See “Connect the Remote Console” in Chapter 3, or Chapter 5, Server Blade Setup for details.

❑ Collecting memory dump

The following screen is displayed during memory dump collection.

- Example of Windows Server 2008 R2 or lower



Memory dump is completed when “100% completed” is displayed on the Windows Server 2012 screen, and when the number on the bottom shows 100 on the screen of Windows Server 2008 R2 or lower.

Note

Do not issue NMI before memory dump is 100% completed.
If you do, the system may not respond.

If the system does not restart after the memory dump is 100% completed, restart the system manually.

❑ After collecting memory dump

The collected memory dump is copied to the specified location after the system re-startup. The default location is “%SystemRoot%¥MEMORY.DMP”. Then, the following event log is output after the memory dump file is copied.

Event ID: 1001

Source: Save Dump for Windows Server 2003 R2

BugCheck for Windows Server 2008 or higher

When you check the memory dump file on MS Explorer, the file is being output if the file size grows every second by updating. If so, wait until the event log above is displayed in the system event log.

If the memory dump file does not exist in the default location after memory dump is collected, the location may be changed from the default. Check the registry using the following items.
Key:
HKEY_LOCAL_MACHINE¥System\CurrentControlSet\ Control\CrashControl
Name: DumpFile

Memory dump for Linux

This subsection describes how to collect memory dump with kdump of Red Hat Enterprise Linux (RHEL) 6/RHEL 5.

See Using Parameters to Stop the System at Hardware Failure, Useful Settings for Red Hat Enterprise Linux in Chapter 13 for memory dump settings.

❑ Triggering memory dump

For an OS failure such as kernel panic, memory dump is automatically collected. When the system hangs up, issuing NMI allows the memory dump to be collected.

To issue NMI, select **NMI** from **Power and Reset** menu of Remote console application, or click **Server Operation tab > Power and LEDs** and click **NMI** button. See Connect the Remote Console in Chapter 3, or Server Blade Setup in Chapter 5 for details.

❑ Collecting memory dump

The following screen is displayed during memory dump collection.

Example of RHEL 6

```
Built 1 zonelists in Zone order, mobility grouping on. Total pages: 32447
Kernel command line: cgroup_disable=memory console=ttyS1,115200 mce=0
nmi_watchdog=0
no_timer_check nr_cpus=1 pcie_aspm=off reset_devices
….
Creating Block Devices
kjournald starting. Commit interval 5 seconds
EXT3-fs (sdb2): using internal journal
EXT3-fs (sdb2): mounted filesystem with ordered data mode
Checking for memory holes :
[ 0 %]
```

The memory dump is completed when **100%** is displayed at the bottom.

If the system does not restart after the memory dump is 100% completed, restart the system manually.

❑ After collecting memory dump

Check that the memory dump is collected after the system re-starts. The default registry for memory dump is “/var/crash/<date-time>/”. <date-time> is when the memory dump is collected.

If the memory dump file does not exist in the default location after memory dump is collected, the location may be changed from the default. Check the location written on the setting file.
Setting file name: /etc/kdump.conf

Memory dump for VMware

This subsection describes how to collect memory dump for Linux.

See “Using Parameters to Stop the System at Hardware Failure” and “Useful Settings for VMware” in Chapter 13 for memory dump settings.

❑ Triggering memory dump

When the local console displays a purple screen, memory dump is automatically collected. When the system hangs up, issuing NMI allows the memory dump to be collected. Follow the steps below to issue NMI.

1 Register the console screen.

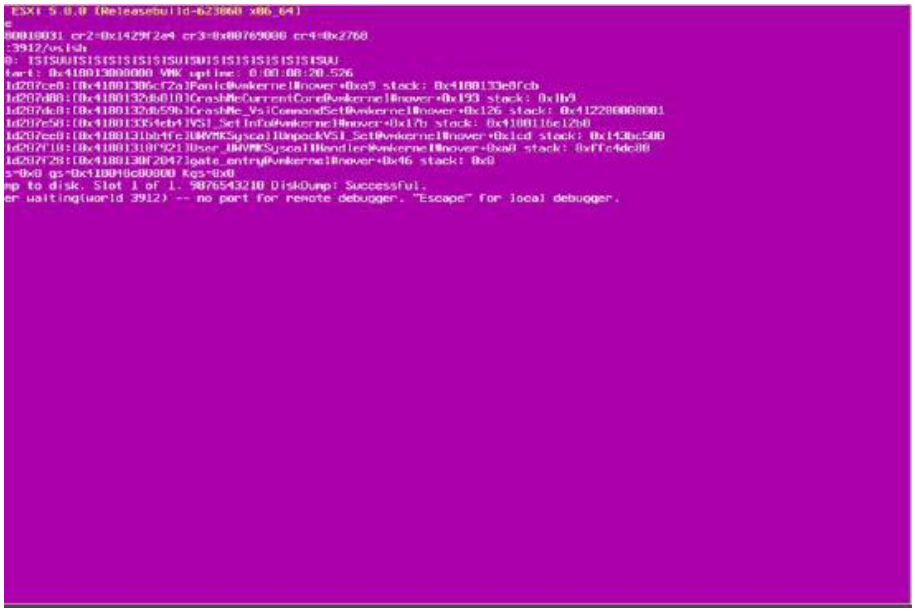
2 Check if the virtual machine is running via the network from another machine. If the virtual machine is running, shut it down.

3 Issue NMI.

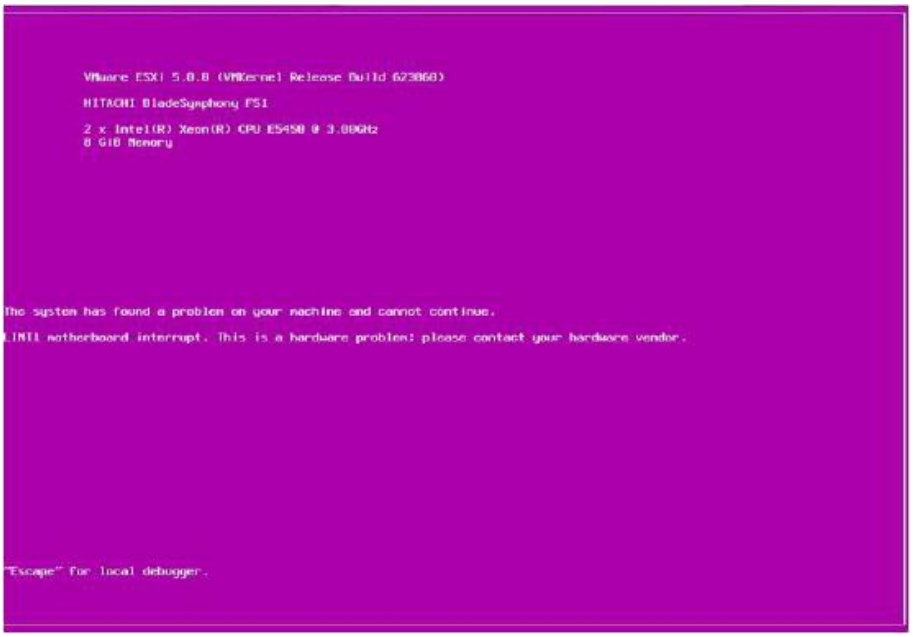
To issue NMI, select **NMI** from the **Power and Reset** menu of Remote console application, or click **Server Operation tab > Power and LEDs**, and click **NMI**. See “Connect the Remote Console” in Chapter 3 or Chapter 5, Server Blade Setup for details.

The following screen is displayed during memory dump collection.

- Purple screen



- When NMI is issued



Memory dump is completed when **"Escape" for local debugger** is displayed.

❑ After collecting memory dump

Follow the steps below to restart VMware from the purple screen.

1 Press the **Esc** key.

2 Type `reboot` with vmkernel debugger, and press **Enter**.

When the system restarts, check that the memory dump is collected. The default location for the memory dump is “/var/core/vmkernel-zdump.X”. “X” is any number.



Multiple “/var/core/vmkernel-zdump.X” files may exist. Check the date for the file using the Is command. If a file has the time that is the same as the system re-startup, the file is the dump file output this time.
When starting the virtual machine after the system startup, proceed as usual. If not restarting the virtual machine, select the maintenance mode.

Error at server blade startup

This section describes what action to take for errors that occur when the server blade boots up.

When error messages appear

When an error is detected during initial diagnosis, an error message appears in the monitor displaying the server blade's screen. When an error message appears, take appropriate steps to solve problems according to the "Cause and Action" listed below. If the problem persists, or you encounter an error message that is not listed below, write it down and consult your reseller or maintenance personnel.

No.	Error message displayed on the screen	Description	Cause and Action
1	Complementary metal–oxide–semiconductor (CMOS) battery failed	Button battery voltage has dropped.	Consult your reseller or maintenance personnel.
2	CMOS Checksum error - Defaults loaded	Button battery voltage has dropped.	Consult your reseller or maintenance personnel.
3	Central processing unit (CPU) Failure	CPU has failed.	Consult your reseller or maintenance personnel.
4	Hard disk Diagnosis fail	Hard disk has failed.	Third-party memory and/or hard disk are not covered by Hitachi's warranty. Confirm that the device supplied by Hitachi is properly connected. If a failure persists, consult your reseller or maintenance personnel.
5	Hard disk fail	Hard disk has failed.	
6	Hard Disk Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T.) Status bad	Hard disk has failed.	
7	Memory Test Fail	Memory has failed.	
8	Error Check and Correct (ECC) Correctable Error Alert	Error was automatically corrected in memory.	This is not a failure.

15

Maintenance and replacement parts

This chapter provides information about how to care for devices routinely, service life limited parts that require replacement and consumables.

Items requiring routine maintenance 1828
Cleaning 1829
Service life limited parts 1831
Notes on maintenance 1832

Items requiring routine maintenance

The system equipment and its built-in devices require routine maintenance. The following table describes the routine maintenance. If abnormal conditions are observed during routine maintenance, consult your dealer or call maintenance personnel.

Item	Description		Cleaned or inspected every:
System equipment	Cleaning	1. Remove dust from vent holes.	6 months (*1)
	Checkout	1. Check fan noise (including system fan modules and power supply modules).	6 months

*1 If the equipment is used in a dusty environment, clean it once a month.

Cleaning

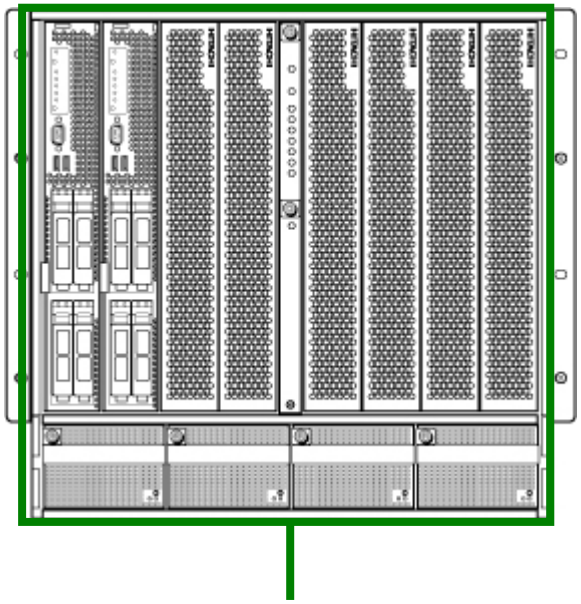
System equipment

Clean the vent holes every six month. If the equipment is used in a dusty environment, clean it once a month.

> **⚠ WARNING**
>
> Turn off the power and pull out the power cable before cleaning the system equipment. If not, the cleaning could cause an electric shock or equipment failure.

❑ How to clean the ventilation holes

Wipe the ventilation holes as shown in the following figure by using a dry cloth, or vacuum them with the system turned off.



To be cleaned.

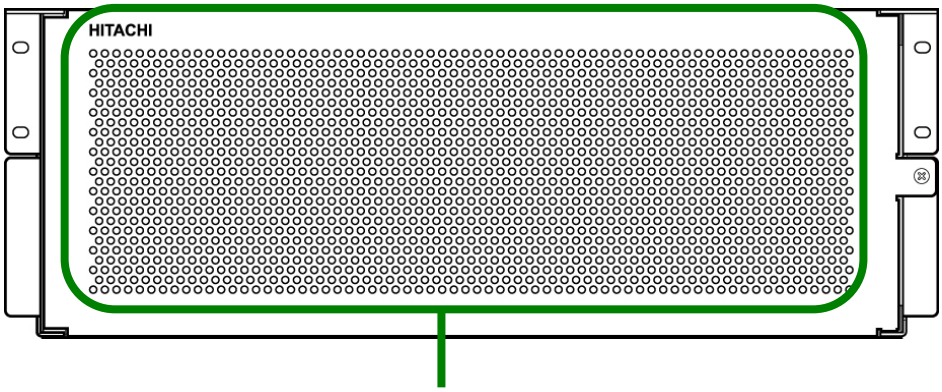
I/O slot expansion unit

Clean the vent holes every six month. If the unit is used in a dusty environment, clean it once a month.

> **⚠ WARNING**
>
> Turn off the power and pull out the power cable before cleaning the I/O slot expansion unit. If the power is not turned off and the power cable is not pulled out, the cleaning could cause an electric shock or equipment failure.

❑ How to clean the ventilation holes

Wipe the ventilation holes as shown in the following figure using a dry cloth, or vacuum them with the I/O slot expansion unit powered off.



To be cleaned.

Service life limited parts

The following parts have respective product life and their performance will be degraded or worn out while in use. Replace them periodically with new parts. For prices and delivery time, consult your reseller.



For details on the options not covered here, see the manuals supplied with those options.

Component	Applicable product model	Note
Hard disk	GVX-UH21471X1/ equipped with the standard server blade	(*1)
	GVX-UH21474X1 equipped with the standard server blade	
	GVX-UH23001X1 equipped with the standard server blade	

*1 The designed service life is about two years if you use the component that is energized for 24 hours a day and 30 days a month under the installation environment defined in "Installation Environment"(Page.2). Should you use the component beyond the above environmental conditions, the system may fail or suffer deteriorated service life.



No life time is set to hard disks described in the table below. Maintenance service is available for five years from the purchase date.

Component	Applicable product model	Note
Hard disk	GVX-UH26001X1/GV-UH26001X1-Y equipped with the standard server blade	-
	GVX-UH21473X1/GV-UH21473X1-Y equipped with the standard server blade	
	GV-UH21471X1-Y equipped with the standard server blade	
	GV-UH23001X1-Y equipped with the standard server blade	
	GVX-UH21475X1/GV-UH21475X1-Y equipped with the standard server blade	
	GVX-UH23003X1/GV-UH23003X1-Y equipped with the standard server blade	
	GVX-UH26002X1/GV-UH26002X1-Y equipped with the standard server blade	
	GVX-UH29001X1/GV-UH29001X1-Y equipped with the standard server blade	
	GVX-UH24001X1/GV-UH24001X1-Y equipped with the standard server blade	
SSD *1 *2 *3 1	GVX-UH22001X1/GV-UH22001X1-Y equipped with the standard server blade	-

*1 Solid state drive (SSD) has features including excellent random access performance, shock resistance, and low power consumption, but restrictions on writing amount. Typical amount written in a server is expected to be around 50 GB/day. In the environment with frequent writing, the amount may reach the upper limit.

*2 If you leave a dead SSD for a long time, the data on the SSD disappears. When SSD's days are numbered, it sends a S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) error. Monitor errors in SSD using the Redundant Arrays of Independent Disks (RAID) management utility. When a S.M.A.R.T. error is detected, replace the SSD

for safety. Proactive replacement is offered on a chargeable basis. Consult your reseller or maintenance personnel.

*3 Optimizing SSDs with a defragmenting program may shorten its useful life, which is different from hard disk drives (HDDs). Do not perform a defragmenting program when using SSDs.

Notes on maintenance

When parts replacement is required in maintenance due to some system failure, usually the latest versions of parts and basic input/output system (BIOS)/extensible firmware interface (EFI) firmware are applied to replacement. BIOS firmware not for target parts may be updated to the latest version as necessary. Note that firmware versions may be different from those before maintenance.

Appendix

Specifications

This appendix contains:

Specifications of system equipment 2
Interface specifications 22
Software license 25

Specifications of system equipment

❑ System specifications

Model name		Compute Blade 2000
Number of units that can be installed	Server blade	Up to 8 units *1
	I/O board module (PCI Express Board)	Up to 16 units
	Switch module	Up to 6 units
	Management module	Up to 2 units
	Power supply module	One unit under the standard configuration Max: up to 4 units
	Fan module	8 units in redundant configuration
	AC power input module	2 units
Outside dimensions (W x D x H: mm)/number of units according to the Electronic Industries Alliance (EIA), standard		447 x 820 x 441 mm/10U
Mass (Maximum)		180 kg
Power source	Input voltage (Frequency)	AC200 V ~ 240 V single phase (50/60 Hz)
	Rated power *2	8 kW
Environmental requirement	Temperature in Celsius	5°C to 35°C
	Humidity in percent (There must be no condensation.)	20% to 80%
EMC standard		FCC, ICES, EN55022, EN55024, EN61000, KC KN24, KC KN22, C-Tick, GOST, BSMI, CCC
Noise		64 dB *3
Rated wind		17.2 m^3/min: 607 CFM *4

*1 The number of server blade may be limited in the redundancy configuration with 1+1 power supplies.

*2 This is the rated value of a server chassis. The actual power consumption changes depending on configuration of blades and modules.

*3 This equipment controls RPM of a fan based on inlet air temperatures and internal temperatures. This value may be exceeded when the inlet air is 25°C or higher; CPU is under heavy load; or one of the fans fails.

*4 This equipment controls RPM of a fan based on inlet air temperatures and internal temperatures. This value may be exceeded when the inlet air is 35°C or higher, or one of the fans fails.

❑ Standard server blade specifications (1/6)

Model name		X55A1		
CPU	Supported CPU	Intel® Xeon® processor E5502	Intel® Xeon® processor E5540	Intel® Xeon® processor X5570
	CPU frequency	1.86 GHz	2.53 GHz	2.93 GHz
	Number of CPUs	Max: 2 (Max: 4 cores)	Max: 2 (Max: 8 cores)	
	3rd Cache memory	4 MB (shared by 2 cores)	8 MB (shred by 4 cores)	
QPI (Quick path interconnect) frequency		4.8 GT/s	5.86 GT/s	6.4 GT/s
Main memory		DDR3 Registered ECC DIMM 2GB/4GB/8GB		
	Memory size	Max: 144GB (8 GB x 18)		
Built-in HDD	Number of HDDs that can be installed	2.5 type x 4 (maximum)		
	Size	Max: 1200 GB (in RAID 0 configuration)		
	Feature	Supports RAID 0, 1, 5, 6, 10; Hotplug; Hotspare*4		
Number of mezzanine slots		2		
Network interface		GB Ethernet x 2 ports		
Management interface		Server blade Web console Remote console OS console (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet)		
Front interface		USB 2.0 x 2; Serial port (COM2) x 1 *5		
Outside dimension (W x D x H: mm)		47.7 x 547 x 336 (except backplane connector)		
Mass		8.36 kg		
Power consumption (Maximum) *1		357 W	480 W	486 W
Power consumption in operation*2		257 W	358 W	382 W
Indications based on the Energy Saving Law	Classification	b	Not targeted	
	Energy consumption efficiency *3	0.00525	Not targeted	
Supported OS		Microsoft® Windows Server 2008 R2 Microsoft® Windows Server 2008 Microsoft® Windows Server 2003 R2 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6		

*1 Maximum power consumption for the equipment design.

*2 General power consumption in operation

*3 The Energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*4 RAID 6 is supported only with GV-CA2SRD2X1-Y.

*5 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ Standard server blade specifications (2/6)

Model name		X55A2
CPU	Supported CPU	Intel Nehalem-EP Processor E5503
	Operating frequency of processors	2.0 GHz
	Number of processors	Max:2 (Max: 4 cores)
	3rd Cache memory	4 MB
QPI (Quick path interconnect) frequency		4.8 GT/s
Main memory		DDR3 Registered ECC DIMM 1333 MHz 2 GB / 4 GB / 8 GB / 16 GB
	Memory size	Max 192 GB (16 GB x 12)
Built-in HDD	Number of HDDs that can be installed	2.5 type x Max 4
	Size	Max 1800 GB (with RAID0 or RAID5) *4
	Feature	Supports: RAID 0, 1, 5, 6, 10/ Hot-plug, Hot-spare *5
Number of mezzanine slots		2
Network interface		Gb Ethernet x 2 ports
Management interface		Server blade Web console Remote console OS console (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet)
Front interface		USB（2.0）×2; Serial port (COM2) x 1 *6
Outside dimension (W x D x H: mm)		47.7×547×336 (except the Backplane connector)
Mass		8.56 kg
Power consumption (Max) *1		337 W
Power consumption in operation *2		270 W
Indications based on the Energy Saving law	Classification	J
	Energy consumption efficiency *3	3.5
Supported OS		Microsoft® Windows Server 2012 Microsoft® Windows Server 2008 R2 Microsoft® Windows Server 2008 Microsoft® Windows Server 2003 R2 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6

*1 Maximum power consumption for the equipment design.

*2 General power consumption in operation

*3 The energy consumption efficiency is obtained by dividing the electric power consumption

measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*4 When configuring a single RAID Group (logical drive), the capacity is available up to 2 TB.

*5 RAID 6 is supported only with GV-CA2SRD2X1-Y or GV-CA2SRD4X1-Y.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ Standard server blade specifications (3/6)

Model name		X55A2							
CPU	Supported CPU	Intel Westmere-EP processor							
		E5603	L5630	E5640	E5649	X5670	X5675	X5680	X5690
	Operating frequency of processors	1.6 GHz	2.13 GHz	2.66 GHz	2.53 GHz	2.93 GHz	3.06 GHz	3.33 GHz	3.46 GHz
	Number of processors	Max:2 (Max: 8 cores)			Max:2 (Max: 12 cores)				
	3rd Cache memory	4 MB	12 MB						
QPI (Quick path interconnect) frequency		4.8 GT/s	5.86 GT/s			6.4 GT/s			
Main memory		DDR3 Registered ECC DIMM 2 GB / 4 GB / 8 GB / 16 GB LV-DDR3 Registered ECC DIMM 2 GB / 4 GB / 8 GB							
	Memory size	Max 192 GB (16 GB x 12)							
Built-in HDD	Number of HDDs that can be installed	2.5 type x Max 4							
	Size	Max 1800 GB (with RAID0 or RAID5) *4							
	Feature	Supports: RAID 0, 1, 5, 6, 10/ Hot-plug, Hot-spare *5							
Number of mezzanine slots		2							
Network interface		Gb Ethernet x 2 ports							
Management interface		Server blade Web console Remote console OS console (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet)							
Front interface		USB (2.0) × 2; Serial port (COM2) x 1 *6							
Outside dimension (W x D x H: mm)		47.7×547×336 (except the Backplane connector)							
Mass		8.56 kg							
Power consumption (Max) *1		359 W	364 W	432 W	429 W	467 W	457 W	533 W	526 W
Power consumption in operation *2		279 W	293 W	347 W	336 W	437 W	404 W	458 W	442 W
Indications based on the Energy Saving law	Classification	J							
	Energy consumption efficiency *3	2.1	1.7	1.5	0.95	0.93	0.80	0.81	0.69

Model name	X55A2
Supported OS	Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2008 Microsoft® Windows Server® 2003 R2 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6

*1 Maximum power consumption for the equipment design.

*2 General power consumption in operation.

*3 The energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*4 When configuring a single RAID Group (logical drive), the capacity is available up to 2 TB.

*5 RAID 6 is supported only with GV-CA2SRD2X1-Y or GV-CA2SRD4X1-.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ Standard server blade specifications (4/6)

Model name		X55R3						
CPU	Supported CPU	Intel SandyBridge-EP processor						
		E5-2690	E5-2670	E5-2643	E5-2640	E5-2630	E5-2603	E5-2637
	Operating frequency of processors	2.90 GHz	2.60 GHz	3.30 GHz	2.50 GHz	2.00 GHz	1.80 GHz	3.00 GHz
	Number of processors	Max:2 (Max:8 cores)		Max:2 (Max:4 cores)	Max:2 (Max: 6 cores)		Max:2 (Max:4 cores)	Max:2 (Max:4 cores)
	3rd Cache memory	20 MB	20 MB	10 MB	15 MB	15 MB	10 MB	5 MB
QPI (Quick path interconnect) frequency		8.0 GT/s	8.0 GT/s	8.0 GT/s	7.2 GT/s	7.2 GT/s	6.4 GT/s	8.0 GT/s
Main memory		DDR3-LV Registered ECC DIMM 1333 MHz 4 GB/8 GB/16 GB/32 GB DDR3 LRDIMM 1333MH z 32GB						
	Memory size	Max 768 GB (32 GB x 24)						
Built-in HDD	Number of HDDs that can be installed	2.5 type x Max 6						
	Size *1	Max 1800 GB (with RAID0 or RAID5)						
	Feature	Supported: RAID0, 1, 10, 5, 6/ hotplug, hotspare						
Number of mezzanine slots		2						
Management interface		Remote KVM Serial redirection (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet port 0: Applying the dedicated driver allows port 1 available.)						
Front interface		USB (2.0) × 2; Serial port (COM2) x 1 *6						
Outside dimension (W x D x H: mm)		47.7 × 547 × 336 (except connector bumps on the backplane surface)						
Mass		9.2kg						
Power consumption (Max) *2		630W	614 W	531 W	577 W	476 W	356 W	431 W
Power consumption in operation *3		544 W	515 W	434 W	446 W	395 W	294 W	354 W
Indications based on the Energy Saving law	Classification	Out of target *5		J				
	Energy consumption efficiency *4			0.91	0.83	1.0	1.7	1.8
Supported OS		Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2008 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6						

*1 When you configure a single RAID Group (logical drive), the capacity is available up to 2TB.

*2 Maximum value of the power consumption for facility design

*3 Guideline of the power consumption for normal operation

*4 The energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*5 Theoretical performance of multiple processors is out of target for Energy Conservation law.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ Standard server blade specifications (5/6)

Model name		X55S3						
CPU	Supported CPU	Intel SandyBridge-EP processor						
		E5-2690	E5-2670	E5-2643	E5-2640	E5-2630	E5-2603	E5-2637
	Operating frequency of processors	2.90 GHz	2.60 GHz	3.30 GHz	2.50 GHz	2.00 GHz	1.80 GHz	3.00 GHz
	Number of processors	Max:2 (Max:8 cores)		Max:2 (Max:4 cores)	Max:2 (Max: 6 cores)		Max:2 (Max:4 cores)	Max:2 (Max:4 cores)
	3rd Cache memory	20 MB	20 MB	10 MB	15 MB	15 MB	10 MB	5 MB
QPI (Quick path interconnect) frequency		8.0 GT/s	8.0 GT/s	8.0 GT/s	7.2 GT/s	7.2 GT/s	6.4 GT/s	8.0 GT/s
Main memory		DDR3-LV Registered ECC DIMM 1333 MHz 4 GB/8 GB/16 GB/32 GB DDR3 LRDIMM 1333MH z 32GB						
	Memory size	Max 768 GB (32 GB x 24)						
Number of mezzanine slots		2						
Management interface		Remote KVM Serial redirection (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet port 0: Applying the dedicated driver allows port 1 available.)						
Front interface		USB (2.0) × 2; Serial port (COM2) x 1 *6						
Outside dimension (W x D x H: mm)		47.7 × 547 × 336 (except connector bumps on the backplane surface)						
Mass		8.8 kg						
Power consumption (Max)*2		576 W	560 W	477 W	523 W	422 W	302 W	377 W
Power consumption in operation*3		486 W	456 W	374 W	384 W	334 W	234 W	289 W
Indications based on the Energy Saving law	Classification	Out of target *5			J			
	Energy consumption efficiency *4			0.77	0.70	0.87	1.5	1.5
Supported OS		Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2008 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6						

*1 When you configure a single RAID Group (logical drive), the capacity is available up to 2TB.

*2 Maximum value of the power consumption for facility design

*3 Guideline of the power consumption for normal operation

*4 The Energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*5 Theoretical performance of multiple processors is out of target for Energy Conservation law.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ Standard Server Blade Specifications (6/6)

Model name		X55R4						
CPU	Supported CPU	Intel IvyBridge-EP processor						
		E5-2697v2	E5-2690v2	E5-2670v2	E5-2650v2	E5-2637v2	E5-2630v2	E5-2603v2
	Operating frequency of processors	2.70 GHz	3.00 GHz	2.50 GHz	2.60 GHz	3.50 GHz	2.60 GHz	1.80 GHz
	Number of processors	Max: 2 (Max: 24 cores)	Max: 2 (Max: 20 cores)	Max: 2 (Max: 20 cores)	Max: 2 (Max: 16 cores)	Max: 2 (Max: 8 cores)	Max: 2 (Max: 12 cores)	Max: 2 (Max: 8 cores)
	3rd Cache memory	30 MB	25 MB	25 MB	20 MB	15 MB	15 MB	5 MB
QPI (Quick path interconnect) frequency		8.0 GT/s	8.0 GT/s	8.0 GT/s	8.0 GT/s	8.0 GT/s	7.2 GT/s	6.4 GT/s
Main memory		DDR3-LV Registered ECC DIMM 1600 MHz 4 GB/8 GB/16 GB DDR3-LV Registered ECC DIMM 1866MHz 8GB/16GB DDR3 LRDIMM 1600 MHz 32 GB						
	Memory size	Max 768 GB (32 GB x 24)						
Embedded HDD	Type and number	Type: 2.5 x Max: 6						
	Capacity *1	Max 7200 GB (with RAID 0 or RAID 5)						
	Functions	Supports RAID 0, 1, 10, 5, 6; Hotplug, Hotspare						
Number of mezzanine slots		2						
Management interface		Remote KVM Serial redirection (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet port 0: Applying the dedicated driver allows port 1 available.)						
Front interface		USB (2.0) × 2; Serial port (COM2) x 1 *6						
Outside dimension (W x D x H: mm)		47.7 × 547 × 336 (except connector bumps on the backplane surface)						
Mass		9.2 kg						
Power consumption (Max)*2		628 W	625 W	533 W	493 W	486 W	427 W	347 W
Power consumption in operation*3		512 W	510 W	436 W	404 W	398 W	351 W	287 W
Indications based on the Energy Saving law	Classification	Out of target *5				J		
	Energy consumption efficiency					0.9	0.86	1.8

Model name		X55R4			
	*4				
Supported OS		Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6			

*1 When you configure a single RAID Group (logical drive), the capacity is available up to 2TB.

*2 Maximum value of the power consumption for facility design

*3 Guideline of the power consumption for normal operation

*4 The Energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*5 Theoretical performance of multiple processors is out of target for Energy Conservation law.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ High-performance server blade specifications (1/2)

Model name		X57A1		
CPU	Supported CPU	Intel® Xeon® processor E7540	Intel® Xeon® processor X7550,	Intel® Xeon® processor X7560
	Operating frequency of processors	2.00 GHz		2.26 GHz
	Number of processors	Max:2 [8] (Max: 12 [48] cores) *1	Max:2 [8] (Max: 16 [64] cores) *1	
	LLC (Last Level Cache)	18 MB	18 MB	24 MB
QPI (Quick path interconnect) frequency		6.4 GT/s		
Main memory		DDR3 Registered ECC DIMM 2GB/4GB/8GB		
	Size	Max 256 [1024] GB (8 GB x 32 [128]) *1		
Number of mezzanine slots		2 [8] *1		
Network interface		Gb Ethernet x 2 [8] ports *1		
Management interface		Server blade Web console Remote console OS console (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet to the Primary blade)		
Front interface		USB（2.0）x 2 (available only for the primary blade) Serial port (COM2) x 1 (available only for the primary blade) *5 QPI Full Width 6.4 GT/s 4 ports		
Outside dimension （W x D x H: mm）		47.7 x 547 x 336 (except the Backplane connector)		
Mass		10.8 kg		
Power consumption (Max) *2		638	688	694
Power consumption in operation *3		473	519	530
Indications based on the Energy Saving law	Classification	J		
	Energy consumption efficiency *4	2.8	2.1	1.9
Supported OS		Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2008 Microsoft® Windows Server® 2003 R2 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6		

*1 A number in the square brackets indicates the value with 4-blade SMP configuration.

*2 Maximum power consumption for the equipment design.

*3 General power consumption during operation.

*4 The energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*5 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ High-performance server blade specifications (2/2)

Model name		X57A2		
CPU	Supported CPU	Intel® Xeon® processor E7-8830	Intel® Xeon® processor E7-8860	Intel® Xeon® processor E7-8870
	Operating frequency of processors	2.13 GHz	2.26 GHz	2.40 GHz
	Number of processors	Max:2 [8] (Max: 16 [64] cores) *1	Max:2 [8] (Max: 20 [80] cores) *1	
	LLC (Last Level Cache)	24 MB	24 MB	30 MB
QPI (Quick path interconnect) frequency		6.4 GT/s		
Main memory		DDR3 Registered ECC DIMM 2GB/4GB/8GB/16GB DDR3-LV Registered ECC DIMM 16GB/32GB		
	Size	Max 768 [3072] GB (16 GB x 16 [64] + 32 GB x 16 [64]) *1		
Number of mezzanine slots		2 [8] *1		
Network interface		Gb Ethernet x 2 [8] ports *1		
Management interface		Server blade Web console Remote console OS console (via Telnet /SSL) IPMI 2.0. (Support only for it connected with a product verified by Hitachi.) Wake On LAN (Available only for onboard Gb Ethernet to the Primary blade)		
Front interface		USB（2.0）x 2 (available only for the primary blade) Serial port (COM2) x 1 (available only for the primary blade) *6 QPI Full Width 6.4 GT/s 4 ports		
Outside dimension （W x D x H: mm）		47.7 x 547 x 336 (except the Backplane connector)		
Mass		10.8 kg		
Power consumption (Max) *2		575 W / 553 W	652 W / 630 W	664 W / 642 W
Power consumption in operation *3		478 W / 456 W	501 W / 479 W	512 W / 490 W
Indications based on the Energy Saving law	Classification	J		
	Energy consumption efficiency *4	1.4	1.0	Out of target *5
Supported OS		Microsoft® Windows Server® 2012 R2 Microsoft® Windows Server® 2012 Microsoft® Windows Server® 2008 R2 Microsoft® Windows Server® 2008 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6		

*1 A number in the square brackets indicates the value with 4-blade SMP configuration.

*2 Maximum power consumption for the equipment design.

*3 General power consumption in operation

*4 The energy consumption efficiency is obtained by dividing the electric power consumption measured with the measurement method defined by the Energy Saving Law, by the composite theoretical performance defined by the Energy Saving Law.

*5 Theoretical performance of multiple processors is out of target for Energy Conservation law.

*6 The data transfer rate for the serial port (COM2) is fixed to 115200 bps.

❑ I/O board module specifications

Item		Specification
Expansion slot	Interface	PCI Express 2.0 (x8): 1 slot
	Card size	Low profile (L x H: 167.65 mm x 68.90 mm or smaller)
	Power supply for the card	3.3 V (Max. 3 A)/12 V (Max: 2.1 A) *1
	Power consumed by the card	Max: 25 W
Indicator		Power (green); Attention (orange)
Input power supply		12 V
Maximum power consumption		25 W
Outside dimension (W x D x H: mm)		25.6 x 239 x 80.6 (except Backplane connector)
Mass		0.48 kg

*1 Auxiliary (AUX) is not supported.

❑ Switch module specifications

Specifications of the built-in LAN switch module

Item			Specification	
			1-Gbps LAN switch module	1/10-Gbps LAN switch module
Capacity	Switch capacity (half duplex)		48 Gps	
	Packet processing		35.7 Mpps	
LAN port	External port		10/100/1000BASE-T x 4 ports	
			-	10GBASE-R x 2 ports
	Internal port		1000BASE-Serdes x 10 ports (Server blade I/F)	
Connector	10/100/1000BASE-T x 4		RJ-45	
	10G		XFP	
Console port (Management port)			10/100 Ethernet (RJ-45) Serial port (RS-232C) * In-band via the management module	
Layer-2 function	VLAN		Port VLAN, Tag-VLAN (IEEE802.1Q), Protocol VLAN, MAC-VLAN, Tag conversion	
	Spanning tree protocol		STP (IEEE802.1D), RST P(IEEE802.1w), PVST+, MSTP(IEEE802.1s)	
	Other functions		IGMP, snooping, MLD snooping, Link aggregation, jumbo frame, IEEE802.3ah/UDLD, Ring protocol	
Layer-3 function	IPv4 routing	Uni-cast	Static, RIP, RIP2, OSPF, BGP4	
		Multi-cast	IGMPv2/v3, PIM-SM, PIM-SSM	
	Ipv6 routing	Uni-cast	Static, RIPing, OSPFv3, BGP4+	
		Multi-cast	MLDv1/v2, PIM-SM, PIM-SSM	
Network function	Security function		Filter (L2/IPv4/IPv6/L4), and port to port relay interruption, IEEE802.1X authentication	
	Quality of Service (QoS)		Flow detection (L2/IPv4/IPv6/L4), band monitoring (rate control), marking (DSCP/User Priority), Priority control (Flow base, User priority mapping), disposal control (taildrop), shaper (eight classes, port band control), scheduling (PQ, WRR, PQ+DRR, WFQ)), Diff-serv, IEEE802.1p	
	High reliability; Advanced operation		Load balance (IPv4/IPV6), VRRP (IPv4/IPv6), Static polling, VRRP polling, Link aggregation (IEEE802.3ad), GSRP, Graceful Restart (Helper), Storm control	
	L2-VPN		VLAN tunneling	
Operation management function			SNMPv1/v2/v3, MIB II, IPv6MIB, RMON, syslog, ping, traceroute, SSH, telnet, ftp, tftp, NTP, IPv4DHCP server/relay, PrefixDelegation, LLDP, OADP, port mirroring, RADIUS, TACACS+, Uplink failover, (Dynamic) Flow statistics/information (sFlow)	
Power supply			12 V	
Outside dimensions (W x D x H: mm)			161 x 243 x 32.3 (except Backplane connector)	
Mass			1.16 kg	1.40 kg

Specifications of 10-Gb DCB switch module

Item	Specification
Link speed	10 Gbps, 1 Gbps
Ethernet	Flow control (802.3x), Jumbo frame
Layer 2	Function port VLAN, Tag-VLAN (IEEE 802.1Q), Protocol VLAN, MAC-VLANSTP (IEEE 802.1D), RSTP (IEEE 802.1w), PVST+, MSTP (IEEE 802.1s) link aggregation (static, IEEE 802.3ad), uplink-failover IGMP V2/V3 snooping, Storm Control
Security	ACLs (standard, VLAN-based, Port-based), IEEE 802.1X, Radius, TACACS+
QoS	8 Class Queue, CoS, Priority Queue, DWRR
Management	telnet, ftp, IPv4 SNMP (v1/v2), Ping, tracert, Cisco like CLI
CEE (Converged Enhanced Ethernet)	Priority-based Flow Control(PFC) – IEEE 802.1Qbb Enhanced Transmission Selection (ETS) – IEEE 802.1Qaz Data Center Bridging eXchange (DCBX) – IEEE DCB
High availability	Function associated with LAN controller redundancy (failover association), hot-plug replacement, configuration backup

Specifications of 1 Gb LAN pass through module

Item		Specification
Model name		1 Gbps LAN pass through module
LAN port	External port	1000BASE-T x 16 ports
	Internal port	1000BASE-Serdes x 16 ports (server blade I/F)
Connector		RJ-45
Circuit		1 Gbps/Full Duplex fixed, Auto-Negotiation enabled (fixed), Auto MDI/MDI-X enabled, support for Jumbo frame
	Auto-Negotiation parameter	Circuit speed: 1000 Mbps (fixed) Rotation mode: Full Duplex (fixed) Auto MDI/MDI-X: enabled Hardware flow control: tx/rx, both enabled
Indicator (LED)		Module (Power/LOCID) Circuit (Link/Activity)
Operation		Module operations only with management modules (No operation available with the module itself.)
Power supply		12 V
Mass		1.5 kg
Cooling		Forced air cooling
Hardware	hot swap	Available
Dimension (W x D x H: mm)		161 x 252 x 32.3

Specifications of 10 Gb LAN pass-through module

Item		Specification
Model name		10 Gbps LAN pass through module
LAN port	External port	10GBASE-SR (10 Gb) x 16 ports
	Internal port	10GBASE-KR (10 Gb) x 16 ports (server blade I/F)
Connector		SFP+
Circuit		10 Gbps/Full Duplex fixed, Auto-Negotiation enabled (fixed),
Indicator (LED)		Module ((Power/Status1/UID) Circuit (Link/Activity)
Operation		Module operations only with management modules (No operation available with the module itself.)
Power supply		12 V
Mass		1.4 kg without SFP+ optical transceiver (0.019 kg per unit)
Cooling		Forced air cooling
Hardware	hot swap	Available
Dimension (W x D x H: mm)		161 x 252 x 32.3

Specifications of built-in Fibre-channel switch module

Item		Specification
Product name		Brocade 8 Gb Fibre Channel switch module
Model name		GVX-BE2FSW1X1 (BX)/GV-BE2FSW1X1-Y: 12 ports active; with SFP+ x2 GVX-BE2FSW2X1 (BX): 22 ports active; with SFP+ x4
FCSW component		Brocade 5460
Fibre channel port		Minimum: 12 ports, internal and/or external to be assigned as you like. Maximum: 16 internal ports (Serdes server blade I/F) 6 external ports
Performance		2.125 Gbit/sec line speed, full duplex; 4.25 Gbit/sec line speed, full duplex; 8.5 Gbit/sec line speed, full duplex
Entire bandwidth		374 Gbit/sec 22 ports x 8.5 Gbit/sec (line rate) x 2 (full duplex)
Fabric latency		700 ns (8 Gbit/sec cut-through routing)
Fibre channel specification	Supported standard	FC-FG, FC-AL, FC-FLA, FC-PLCD, FC-VI, FC-PH, FC-GS-2, FC-PH-3, FC-SW, IPFC RFC, FC-AL2
	Service class	Class 2, class 3, class F
Maximum frame size		2112 byte payload
Data traffic		Unicast, multicast, broadcast
Media type		8 Gb SFP+, LC connector, short-wave laser Maximum: 500 m at 1 Gbps; 300 m at 2 Gbps; 150 m at 4 Gbps; 50 m at 8 Gbps
Scalability		Full-fabric architecture with up to 239 switches
Console port: management port		10/100 Ethernet (RJ-45) Serial port (RS-232C) Inband via management module
Fabric service	Ordinary	Simple Name Server (SNS) Registered State Change Notification (RSCN) Brocade Advanced Zoning Brocade Web Tools NPIV
	Option (charged)	Ports On Demand (POD) Fabric Watch ISL Trunking
Hardware option		SFP+ (for adding one external port)
		USB memory (for updating firmware; backing up and restoring configuration) These functions are available via FTP server without this option.
Operation management		SNMPv1, syslog, telnet, http, ftp
Power supply		12 V
Mass		1.4 kg (including SFP+)
Outside dimensions (W x D x H: mm)		161 x 252 x 32.3

❑ Management module specifications per module

Item		Specification
External interface	LAN for management	100BASE-T/100BASE-TX/10BASE-T x 2 ports.
	LAN for maintenance	100BASE-TX/10BASE-T x 1 port.
	Serial	One port
Internal interface	Between server blades	1000BASE-X x 10 ports
		I2C x 10 ports
		IPMB
	Between management modules	1000BASE-X x 1 port
	Switch	100BASE-X x 10 ports/I2C x 10 ports
	Between a fan and power supply	I2C x 12 ports
Indicator (LED)		Six LEDs are installed: shows status of Power, Master, Error, Remote, Location, and Heart Beat.
Console function	SVP console (CLI)	Offers the CLI (Command Line Interface) for system operation and management. The CLI is managed by a user.
	SVP console (GUI)	Supports the system Web console.
Middleware coordinating function	HA monitor	Provides coordination with the high availability (HA) cluster (HA monitor).
	Server management software	Provides coordination with Server Conductor/BladeServer Manager.
	Smart Configure	Collects information to execute N+M cold standby and switches configurations.
Remote maintenance function	E-mail notification	E-mail notification of error information (alert).
	Remote maintenance	Remote maintenance function linked with the remote maintenance system (ASSIST)
	Firmware update	To be supported.
Outside dimensions (W x D x H: mm)		24 x 239 x 174 (except Backplane connector)
Mass		1.22 kg

❑ Power supply module specifications per module

For A1 chassis

Item			Specification	
Input	Rated voltage		200 to 240 VAC	
	Permissible variation		178 to 264 VAC (sequence); 160-276 (0.5 s)	
	Frequency		50/60 Hz (±3 Hz)	
	Rated current		24 A	
	Efficiency		92% typ	
	Power factor		0.9 or higher	
	Inrush current		50 A or lower	
	Leaking current		0.7 mA or lower (Input voltage: 264 V; Frequency: 60 Hz)	
Output	Ch		Main	Sub
	Rated voltage		+12 VDC	+12 VDC
	Rated current		0 to 334 ADC	0 to 5 ADC
	Rated power		4008 W	60 W
	Protection	Over current	340 to 500 A	7 to 9 A
		Over voltage	13.8 to 16.8 V	13.8 to 16.8 V
		UV detection	3.6 to 9.6 V	3.6 to 9.6 V
	Retaining in power interruption		20 ms or longer	
Outside dimensions (W x D x H: mm)			104 x 740 x 70 (except Backplane connector)	
Mass			6.38 kg	

For A2 chassis

Item			Specification	
Input	Rated voltage		200 to 240 VAC	
	Permissible variation		178 to 264 VAC (sequence); 160-276 (0.5 s)	
	Frequency		50/60 Hz (±3 Hz)	
	Rated current		20 A	
	Efficiency		92% typ	
	Power factor		0.9 or higher	
	Inrush current		50 A or lower	
	Leaking current		0.7 mA or lower (Input voltage: 264 V; Frequency: 60 Hz)	
Output	Ch		Main	Sub
	Rated voltage		+12 Vdc	+12 Vdc
	Rated current		0 to 295 Adc	0 to 5 Adc
	Rated power		3540 W	60 W
	Protection	Over current	340 to 500 A	7 to 9 A
		Over voltage	13.8 to 16.8 V	13.8 to 16.8 V
		UV detection	3.6 to 9.6 V	3.6 to 9.6 V
	Retaining in power interruption		20 ms or longer	
Outside dimensions (W x D x H: mm)			104 x 797 x 70 (except Inlet connector)	
Mass			6.64 kg	

❑ Fan module specifications per module

Item	Specification
Rated voltage (permissible variation)	12 (10.8 to 13.2) V
Rated current	12 A
Rated input power	144 W
Number of installed fan modules	3
Maximum wind amount	4.5 m3/min: 159 CFM
Maximum static pressure (Pa: inchiH2O)	1600 Pa: inchiH2O
Sound pressure level (dB[A])	74.3 dB[A]
Permissible humidity variation (°C)	5 to 70°C
Rotation control method	Pulse width modulation (PWM) control via I2CBus
Unplugging/plugging method	HotSwap
Protection method	Breaks the over current with a fuse. HotSwap Controller OCP function
Redundancy method	N+1
Indicator	Active (green); Failure (orange)
Humidity sensor	Installed on the control board.
Outside dimension (W x D x H: mm)	83 x 237 x 85.8 (except Backplane connector)
Mass	1.44 kg

❑ AC power input module specifications per module

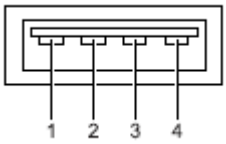
Item	Specification	
	2 input connectors	1 input connector
AC cable	4.5 m x 2 cables	4.5 m x 1 cable
AC plug	NEMA L6-30P（GVX-BE2ACM1X1） IEC60309-32（GVX-BE2ACM1X2）	
Rated voltage	AC200 V to 240 V	
Rated current	24 A/AC cable	24 A
Outside dimension (W x D x H: mm)	209 x 62.7 x 42.5 (except connector)	
Mass	2.56 kg	1.43 kg

❑ I/O slot expansion unit specifications

Item		Specification
I/O module		2 as standard
Number of expanded slots		16 as standard per I/O module: PCI Express 2.0 (x8) x 4 slots PCI Express 2.0 (x4) x 4 slots
Server chassis connect port		4 as standards: 2 per I/O module
Power supply module		2 as standards: 1 + 1 redundancy
Cooling fan module		4 as standards: 2 per I/O module; 1 + 1 redundancy
Outside dimension（W x D x H: mm）		449 x 759 x 174
EIA standard unit		4 U
Mass: Maximum		About 48 kg
Power supply	Input voltage: frequency	AC 200 V to 240 V single-phase (50/60 Hz)
	Max rated voltage	1 kW
Environment	Temperature (°C)	5 to 35°C
	Humidity (%)	20 to 80%; No condensation is allowed.

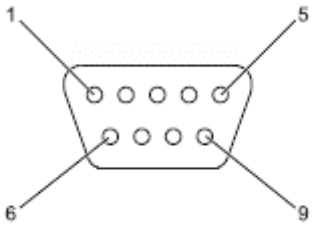
Interface specifications

USB connector



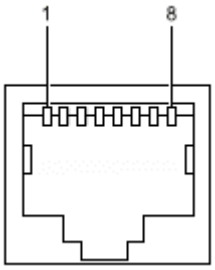
Pin	Signal Name	Description	Direction
1	VCC	Cable power	Output
2	DATA –	Differential signal –	Input/Output
3	DATA +	Differential signal +	Input/Output
4	GND	Cable Ground	–

RS-232C interface connector (management module)



Pin	Signal Name	Description	Direction
1	CD	Carrier Detect	Input
2	RD	Receive Data	Input
3	TD	Transmit Data	Output
4	DTR	Data Terminal Ready	Output
5	GND	Signal Ground	–
6	DSR	Data Set Ready	Input
7	RTS	Request to Send	Output
8	CTS	Clear to Send	Input
9	RI	Ring Indicator	Input

LAN interface connector (management module)



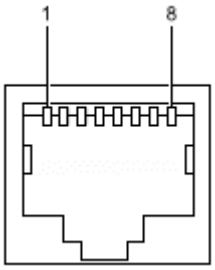
Connected with 1000BASE-T

Pin	Signal Name	Description	Direction
1	TP0+	Transmit/Receive Data	Output/Input
2	TP0-	Transmit/Receive Data	Output/Input
3	TP1+	Transmit/Receive Data	Output/Input
4	TP2+	Transmit/Receive Data	Output/Input
5	TP2-	Transmit/Receive Data	Output/Input
6	TP1-	Transmit/Receive Data	Output/Input
7	TP3+	Transmit/Receive Data	Output/Input
8	TP3-	Transmit/Receive Data	Output/Input

Connected with 100BASE-TX/10BASE-T

Pin	Signal Name	Description	Direction
1	TX+	Transmit Data +	Output
2	TX–	Transmit Data –	Output
3	RX+	Receive Data +	Input
4	NC	Reserved	–
5	NC	Reserved	–
6	RX–	Receive Data –	Input
7	NC	Reserved	–
8	NC	Reserved	–

LAN interface connector (switch module)



Connected with 1000BASE-T

Pin	Signal Name	Description	Direction
1	TP0+	Transmit/Receive Data	Output/Input
2	TP0-	Transmit/Receive Data	Output/Input
3	TP1+	Transmit/Receive Data	Output/Input
4	TP2+	Transmit/Receive Data	Output/Input
5	TP2-	Transmit/Receive Data	Output/Input
6	TP1-	Transmit/Receive Data	Output/Input
7	TP3+	Transmit/Receive Data	Output/Input
8	TP3-	Transmit/Receive Data	Output/Input

Connected with 100BASE-TX/10BASE-T

Pin	Signal Name	Description	Direction
1	TX+	Transmit Data +	Output
2	TX–	Transmit Data –	Output
3	RX+	Receive Data +	Input
4	NC	Reserved	–
5	NC	Reserved	–
6	RX–	Receive Data –	Input
7	NC	Reserved	–
8	NC	Reserved	–

Software license

Information on software license

Software incorporated in the baseboard management controller (BMC) consists of independent multiple pieces of software. Each of them is copyrighted by Hitachi, Ltd. or third parties.

The property rights and the intellectual property rights of software incorporated in BMC, which Hitachi, Ltd. has developed or created, are owned by Hitachi, Ltd. The property rights and the intellectual property rights of documents related to the software are owned by Hitachi, Ltd. Those are protected by the copyright and other laws.

BMC uses open source software shown in the following table in compliance with each software license agreement as well as software developed or created by Hitachi, Ltd.

We provide you with source code of software licensed under the terms of the license, such as GNU's Not UNIX (GNU) General Public License (GPL), which indicates that we must distribute the source code, on CDROM or DVD by your request. Please take note that you will be charged for the media, shipping fee, and commission. When you need to have source code media, check the BMC firmware version on the Web console screen, write it down, and contact your reseller to give them the version.

For the following open source software, consult your reseller.

Software	License Agreement
Linux Kernel U-Boot busybox iptables mii-tool gawk rsync liblzo cron ethtool logrotate mtd-utils e2fsprogs	GNU General Public License version 2: Visit the following URL. http://www.gnu.org/licenses/gpl-2.0.html
zlib	zlib license Visit the following URL. http://www.zlib.net/zlib_license.html
openssl	OpenSSL License Visit the following URL. http://www.openssl.org/source/license.html
openssh	BSD License Visit the following URL. http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD
openldap	The OpenLDAP Public License Visit the following URL. http://www.openldap.org/software/release/license.html
pam_ldap	GNU LESSER GENERAL PUBLIC LICENSE Visit the following URL.

Software	License Agreement
	http://www.gnu.org/copyleft/lesser.html
perl	GNU General Public License/Artistic License Visit the following URL. http://dev.perl.org/licenses/
netkit-tftp syslogd	BSD License Visit the following URL. http://www.freebsd.org/copyright/license.html
stunnel	stunnel license Visit the following URL. https://www.stunnel.org/sdf_copying.html
ntp ntpdate	NTP License Visit the following URL. http://opensource.org/licenses/NTP
rsyslog	GNU General Public License version 3 Visit the following URL. http://www.rsyslog.com/doc/licensing.html

Glossary

This glossary defines the special terms used in this document. Click the desired letter below to display the glossary entries that start with that letter.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A

AC

alternating current

ACPI

advanced configuration and power interface

ADSI

active directory service interface

AER

advanced error reporting

AFT

adapter fault tolerance

ALB

adaptive load balancing

ALM

alarm lamp

AMPP

automatic migration of port profiles

APIC

advanced programmable interrupt controller

ASCII

American Standard Code for Information Interchange

AUX

auxiliary

B

BBU

battery backup unit

BGI

background initializing

BIOS

basic input/output system

BMC

baseboard management controller

BSM

Blade Server Manager

C

CA

certificate authority

CAS

column address strobe

CBL

cable removal tool

CC

consistency check

CD

compact disc

CEE

Converged Enhanced Ethernet

CIM

Common Information Model

CLI

command line interface

Client

client PC

CLP

Command Line Protocol

CMOS

Complementary metal– oxide–semiconductor

CN

Common Name

CNA

converged network adapter

CND

condition lamp

COM

communication port

CPU

central processing unit

CRLF

carriage return/line feed

CRT

cathode ray tube

CSR

certificate signing request

CSV

comma-separated values

CUI

character-based user interface

D

DBS

Demand Base Switching

DCB

Data Center Bridging

DDR

double data rate

DER

Distinguished Encoding Rules

DHCP

Dynamic Host Configuration Protocol

DIMM

dual inline memory module

DL

dump log

DMTF

Distributed Management Task Force

DN

domain name

distinguished name

DNS

domain name system

DPM

Deployment Manager

DSA

digital signature algorithm

DST

Daylight Savings Time

DVD

digital versatile disc

E

EC

Event Code

ECC

Error Check and Correct

EFI

extensible firmware interface

EIA

Electronic Industries Alliance

EIST

Enhanced Intel SpeedStep Technology

EKMS

electronic key management systems

F

FC

Fibre Channel

FCoE

Fibre Channel over Ethernet

FD

floppy disk

FDD

floppy disk drive

FDE

full disk encryption

FFB

fuse free breaker

FPGA

field programmable gatearray

FQDN

qualified domain name

FRU

field replaceable unit

FTP

File Transfer Protocol

G

GMT

Greenwich Mean Time

GNU

GNU’s Not Unix

GPL

GNU General Public License

GPT

GUID partition table

GSRP

Gigabit Switch Redundancy Protocol

GUID

globally unique identifier

H

HA

high availability

HBA

host bus adapter

HCSM

Hitachi Compute Server Manager

HDD

hard disk drive

HDLM

HiCommand Dynamic Link Manager

HFC-PCM

Hitachi Fibre Channel – Path Control Manager

HPET

high precision event timer

HTTP

HyperText Transfer Protocol

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer

HVM

Hitachi Virtualization Manager

HvmSh

HVM Shell command: used like a proper noun.

I

IAC

interpreted as command

ICMP

Internet Control Message Protocol

IOCD

input/output control device

IOSW

input output switch

IP

Internet Protocol

IPMI

intelligent platform management interface

iSCSI

Internet small computer system interface

ITRM

IT Resource Management – Manager

J

Java

A programming language created by James Gosling and now developed by Sun; used to produce software for multiple platforms

JRE

Java Runtime Environment

K

KVM

keyboard, video and mouse

L

L

Locality Name

LACP

Link Aggregation Control Protocol

LACPDU

LACP data unit

LAN

local area network

LC

LAN configuration

LCD

liquid crystal display
Local Configuration Datastore

LDAP

Lightweight Directory Access Protocol

LED

light emitting diode

LF

line feed

LFT

Link Fault Tolerance

LID

Location ID Lamp

LLC

last level cache

LOCID

location ID LED

LOM

legacy OS mode

LP/LPAR manager

logical partitioning manager

LPAR

logical partition

LPVID

logical port VLAN ID

LTO

Linear Tape-Open

LU

logical unit

LUN

logical unit number

M

MAC

media access control

MAR

maintenance action report

MC

memory card slot
memory card

MDI-X

medium dependent interface crossover

MIB

management information base

MMC

Microsoft Management Console

MN

memory node

MSR LED

Master LED

MTU

maximum transfer unit

N

NAS

network attached storage

NCQ

native command queuing

NEMA

National Electrical Manufacturers Association

NIC

network interface card

NMI

non-maskable interrupt

NPIV

N-Port ID Virtualization

NTP

Network Time Protocol

NUMA

non-uniform memory access

NVDATA

A type of name for RAID controller setting files

NVRAM

non volatile RAM

O

O

Organization Name

OEM

original equipment manufacturer

OID

object ID

OU

Organization Unit Name

P

PCI

peripheral components interconnect

PCIe

PCI Express

PDU

power distribution unit

PEM

privacy enhanced mail

PFM

Performance Management

PIT

programmable interval timer

POD

Ports On Demand

POST

power on self test

PWM

Pulse width modulation

PXE

Preboot eXecution Environment

Q

QoS

Quality of Service

QPI

Quick path interconnect

R

RAID

Redundant Arrays of Independent Disks

RAS

reliability availability serviceability

RC

Read Create
Reference Code

RE

RC type enhanced bit

RHEL

Red Hat Enterprise Linux

RO

read-only

ROM

Read Only Memory

RPM

revolutions per minute

RSA

Public-key cryptosystem: the algorithm of which was first publicly described by Rivest, Shamir, and Adleman. The acronym stands for names of the three.

RST

Reset button
Reset

RTC

real-time clock

RW

read- write

S

SAC

Special Administration Console

SAN

storage area network

SAS

serial attached SCSI

SBR

serial boot ROM

SC

ServerConductor

Schd

scheduling mode

SCOM MP

System Center Operations Manager Management Pack

SD

Secure Digital

SDN

Software Defined Networking

SEL

system event log

SFP+

small form-factor pluggable plus

SFT

switch fault tolerance

SFTP

SSH File Transfer Protocol

S.M.A.R.T.

Self-Monitoring Analysis and Reporting Technology

SMASH

Systems Management Architecture for Server Hardware

SMP

Symmetric Multiprocessing

SMT

simultaneous multi-threading

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

Srv

service ratio

SSD

solid state drive

SSH

Secure SHell

SSL

Secure Socket Layer

ST

State or Province Name

STS

status LED

SVGA

Super Video Graphics Array

SVP

service processor

T

TCP

Transmission Checksum Protocol

TEP

temperature LED

TLS

Transport Layer Security

TPM

trusted platform module

TSC

time stamp counter

TSO

TCP segmentation offload

U

UDP

User Datagram Protocol

UFEI

unified extensible firmware interface

UID

unit ID

UPS

uninterruptible power supply

USB

Universal Serial Bus

UTC; U/L

Coordinated Universal Time
Often spelled out as Universal Time Coordinated and sometimes as Universal Coordinated Time because abbreviated as UTC.
The time standard commonly used across the world since 1972 and used to synchronize time across internet networks.

UTP

Unshielded Twist Pair cable

UUID

universal unique ID

V

VD

Virtual Drives

VFP

virtual front panel

VGA

video graphics array

VLAN

virtual local area network

VNIC

virtual NIC

VRRP

Virtual Router Redundancy Protocol

VT

Intel Virtualization Technology
Video Terminal

W

WDT

Watch Dog Timer

WinRM

Windows Remote Management

WOL

Wake On LAN

WS-MAN

Web Service Management

WWN

world wide name

WWNN

world wide node name

WWPN

world wide port name

Z

ZMODEM

A type of name: A file transfer protocol updated from XMODEM and YMODEM mainly by supporting sliding window.

Glossary

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-99BDS2K001-16