
PRIMEQUEST

500A/500/400 SERIES

REFERENCE MANUAL:
TOOLS/OPERATION INFORMATION

FOR SAFE OPERATION

This manual contains important information regarding the use and handling of this product. Read this manual thoroughly. Pay special attention to the section "NOTE ON SAFETY" Use the product according to the instructions and information available in this manual. Keep this manual handy for further reference.

Fujitsu makes every effort to prevent users and bystanders from being injured or from suffering damage to their property. Use the product according to this manual.

ABOUT THIS PRODUCT

This product is designed and manufactured for use in standard applications such as office work, personal device, household appliance, and general industrial applications. This product is not intended for use in nuclear-reactor control systems, aeronautical and space systems, air traffic control systems, mass transportation control systems, medical devices for life support, missile launch control systems or other specialized uses in which extremely high levels of reliability are required, the required levels of safety cannot be guaranteed, or a failure or operational error could be life-threatening or could cause physical injury (referred to hereafter as "high-risk" use). You shall not use this product without securing the sufficient safety required for high-risk use. If you wish to use this product for high-risk use, please consult with sales representatives in charge before such use.

RADIO FREQUENCY INTERFERENCE STATEMENT

The following notice is for EU users only.

WARNING: This is a product which meets Class A of EN55022. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

The following notice is for USA users only.

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 his own expense.

Laser standards

This equipment includes Class 1 laser products and complies with FDA Radiation Performance Standards, 21 CFR 1040.10 and 1040.11, and the International Laser Safety Standards IEC60825-1: 2001.

TRADEMARK ACKNOWLEDGEMENTS

- Microsoft, Windows, MS, Windows NT, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- Red Hat, RPM, and all Red-Hat-based marks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- SUSE is a registered trademark of Novell Inc. in the United States and other countries.
- Intel, Xeon, and Itanium are trademarks or registered trademarks of Intel Corporation.
- Ethernet is a registered trademark of Fuji Xerox Co., Ltd. and Xerox Corporation in the United States and other countries.
- All other product names mentioned herein are the trademarks or registered trademarks of their respective owners.
- System and product names in this manual are not always noted with trademark or registered trademark symbols (™), (®).

TERMS AND CONDITIONS

The product includes software provided by third parties in addition to that provided by Fujitsu Ltd. You are granted permission to use the third parties' software subject to the terms and conditions below. If you acquire the source code of the software to which the following terms and conditions apply, refer to LICENSE1_EN.pdf and LICENSE2_EN.pdf, which are provided with the 'PRIMEQUEST Manuals' (C122-E013-C2).

THIS SOFTWARE IS PROVIDED "AS IS" AND FUJITSU LIMITED MAKES NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER WHATSOEVER REGARDING TO THIS SOFTWARE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

IN NO EVENT SHALL FUJITSU LIMITED BE LIABLE FOR ANY CLAIM FROM A THIRD PARTY, OR SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE, COPYING, MODIFICATION OR DISTRIBUTION OF THIS SOFTWARE.

The contents of this manual shall not be disclosed in any way or reproduced in any media without the express written permission of Fujitsu Limited.

All Rights Reserved, Copyright © FUJITSU LIMITED 2007, 2008

Revision History

(1/1)

Edition	Date	Revised section (Added/ Deleted/ Altered)(Note)	Details
01	2007-08-31	—	—
02	2008-03-10	Entire manual (addition)	Addition of description for PRIMEQUEST 580A/540A/520A
03	2008-04-10	Section 10.2.3, 10.2.5 (correction)	Error corrections

Note: In this table, the revised section is indicated by its section number in the current edition.

An asterisk (*) indicates a section in the previous edition.

Preface

This manual provides auxiliary information required for PRIMEQUEST maintenance and operation. Read this manual together with the manuals referenced in this manual.

This section explains:

- [Structure and Contents of This Manual](#)
- [Other Reference Manuals](#)
- [Abbreviations](#)
- [Text Conventions](#)
- [Syntax of the Command Line Interface \(CLI\)](#)
- [Notes Regarding Notations Used in This Manual](#)
- [Conventions for Alert Messages](#)
- [Environmental Requirements for Using This Product](#)
- [Reader Feedback](#)

Structure and Contents of This Manual

This manual is organized as described below:

[CHAPTER 1 System Maintenance](#)

Explains system maintenance, which includes dump, backup, and restore operations.

[CHAPTER 2 Physical Locations of Components](#)

Describes the mounting locations of components.

[CHAPTER 3 Hot Plug](#)

Explains the PCI card hot-plug procedure

[CHAPTER 4 Manual PSA Installation](#)

Describes how to manually install the PSA and the settings required after installation.

[CHAPTER 5 Physical Locations and Bus Numbers](#)

Describes the physical locations and Bus Numbers of Built-in I/Os.

[CHAPTER 6 Management LAN Reconfiguration Required at the Time of BMM Replacement](#)

Describes reconfiguration of management LAN required at the time of BMM replacement.

CHAPTER 7 REMCS

Explains how to operate the REMCS (Remote Customer Support System).

CHAPTER 8 Onboard GbE (Broadcom Ethernet) Network Configuration Under Windows Environment

Explains the network configuration procedure for networks running in a Windows environment.

CHAPTER 9 MIB Tree Provided by PRIMEQUEST

Describes the MIB tree system provided by PRIMEQUEST.

CHAPTER 10 Status Confirmation from LED

Describes PRIMEQUEST operator panel (OPL) and LED display of the boards.

Appendix A Alternative Key Combinations for Some Special Keys on Serial Terminals

Describes alternate inputs for specific keys on serial terminals.

Index

Describes keywords and corresponding reference page numbers.

Other Reference Manuals

The following manuals are provided for reference:

a) PDF manuals included on the *PRIMEQUEST Manuals* CD-ROM disk
(C122-E013-C2)

Title	Description	Manual code
<i>PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide</i>	Explains requirements, considerations, and notes on the system operation design of the PRIMEQUEST 580A/540A/580/540/480/440.	C122-B001EN
<i>PRIMEQUEST 580A/540A/580/540/480/440 Installation Planning Manual</i>	Explains specifications and requirements for installation sites that are applicable to the installation of the PRIMEQUEST 580A/540A/580/540/480/440.	C122-H001EN
<i>PRIMEQUEST 520A/520/420 System Design Guide</i>	Explains requirements, considerations, and notes on the system operation design of the PRIMEQUEST 520/420.	C122-B009EN
<i>PRIMEQUEST 520A/520/420 Installation Planning Manual</i>	Explains specifications and requirements for installation sites that are applicable to the installation of the PRIMEQUEST 520A/520/420.	C122-H002EN
<i>PRIMEQUEST 500A/500/400 Series Installation Manual</i>	Explains the setup of the PRIMEQUEST, including the preparation for the installation, initial settings, and software installation.	C122-E001EN
<i>PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands</i>	Explains operations, setup methods, and the system management method that are required for the system operation of the PRIMEQUEST. The explanation covers basic operations and functions of the MMB, PSA, and EFI.	C122-E003EN
<i>PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information</i>	Explains system maintenance, Hot Plug, REMCS, and LEDs and other information required for system operation. Also, the manual provides supplementary information such as information on the physical locations of components.	C122-E074EN
<i>PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs</i>	Explains measures to be taken against problems that occur during operation and describes various types of messages.	C122-E004EN
<i>PRIMEQUEST GSWB User's Manual</i>	Explains the requirements, points to consider, and notes concerning installing and operating GSWB, an optional product.	C122-E028EN
<i>SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual</i>	Explains basic information and policy on installation planning and facilities planning that are required for the installation of the SPARC Enterprise series and PRIMEQUEST series.	C120-H007EN
<i>PRIMEQUEST 580A/540A Dynamic Partitioning (DP) Manual</i>	Explains the Dynamic Partitioning (DP) function which the PRIMEQUEST 580A/540A supports.	C122-E085EN

b) Printed manual

For the printed manual (sold separately), contact your certified service engineer.

- *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN)

Abbreviations

In this manual, the product names are abbreviated as follows:

Long title	Abbreviations
Red Hat® Enterprise Linux® AS (v.4 for Itanium)	Red Hat (*1)
Red Hat® Enterprise Linux® 5 (for Intel Itanium)	
Red Hat® Enterprise Linux® AS (v.4 for Itanium)	RHEL-AS4 (IPF)
Red Hat® Enterprise Linux® 5 (for Intel Itanium)	RHEL5 (IPF) (*2)
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family	
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE9
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family	SUSE10
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based Systems	Windows Windows Server 2003
Microsoft® Windows Server® 2003, Datacenter Edition for Itanium-based Systems	
Microsoft® Windows Server® 2008 for Itanium-Based Systems	Windows Windows Server 2008

*1: Version-independent abbreviation

*2: A description in the form of "RHEL5.x (IPF)" indicates an updated version.

Text Conventions

This manual uses the following symbols to express specific types of information:

Fonts/symbols	Meaning	Example
<i>Italic</i>	Indicates names of manuals.	See the <i>PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide</i> .
" "	Indicates names of chapters, sections, items, buttons, or menus.	See Chapter 5, "System Maintenance.
[]	Indicates window names, window button names, tab names, and dropdown menu selections.	Click the [OK] button.

Syntax of the Command Line Interface (CLI)

The command syntax is described below.

Command syntax

The command syntax is as follows:

- A variable that requires input of a value must be enclosed in < >.
- An optional element must be enclosed in [].
- A group of options for an optional keyword must be enclosed in [] and delimited by |.
- A group of options for a mandatory keyword must be enclosed in { } and delimited by |.



The command syntax is shown in a frame such as this one.

Notes Regarding Notations Used in This Manual

- Items marked with "Linux" apply to both Red Hat® Enterprise Linux® AS (v.4 for Itanium), Red Hat® Enterprise Linux® 5 (for Intel Itanium), SUSE™ Linux Enterprise Server 9 for Itanium Processor Family and SUSE™ Linux Enterprise Server 10 for Itanium Processor Family (*).
*: For details, contact a Fujitsu certified service engineer.
- The IO Unit is indicated as "IOU" in the MMB Web-UI and in the figures shown in this manual.

Conventions for Alert Messages

This manual uses the following conventions to show alert messages. An alert message consists of an alert signal and alert statements.

 WARNING	This indicates a hazardous situation that <i>could</i> result in serious personal injury if the user does not perform the procedure correctly.
 CAUTION	This indicates a hazardous situation that <i>could</i> result in minor or moderate personal injury if the user does not perform the procedure correctly. This signal also indicates that damage to the product or other property may occur if the user does not perform the procedure correctly.
IMPORTANT	This indicates information that could help the user to use the product more effectively.

Alert messages in the text

In the text, alert messages are indented to distinguish them from regular text. A wider space precedes and follows the message to show where the message begins and ends.

⚠ WARNING

Certain tasks in this manual should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause electric shock, injury, or fire.

- Installation and reinstallation of all components, and initial settings
- Removal of front, rear, or side covers
- Mounting/de-mounting of optional internal devices

Environmental Requirements for Using This Product

This product is a computer which is intended to be used in a computer room. For details on the operational environment, see the following manuals:

- *PRIMEQUEST 580A/540A/580/540/480/440 Installation Planning Manual (C122-H001EN)*
- *PRIMEQUEST 520A/520/420 Installation Planning Manual (C122-H002EN).*

Reader Feedback

- In this manual, it is assumed that two BMMs (optional products) can be connected to a single IO Unit and IOX; this is reflected both in the explanations and in the figures included in this manual. At present, however, the PRIMEQUEST 400 series supports only connection to one BMM (BMM#0) per IO Unit and IOX.
- In this manual, the term BP (BackPlane) used in descriptions for the PRIMEQUEST 480/440 series actually stands for MP (MidPlane).
- The screen images in this manual may be different from the actual screen images.
- If you find any errors or unclear statements in this manual, please fill in the "Reader's Comment Form" sheet at the back of this manual and forward it to the address indicated at the bottom of the sheet.
- This manual is subject to revision without prior notice.
- The PDF version of this manual is best viewed in Adobe® Reader® with a magnification of 100% and Single Page for the page layout.

Product Handling

Maintenance

WARNING

Certain tasks in this manual should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause electric shock, injury, or fire.

- Installation and reinstallation of all components, and initial settings
- Removal of front, rear, or side covers
- Mounting/de-mounting of optional internal devices
- Plugging or unplugging of external interface cards
- Maintenance and inspections (repairing, and regular diagnosis and maintenance)

CAUTION

The following tasks regarding this product and the optional products provided from Fujitsu should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause malfunction.

- Unpacking optional adapters and such packages delivered to the users

Remodeling/Rebuilding

CAUTION

Do not make mechanical or electrical modifications to the equipment.
Using this product after modifying or overhauling may cause unexpected injury or damage to the property, the user, or bystanders.

Contents

Preface	i
Structure and Contents of This Manual	i
Other Reference Manuals	ii
Abbreviations	iv
Text Conventions	iv
Syntax of the Command Line Interface (CLI)	v
Notes Regarding Notations Used in This Manual	v
Conventions for Alert Messages	v
Environmental Requirements for Using This Product	vi
Product Handling	vii
Maintenance	vii
Remodeling/Rebuilding	vii
CHAPTER 1 System Maintenance	1-1
1.1 System Maintenance	1-1
1.2 Notes on the Maintenance of PCI Cards	1-1
1.3 Hot Swapping of Hard Disk	1-2
1.3.1 Addition, removal, replacement, and location check of hard disks	1-3
1.3.1.1 Procedure for addition	1-3
1.3.1.2 Procedure for removal	1-6
1.3.1.3 Procedure for replacement (Except for failures in which the hard disk fails to respond)	1-10
1.3.1.4 Procedure for replacement (For failures in which the hard disk fails to respond)	1-16
1.4 REMCS Service	1-22
1.4.1 Overview of REMCS service	1-22
1.4.2 Supported connection modes	1-24
1.5 Collecting Maintenance Data (Linux)	1-25
1.6 Collecting Maintenance Data (Windows Server 2003)	1-26
1.6.1 Early troubleshooting [DSNAP]	1-26
1.6.2 Software Support Guide	1-27
1.6.2.1 Collecting information with Software Support Guide	1-28
1.7 Setting Dump Environments (Windows Server 2003)	1-31
1.7.1 Memory dump/paging file	1-31
1.7.1.1 Different information that can be collected with a memory dump	1-31
1.7.1.2 Setting a memory dump	1-33

1.7.1.3	Verifying the memory dump settings	1-34
1.7.1.4	Setting paging files	1-35
1.7.1.5	Note	1-37
1.8	Backup and Restoration	1-38
1.8.1	Backup Requirements	1-38
1.8.2	Linux (Red Hat) backup	1-38
1.8.2.1	Backup when PRIMECLUSTER GDS is not used	1-39
1.8.2.2	Backup when PRIMECLUSTER GDS is used	1-46
1.8.3	Linux (Red Hat) restoration	1-47
1.8.3.1	Restoration when PRIMECLUSTER GDS is not used	1-47
1.8.3.2	Restoration when PRIMECLUSTER GDS is used	1-58
1.8.4	Windows backup	1-59
1.8.5	Windows restoration	1-59
1.9	Notes on Setting a Device Name (Linux: Red Hat)	1-60
1.9.1	Disk system devices	1-61
1.9.1.1	Details on device names	1-62
1.9.1.2	Commands and files with awareness of device names	1-63
1.9.1.3	Notes on using new devices	1-63
1.9.2	Network Devices	1-64
CHAPTER 2	Physical Locations of Components	2-1
2.1	Component, LED, and Interface Locations (PRIMEQUEST 580A/540A/580/540/480/440)	2-1
2.2	Component, LED, and Interface Locations (PRIMEQUEST 520A/520/420)	2-12
CHAPTER 3	Hot Plug	3-1
3.1	Overview of Hot Plugging	3-1
3.2	Hot Plugging Procedure	3-3
3.2.1	General workflow	3-3
3.2.2	Installation of a PCI Hot Plug driver	3-4
3.2.3	Power operation procedure	3-4
3.2.3.1	Checking the power status	3-5
3.2.3.2	Power-on and power-off procedures	3-5
3.3	Common Procedures for Hot Plugging PCI Cards	3-6
3.3.1	Addition procedure	3-6
3.3.2	Removal procedure	3-6
3.3.3	Swapping procedure	3-6
3.4	Hot Plugging a Network Card	3-7
3.4.1	Hot plugging a network card used independently (used without GLS)	3-7
3.4.1.1	Addition procedure	3-8

3.4.1.2	Removal procedure	3-12
3.4.1.3	Swapping procedure	3-17
3.4.2	Hot plugging a network card under GLS control	3-23
3.4.2.1	Addition procedure	3-25
3.4.2.2	Removal procedure	3-31
3.4.2.3	Swapping procedure	3-35
3.4.3	Handling kudzu	3-40
3.4.4	Assigning a specific interface name to an interface	3-41
3.4.5	Installation verification procedure	3-44
3.5	Hot Plugging a SCSI Card (FC Card)	3-45
3.5.1	Hot plugging an HBA running without PRIMECLUSTER GDS and ETERNUS multipath driver	3-46
3.5.1.1	Addition procedure	3-46
3.5.1.2	Removal procedure	3-47
3.5.1.3	Swapping procedure	3-48
3.5.1.4	Checking installation results	3-49
3.5.2	Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS	3-51
3.5.2.1	Addition procedure	3-51
3.5.2.2	Removal procedure	3-52
3.5.2.3	Swapping procedure	3-54
3.5.3	Hot plugging an HBA running with both PRIMECLUSTER GDS and ETERNUS multipath driver	3-55
3.5.3.1	Addition procedure	3-55
3.5.3.2	Removal procedure	3-56
3.5.3.3	Swapping procedure	3-57
3.6	Resource Names (Reference)	3-60
CHAPTER 4	Manual PSA Installation	4-1
4.1	Manual PSA installation (Linux: Red Hat) (PRIMEQUEST 580A/540A/580/540/480/440)	4-1
4.1.1	Installation Workflow	4-2
4.1.2	Preinstallation check items	4-3
4.1.2.1	Checking the management LAN settings	4-3
4.1.2.2	Checking the required functions for PSA operation	4-11
4.1.2.3	Checking the SELinux function settings	4-12
4.1.3	PSA installation	4-12
4.1.4	Items automatically set during PSA installation	4-13
4.1.5	Installing SIRMS	4-13
4.1.6	Rebooting the partition	4-13
4.1.7	Settings after PSA installation	4-13
4.1.7.1	Checking the firewall function (releasing ports)	4-14

4.1.7.2	Setting the destination of trap sending from the partition.	4-15
4.1.7.3	Setting the destinations of trap and e-mail sending via the MMB.	4-18
4.1.7.4	Other settings.	4-18
4.1.8	PSA update installation.	4-20
4.1.9	SIRMS update installation.	4-21
4.1.10	PSA uninstallation.	4-21
4.1.11	SIRMS uninstallation.	4-21
4.2	Manual PSA installation (Linux: Red Hat) (PRIMEQUEST 520A/520/420).	4-22
4.2.1	Installation Workflow.	4-23
4.2.2	Preinstallation check items.	4-24
4.2.2.1	Checking the management LAN settings.	4-24
4.2.2.2	Checking the required functions for PSA operation.	4-27
4.2.2.3	Checking the SELinux function settings.	4-29
4.2.3	PSA installation.	4-29
4.2.4	Items automatically set during PSA installation.	4-30
4.2.5	Installing SIRMS.	4-30
4.2.6	Rebooting the OS.	4-30
4.2.7	Settings after PSA installation.	4-30
4.2.7.1	Checking the firewall function (releasing ports).	4-31
4.2.7.2	Setting the destination of trap sending from the partition.	4-32
4.2.7.3	Setting the destinations of trap and e-mail sending via the MMB.	4-35
4.2.7.4	Other settings.	4-35
4.2.8	PSA update installation.	4-37
4.2.9	SIRMS update installation.	4-38
4.2.10	PSA uninstallation.	4-38
4.2.11	SIRMS uninstallation.	4-38
4.3	Manual PSA installation (Linux: SUSE) (PRIMEQUEST 500A/500/400 Series common).	4-39
4.3.1	Installation Workflow.	4-39
4.3.2	Preinstallation check items.	4-40
4.3.2.1	Checking the management LAN settings.	4-40
4.3.2.2	Procedures for monitoring syslog.	4-51
4.3.2.3	Checking the required functions for PSA operation.	4-56
4.3.2.4	SELinux function.	4-57
4.3.3	PSA installation.	4-57
4.3.4	Items automatically set during PSA installation.	4-57
4.3.5	Rebooting the partition.	4-57

4.3.6	Settings after PSA installation	4-58
4.3.6.1	Checking the firewall function (releasing ports)	4-58
4.3.6.2	Setting the destination of trap sending from the partition	4-59
4.3.6.3	Setting the destinations of trap and e-mail sending via the MMB	4-63
4.3.6.4	Other settings	4-63
4.3.7	PSA update installation	4-65
4.3.8	PSA uninstallation	4-66
4.4	Manual PSA Installation (Windows Server 2003) (PRIMEQUEST 580A/540A/580/540/480/440)	4-67
4.4.1	Installation Workflow	4-68
4.4.2	Preinstallation check items	4-69
4.4.2.1	Checking the management LAN settings	4-69
4.4.2.2	Verifying the services required for PSA operation	4-76
4.4.3	Installing PSA	4-77
4.4.4	Items automatically set during PSA installation	4-79
4.4.5	Settings after PSA installation	4-81
4.4.5.1	Setting the destination of trap sending from the partition	4-81
4.4.5.2	Setting the destinations of trap and e-mail sending via the MMB	4-82
4.4.5.3	Windows firewall setting	4-83
4.4.5.4	Setting Watchdog monitoring after a STOP error (a fatal system error) occurs	4-85
4.4.6	PSA update installation	4-86
4.4.7	PSA uninstallation	4-89
4.5	Manual PSA Installation (Windows Server 2003) (PRIMEQUEST 520A/520/420)	4-90
4.5.1	Installation Workflow	4-91
4.5.2	Preinstallation check items	4-92
4.5.2.1	Checking the management LAN settings	4-92
4.5.2.2	Verifying the services required for PSA operation	4-93
4.5.3	Installing PSA	4-94
4.5.4	Items automatically set during PSA installation	4-96
4.5.5	Settings after PSA installation	4-98
4.5.5.1	Setting the destination of trap sending from the partition	4-98
4.5.5.2	Setting the destinations of trap and e-mail sending via the MMB	4-99
4.5.5.3	Windows firewall setting	4-100
4.5.5.4	Setting Watchdog monitoring after a STOP error (a fatal system error) occurs	4-102

4.5.6	PSA update installation	4-103
4.5.7	PSA uninstallation	4-106
4.6	Manual PSA Installation (Windows Server 2008)	
	(PRIMEQUEST 580A/540A/580/540)	4-107
4.6.1	Installation Workflow	4-108
4.6.2	Preinstallation check items	4-109
4.6.2.1	Checking the management LAN settings	4-109
4.6.2.2	Verifying the services required for PSA operation	4-115
4.6.3	Installing PSA	4-116
4.6.4	Items automatically set during PSA installation	4-118
4.6.5	Settings after PSA installation	4-120
4.6.5.1	Setting the destination of trap sending from the partition.	4-120
4.6.5.2	Setting the destinations of trap and e-mail sending via the MMB	4-121
4.6.5.3	Windows firewall setting	4-122
4.6.5.4	Setting Watchdog monitoring after a STOP error (a fatal system error) occurs.	4-124
4.6.5.5	Installing the PSHED plug-in driver	4-125
4.6.6	PSA update installation	4-126
4.6.7	PSA uninstallation	4-131
4.7	Manual PSA Installation (Windows Server 2008)	
	(PRIMEQUEST 520A/520)	4-133
4.7.1	Installation Workflow	4-134
4.7.2	Preinstallation check items	4-135
4.7.2.1	Checking the management LAN settings	4-135
4.7.2.2	Verifying the services required for PSA operation	4-136
4.7.3	Installing PSA	4-137
4.7.4	Items automatically set during PSA installation	4-139
4.7.5	Settings after PSA installation	4-141
4.7.5.1	Setting the destination of trap sending from the partition.	4-141
4.7.5.2	Setting the destinations of trap and e-mail sending via the MMB	4-142
4.7.5.3	Windows firewall setting	4-143
4.7.5.4	Setting Watchdog monitoring after a STOP error (a fatal system error) occurs.	4-145
4.7.5.5	Installing the PSHED plug-in driver	4-146
4.7.6	PSA update installation	4-147
4.7.7	PSA uninstallation	4-152

CHAPTER 5	Physical Locations and Bus Numbers	5-1
5.1	Physical Locations and Bus Numbers of Built-in I/Os of PRIMEQUEST 580A/540A/580/540/480/440	5-1
5.2	Physical Locations and Bus Numbers of Built-in I/Os of PRIMEQUEST 520A/520/420	5-6
5.3	Physical Locations and Bus Numbers of PCI Slots of PRIMEQUEST 580A/540A/580/540/480/440	5-7
5.4	Physical Locations and Bus Numbers of PCI Slots of PRIMEQUEST 520A/520/420	5-15
CHAPTER 6	Management LAN Reconfiguration Required at the Time of BMM Replacement	6-1
6.1	Red Hat	6-2
6.1.1	For PRIMEQUEST 580A/540A/580/540/480/440 (bonding or GLS sharing)	6-2
6.1.2	For PRIMEQUEST 520A/520/420	6-5
6.2	SUSE 9	6-7
6.2.1	For PRIMEQUEST 580A/540A/580/540/480/440 (bonding in use)	6-7
6.2.2	For PRIMEQUEST 580A/540A/580/540/480/440 (GLS in use)	6-7
6.2.3	For PRIMEQUEST 520A/520/420	6-9
6.3	Windows Server 2003	6-11
6.3.1	For PRIMEQUEST 580A/540A/580/540/480/440	6-11
6.3.2	For PRIMEQUEST 520A/520/420	6-15
6.4	Procedure for Restoring Settings If the Network Adapter Name Is Changed	6-16
6.4.1	Confirming the Old Settings	6-16
6.4.2	Changing the Adapter Names	6-16
6.5	Action Required When Kudzu Starts Up	6-17
6.6	Notes on Startup in Linux Single-User Mode	6-19
CHAPTER 7	REMCS	7-1
7.1	Use of REMCS Service	7-1
7.1.1	Mode of connection to the REMCS Center	7-1
7.1.2	Service startup procedure	7-5
7.1.3	REMCS service operation procedure	7-26
7.1.4	Detail Setup of REMCS	7-40
7.1.5	REMCS messages	7-46
7.1.6	MMB log downloading	7-57
7.1.7	Notes on using the REMCS GUI	7-58

CHAPTER 8	Onboard GbE (Broadcom Ethernet) Network Configuration Under Windows Environment.	8-1
8.1	Outline (PRIMEQUEST 580A/540A/580/540/480/440)	8-1
8.1.1	Broadcom LiveLink settings	8-11
8.2	Outline (PRIMEQUEST 520A/520/420)	8-14
8.2.1	Broadcom LiveLink settings	8-21
8.3	Smart Load Balance Setting Procedure	8-25
8.4	Smart Load Balance LiveLink Setting Procedure	8-29
8.5	Generic Trunking (FEC/GEC) Setting Procedure	8-38
8.6	Link Aggregation (802.3ad) Setting Procedure	8-42
CHAPTER 9	MIB Tree Provided by PRIMEQUEST	9-1
CHAPTER 10	Status Confirmation from LED	10-1
10.1	LED Display on the Operator Panel	10-2
10.2	LED Display of Each Board or Component	10-3
10.2.1	LED display for each board or component	10-3
10.2.1.1	LED display of the MMB	10-4
10.2.1.2	LED display of a GTHB	10-5
10.2.2	Other boards	10-5
10.2.3	List of LED displays for different boards and components	10-6
10.2.4	LED display at power-on	10-14
10.2.5	Display function of HDD LEDs	10-15
10.2.6	Link-Act-LED display function of network interface	10-16
Appendix A	Alternative Key Combinations for Some Special Keys on Serial Terminals	A-1
Glossary	GL-1
Index	IN-1

Figures

Figure 1.1	Preventive replacement of hard disk	1-15
Figure 1.2	Outline of system information collection by fjsnap	1-25
Figure 1.3	Startup and Recovery dialog box	1-33
Figure 1.4	Detail Settings dialog box	1-35
Figure 1.5	Virtual Memory dialog box	1-36
Figure 1.6	[System Control Panel Applet] dialog box	1-37
Figure 1.7	Configuration example of device names	1-61
Figure 1.8	By-path name format	1-62
Figure 1.9	Example of ifcfg-eth<x> file	1-65
Figure 2.1	OP-Panel location (PRIMEQUEST 580A/540A/580/540/480/440)	2-2
Figure 2.2	SB locations (PRIMEQUEST 580A/540A/580/540/480/440)	2-3
Figure 2.3	MMB location (PRIMEQUEST 580A/540A/580/540/480/440)	2-4
Figure 2.4	GSWB location (PRIMEQUEST 580A/540A/580/540/480/440)	2-5
Figure 2.5	GTHB location (PRIMEQUEST 580A/540A/580/540)	2-6
Figure 2.6	IO Unit location (PRIMEQUEST 580A/540A/580/540/480/440)	2-7
Figure 2.7	XAI location (PRIMEQUEST 580A/540A/580/540/480/440)	2-8
Figure 2.8	XDI location (PRIMEQUEST 580A/540A/580/540/480/440)	2-9
Figure 2.9	CPCB location (PRIMEQUEST 580A/540A/580/540/480/440)	2-10
Figure 2.10	KVM location (PRIMEQUEST 580A/540A/580/540/480/440)	2-11
Figure 2.11	OP-Panel location (PRIMEQUEST 520A/520/420)	2-12
Figure 2.12	SB locations (PRIMEQUEST 520A/520/420)	2-13
Figure 2.13	MMB location (PRIMEQUEST 520A/520/420)	2-14
Figure 2.14	IO Unit location (PRIMEQUEST 520A/520/420)	2-15
Figure 2.15	IOX location (PRIMEQUEST 520A/520/420)	2-16
Figure 3.1	Addition of a virtual interface for making the added NICs (ethX, ethY) redundant	3-25
Figure 3.2	Removing NICs whose virtual interface makes them redundant (ethX, ethY)	3-31
Figure 3.3	Swapping a NIC whose virtual interface make it redundant (ethX)	3-35

Figure 3.4	Addition of HBA (FC card) and ETERNUS	3-46
Figure 3.5	Removal of HBA (FC card) and ETERNUS	3-47
Figure 3.6	Swapping of HBA (FA card) and ETERNUS	3-48
Figure 3.7	Path addition by HBA addition	3-51
Figure 3.8	HBA removal (multi-path configuration)	3-52
Figure 3.9	HBA swapping (multi-path configuration)	3-54
Figure 3.10	Adding a path to ETERNUS by adding an HBA	3-55
Figure 3.11	Removing an HBA constituting a multipath	3-56
Figure 3.12	Replacing an HBA constituting a multipath	3-59
Figure 4.1	Concept of management LAN duplication in PRIMEQUEST	4-6
Figure 4.2	Concept of management LAN duplication in PRIMEQUEST (a configuration characterized by improved reliability)	4-6
Figure 4.3	Concept of management LAN duplication in PRIMEQUEST	4-43
Figure 4.4	Concept of management LAN duplication in PRIMEQUEST (a configuration characterized by improved reliability)	4-44
Figure 4.5	Concept of management LAN duplication in PRIMEQUEST	4-47
Figure 4.6	Concept of management LAN duplication in PRIMEQUEST (configuration characterized by improved reliability)	4-47
Figure 4.7	YaST window	4-50
Figure 4.8	YaST start screen	4-51
Figure 4.9	Novell AppArmor- select screen	4-52
Figure 4.10	AppArmor Profile select screen	4-53
Figure 4.11	AppArmor Profile window	4-53
Figure 4.12	Entry addition and selection screen	4-54
Figure 4.13	Adding the Profiles Entry screen	4-54
Figure 4.14	Entry list screen	4-55
Figure 4.15	Saving the profiles screen	4-55
Figure 4.16	[Computer Management] window	4-71
Figure 4.17	[Teaming] tab	4-71
Figure 4.18	[New Team Wizard] window	4-72
Figure 4.19	List of network adapters	4-72
Figure 4.20	List of team mode	4-73
Figure 4.21	Selection Completed window	4-73
Figure 4.22	Team Number 0 Properties window	4-74
Figure 4.23	[Local Area Network Connection Properties] dialog box.	4-75
Figure 4.24	[Advanced] tab	4-75
Figure 4.25	Installation preparation window	4-77

Figure 4.26	Setup window	4-77
Figure 4.27	[Select Features] window	4-78
Figure 4.28	Installation completion window	4-78
Figure 4.29	[Add a Port] dialog box	4-83
Figure 4.30	[Add a Port] dialog box	4-84
Figure 4.31	Installation preparation window	4-86
Figure 4.32	Update installation window	4-86
Figure 4.33	Update completion window	4-87
Figure 4.34	Installation preparation window	4-87
Figure 4.35	[Detected previous version of PSA] window	4-88
Figure 4.36	Confirmation message window	4-89
Figure 4.37	Maintenance completion window	4-89
Figure 4.38	Installation preparation window	4-94
Figure 4.39	Installation window	4-94
Figure 4.40	[Select Features] window	4-95
Figure 4.41	Setup completion window	4-95
Figure 4.42	[Add a Port] dialog box	4-100
Figure 4.43	[Add a Port] dialog box	4-101
Figure 4.44	Installation preparation window	4-103
Figure 4.45	PRIMEQUEST Server Agent Update window	4-103
Figure 4.46	Update completion window	4-104
Figure 4.47	Installation preparation window	4-104
Figure 4.48	[Deleted previous version of PSA] window	4-105
Figure 4.49	Confirmation window	4-106
Figure 4.50	Maintenance completion window	4-106
Figure 4.51	[Computer Management] window	4-110
Figure 4.52	[Teaming] tab	4-111
Figure 4.53	[New Team Wizard] window	4-111
Figure 4.54	List of network adapters	4-112
Figure 4.55	List of team mode	4-112
Figure 4.56	Selection Completed window	4-113
Figure 4.57	Team Number 0 Properties window	4-113
Figure 4.58	[Local Area Network Connection Properties] dialog box	4-114
Figure 4.59	[Select Features] window	4-115
Figure 4.60	Installation preparation window	4-116
Figure 4.61	Installation window	4-116
Figure 4.62	[Select Features] window	4-117
Figure 4.63	[InstallShield Wizard Complete] window	4-117
Figure 4.64	[Windows Firewall Settings] dialog box	4-122
Figure 4.65	[Add a Port] dialog box	4-123

Figure 4.66	[Windows Security] dialog box	4-125
Figure 4.67	Installation preparation window	4-126
Figure 4.68	Update installation window	4-126
Figure 4.69	[Windows Security] dialog box	4-127
Figure 4.70	Update completion window	4-127
Figure 4.71	Installation preparation window	4-128
Figure 4.72	[Detected previous version of PSA] window	4-128
Figure 4.73	Update installation dialog box	4-129
Figure 4.74	[Select Features] dialog box	4-129
Figure 4.75	[Windows Security] dialog box	4-130
Figure 4.76	Update installation completion dialog box	4-130
Figure 4.77	Maintenance dialog box	4-131
Figure 4.78	Confirmation message dialog box	4-131
Figure 4.79	[Uninstall Complete] dialog box	4-132
Figure 4.80	[Select Features] window	4-136
Figure 4.81	Installation preparation window	4-137
Figure 4.82	Installation window	4-137
Figure 4.83	[Select Features] window	4-138
Figure 4.84	Installation completion window	4-138
Figure 4.85	[Windows Firewall Settings] dialog box	4-143
Figure 4.86	[Add a Port] dialog box	4-144
Figure 4.87	[Windows Security] dialog box	4-146
Figure 4.88	Installation preparation window	4-147
Figure 4.89	Update Installation window	4-147
Figure 4.90	[Windows Security] dialog box	4-148
Figure 4.91	Update completion window	4-148
Figure 4.92	Installation preparation window	4-149
Figure 4.93	[Deleted previous version of PSA] window	4-149
Figure 4.94	Update installation dialog box	4-150
Figure 4.95	[Select Features] dialog box	4-150
Figure 4.96	[Windows Security] dialog box	4-151
Figure 4.97	Update installation completion dialog box	4-151
Figure 4.98	Maintenance dialog box	4-152
Figure 4.99	Confirmation message dialog box	4-152
Figure 4.100	[Uninstall Complete] dialog box	4-153
Figure 6.1	[IOU#x] window (PRIMEQUEST 580A/540A/580/540/480/440)	6-2
Figure 6.2	IOU/IOX information window (PRIMEQUEST 520A/520/420)	6-5
Figure 6.3	Sample screenshot of YaST screen	6-8
Figure 6.4	[IOU] window (PRIMEQUEST 520A/520/420)	6-9

Figure 6.5	Network interface list	6-11
Figure 6.6	[Local Area Connection Properties] dialog box	6-12
Figure 6.7	[Device Manager] window	6-13
Figure 6.8	[Team #x Properties] dialog box	6-13
Figure 6.9	[Team Settings] dialog box	6-14
Figure 6.10	[Device Manager] window	6-14
Figure 6.11	[Welcome to Kudzu] screen	6-17
Figure 6.12	[Hardware Removed] screen	6-17
Figure 6.13	[Hardware Removed] screen	6-18
Figure 6.14	[Hardware Added] screen	6-18
Figure 6.15	[Hardware Added] screen	6-19
Figure 7.1	Internet Connection (using network connected to user port)	7-2
Figure 7.2	Internet connection (using REMCS port)	7-2
Figure 7.3	P-P connection	7-3
Figure 7.4	P-P (VPN) connection	7-4
Figure 7.5	Workflow for registration with the REMCS center	7-6
Figure 7.6	"Customer Information Registration Instructions" screen	7-8
Figure 7.7	"Selecting REMCS Center" screen	7-9
Figure 7.8	"Initial Settings" screen	7-10
Figure 7.9	"Internet (Mail Only) connection environment settings" screen	7-11
Figure 7.10	"Point-to-Point Connection environment settings" screen	7-13
Figure 7.11	"Restore from setting file" screen	7-14
Figure 7.12	[Connection check result] screen	7-15
Figure 7.13	"Information Transmit Agreement" screen (automatic setting)	7-16
Figure 7.14	"Automatic setting status" screen	7-17
Figure 7.15	"Periodical Connection settings" screen	7-18
Figure 7.16	"Customer Information" screen	7-19
Figure 7.17	"Customer Information Review" screen	7-21
Figure 7.18	"Information Transmit Agreement" screen	7-22
Figure 7.19	"Registration result" screen	7-23
Figure 7.20	Connection check" screen	7-24
Figure 7.21	"Result of connection check" screen	7-25
Figure 7.22	"REMCS operation" screen	7-26
Figure 7.23	"A setup of an environment of the Internet (Only mail)" screen	7-29
Figure 7.24	"Point-to-Point Connection environment settings" screen	7-30

Figure 7.25	"Periodical Connection settings" screen	7-31
Figure 7.26	"Backup file setting" screen	7-32
Figure 7.27	"Initial Settings" screen during operation	7-33
Figure 7.28	[Connection check] screen	7-34
Figure 7.29	"Result of connection check" screen	7-35
Figure 7.30	"Temporary Disconnection" screen	7-36
Figure 7.31	"Reconnection" screen	7-37
Figure 7.32	"Sending Hardware Configuration Information" screen	7-38
Figure 7.33	"Sending Software Configuration Information" screen	7-39
Figure 7.34	"REMCS FE operation" screen	7-40
Figure 7.35	"Environment settings" screen (POP Before SMTP authentication)	7-41
Figure 7.36	"Environment settings" screen (other than POP Before SMTP authentication)	7-41
Figure 7.37	"Selecting REMCS Center" screen	7-43
Figure 7.38	"Select language (Japanese or English)" screen	7-44
Figure 7.39	"Select to Display Machine ID or Machine Unique Name" screen	7-45
Figure 7.40	REMCS message screen	7-58
Figure 8.1	Broadcom Ethernet configuration (GSWB interface)	8-3
Figure 8.2	Physical positions of Ethernet ports	8-4
Figure 8.3	[Broadcom Advanced Control Suite 2] dialog window	8-4
Figure 8.4	Notes on team setting (BACS setting) (PRIMEQUEST 580A/540A/580/540/480/440)	8-5
Figure 8.5	Example 1 of Smart Load Balance (SLB) configuration	8-6
Figure 8.6	Example 2 of Smart Load Balance (SLB) configuration	8-7
Figure 8.7	Example 3 of Smart Load Balance (SLB) configuration	8-8
Figure 8.8	Example 1 of Smart Load Balance (SLB + LiveLink) configuration	8-9
Figure 8.9	Example 2 of Smart Load Balance (SLB + LiveLink) configuration	8-10
Figure 8.10	Broadcom LAN information of IO unit	8-12
Figure 8.11	Example of Generic Trunking (GEC/FEC) configuration	8-13
Figure 8.12	Physical positions of Ethernet ports (PRIMEQUEST 520A/520/420)	8-16
Figure 8.13	[Broadcom Advanced Control Suite 2] dialog box	8-16
Figure 8.14	Example 1 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)	8-17
Figure 8.15	Example 2 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)	8-18

Figure 8.16	Example 1 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)	8-19
Figure 8.17	Example 2 of Smart Load Balance (SLB + LiveLink) configuration (PRIMEQUEST 520A/520/420)	8-20
Figure 8.18	Broadcom LAN information of IO unit	8-22
Figure 8.19	Example of Generic Trunking (GEC/FEC) configuration (PRIMEQUEST 520A/520/420)	8-23
Figure 8.20	Example of Link Aggregation (802.3ad) configuration (PRIMEQUEST 520A/520/420)	8-24
Figure 8.21	Starting Broadcom Advanced Control Suite 2	8-25
Figure 8.22	[Broadcom Advanced Control Suite 2] window	8-25
Figure 8.23	[Create Teams] dialog box	8-26
Figure 8.24	[Create Teams] dialog box	8-26
Figure 8.25	Message dialog box	8-27
Figure 8.26	[Broadcom Advanced Control Suite 2] window	8-27
Figure 8.27	[Network connections] window	8-28
Figure 8.28	Starting Broadcom Advanced Control Suite 2	8-29
Figure 8.29	[Broadcom Advanced Control Suite 2] window	8-29
Figure 8.30	[Create Teams] dialog box	8-30
Figure 8.31	[Create Teams] dialog box	8-30
Figure 8.32	Message dialog box	8-31
Figure 8.33	[Broadcom Advanced Control Suite 2] window	8-31
Figure 8.34	[Broadcom Advanced Control Suite 2] window	8-32
Figure 8.35	[LiveLink setting] dialog box	8-32
Figure 8.36	[LiveLink setting] dialog box	8-33
Figure 8.37	[LiveLink] dialog box	8-33
Figure 8.38	[LiveLink setting] dialog box	8-34
Figure 8.39	[LiveLink] dialog box	8-34
Figure 8.40	[LiveLink setting] dialog box	8-35
Figure 8.41	[Broadcom Advanced Control Suite 2] window	8-35
Figure 8.42	[Broadcom Advanced Control Suite 2] dialog box	8-36
Figure 8.43	[Broadcom Advanced Control Suite 2] window	8-36
Figure 8.44	[Broadcom Advanced Control Suite 2] window	8-36
Figure 8.45	[Network connections] window	8-37
Figure 8.46	Starting Broadcom Advanced Control Suite 2	8-38
Figure 8.47	[Broadcom Advanced Control Suite 2] window	8-38
Figure 8.48	[Create Teams] dialog box	8-39
Figure 8.49	[Create Teams] dialog box	8-39
Figure 8.50	[Broadcom Advanced Control Suite 2] dialog box	8-40
Figure 8.51	[Broadcom Advanced Control Suite 2] window	8-40
Figure 8.52	[Network connections] window	8-41

Figure 8.53	Starting Broadcom Advanced Control Suite 2	8-42
Figure 8.54	[Broadcom Advanced Control Suite 2] dialog box	8-42
Figure 8.55	[Create Teams] dialog box	8-43
Figure 8.56	[Create Teams] dialog box	8-43
Figure 8.57	Message dialog box	8-44
Figure 8.58	[Broadcom Advanced Control Suite 2] window (Display of virtual adapters)	8-44
Figure 8.59	[Network connections] window	8-45
Figure 10.1	LEDs on the operator panel	10-2
Figure 10.2	LEDs of the MMB	10-4
Figure 10.3	LED display of the GTHB	10-5
Figure 10.4	LEDs of other boards	10-5
Figure 10.5	Example of network interface connection	10-16

Tables

Table 1.1	Tools available to Software Support Guide and information collected by the tools.	1-27
Table 1.2	Information collection.	1-28
Table 1.3	Information check list.	1-30
Table 1.4	Modes and sizes of memory dump	1-32
Table 1.5	Commands and files with awareness of device names.	1-63
Table 3.1	GLS hot plug support.	3-23
Table 3.2	Optional item in kudzu (8) window.	3-24
Table 4.1	secLevel settings.	4-16
Table 4.2	secLevel settings.	4-33
Table 4.3	secLevel settings.	4-60
Table 5.1	Correspondence between physical locations and bus numbers of built-in I/Os (PCI Segment mode).	5-1
Table 5.2	Correspondence between physical locations and bus numbers of built-in I/Os (PCI Bus mode).	5-3
Table 5.3	Correspondence between physical locations and bus numbers of built-in I/Os (PCI Bus mode).	5-6
Table 5.4	Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI segment mode)	5-7
Table 5.5	Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI Bus mode).	5-12
Table 5.6	Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI Bus mode).	5-15
Table 6.1	Correspondence between management LAN NICs	6-3
Table 6.2	Explanation of boot command line options	6-19
Table 7.1	Customer information entry items	7-20
Table 7.2	Explanation of items on REMCS initial screen	7-26
Table 7.3	Explanation of items on FE operation initial screen.	7-40
Table 7.4	Explanation of items on environment detail setting screen	7-42
Table 7.5	Messages on initial setting screen.	7-46
Table 7.6	Messages on setting information restoration screen.	7-46
Table 7.7	Messages on automatic-setting result screen	7-47
Table 7.8	Messages on environment setting (Internet - mail only) screen.	7-47
Table 7.9	Messages on environment setting (P-P) screen	7-48
Table 7.10	Messages on periodic-connection scheduling screen	7-49
Table 7.11	Messages on customer information screen.	7-50
Table 7.12	Messages on customer information screen.	7-51
Table 7.13	Messages on agreement item screen for information transmission	7-51
Table 7.14	Messages on registration result screen.	7-51

Table 7.15	Messages on setting information backup screen.....	7-52
Table 7.16	Messages on connection check screen.....	7-52
Table 7.17	Messages on connection check result screen.....	7-53
Table 7.18	Messages on stop/restart center connection screen.....	7-53
Table 7.19	Messages on hardware configuration information transmission screen.....	7-53
Table 7.20	Messages on software configuration information transmission screen.....	7-53
Table 7.21	Messages on environment detail setting screen.....	7-54
Table 7.22	Messages on connection-destination center change screen.....	7-54
Table 7.23	Communication error messages (SMTP communication).....	7-55
Table 10.1	LED list (PRIMEQUEST 580A/540A/580/540/480/440).....	10-6
Table 10.2	LED list (PRIMEQUEST 520A/520/420).....	10-10
Table 10.3	LED Display of the operator panel (cabinet) and MMB.....	10-14
Table 10.4	LED display of an HDD (PRIMEQUEST 580A/540A/580/540/480/440).....	10-15
Table 10.5	LED display of an HDD (PRIMEQUEST 520A/520/420).....	10-15
Table 10.6	Link-Act-LED display of network interface.....	10-16
Table A.1	Special keys and their alternatives.....	A-1

CHAPTER 1 System Maintenance

1.1 System Maintenance

This section explains the following for system maintenance.

- [Notes on the Maintenance of PCI Cards \(→ 1.2\)](#)
- [Hot Swapping of Hard Disk \(→ 1.3\)](#)
- [REMCS Service \(→ 1.4\)](#)
- [Collecting Maintenance Data \(Linux\) \(→ 1.5\)](#)
- [Collecting Maintenance Data \(Windows Server 2003\) \(→ 1.6\)](#)
- [Setting Dump Environments \(Windows Server 2003\) \(→ 1.7\)](#)
- [Backup and Restoration \(→ 1.8\)](#)

1.2 Notes on the Maintenance of PCI Cards

When a PCI card is replaced, the setting information for this PCI card also needs to be set again.

When an FC card is swapped

When an FC card to which the boot device is connected is swapped, use the procedure described in Appendix D, "Installation of SAN Boot Environment," of the *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN) to set the boot device for the replaced FC card.

Also, perform the required settings of the FC card according to the manuals for the FC switch and storage devices to be connected.

When an SCSI card is swapped

No work is required.

When a LAN card is swapped

As for the setup file of the operating system containing LAN card-specific information (e.g. MAC address), modify its contents so that it accords with the replaced LAN card.

1.3 Hot Swapping of Hard Disk

Remarks:

Only the Linux OS supports this operation.

This function provides support for hot-swapping hardware resources on a partition. When a system maintenance contract is concluded, a certified service engineer replaces the hard disk.

The SCSI controller of a hard disk used on the PRIMEQUEST has a SAF-TE (SCSI Accessed Fault-Tolerant Enclosure) function that turns on/off the power of the disk and inserts and removes the disk. PSA has SAF-TE operator commands to enable safe maintenance by using the SAF-TE function for hardware error detection, disk replacement, and disk extension.

Notes:

- When the PRIMEQUEST hard disk is hot-swapped or hot-expanded, inserting the hard disk does not supply power to it. The SAF-TE operator command must be used to turn on the power.
- The operation does not apply to a RAID unit. See the manual for each device used for details on replacing the hard disk of the RAID unit.
- When the hard disk is replaced with this command, the following message may be displayed, but there is no negative impact on the operation.

```
kernel: mptscsih: ioc0: >> Attempting bus reset!  
(sc=e000004082adc480)  
kernel: mptbase: ioc0: IOCStatus(0x0048): SCSI Task Terminated
```

- If the power must be turned off, i.e., suppose the hard disk has been inserted in an incorrect location, wait about 60 seconds before turning off the power. If the power is immediately turned off, HotPlug processing by the OS is executed and the following message may be displayed.

```
kernel: Device sdb not ready.  
kernel: end_request: I/O error, dev sdb, sector 204706  
kernel: Buffer I/O error on device sdb1, logical block 6396
```

- If PSA starts during SAF-TE operation command execution, PSA operation unpredictable. Start PSA after that command execution is completed.

- Using the SAF-TE operator command to execute multiple operations at the same time may cause the system to terminate abnormally. Retry executing this command after verifying that it is not being used to execute multiple operations at the same time.

The following operations can be performed with the SAF-TE operator command. See Section 8.2, "SAF-TE Operation Command (diskctrl)" in the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN) for details.

- Display of SAF-TE devices and hard disks managed by them
- Hard disk power-on/power-off
- Hard disk location LED ON/OFF

1.3.1 Addition, removal, replacement, and location check of hard disks

This section explains the procedure for adding, removing, replacing a hard disk, and checking a location of it by using the SAF-TE operator command, with an operation example of an IO Unit internal hard disk. The device names displayed with the SAF-TE operator command are /dev/sgx (SAF-TE device) and /dev/sdx (hard disk).

1.3.1.1 Procedure for addition

- 1 Insert a hard disk in an empty slot in the IO Unit
- 2 Use the status display with the SAF-TE operator command to check the location where the hard disk is inserted.

```
# /opt/FJSPsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 /dev/sdc      Power-on      Fault LED-Off
  1 --mount      Not Activated  Fault LED-Off
```

An item with "Not Activated" displayed refers to the inserted hard disk. It is also indicated that the hard disk is inserted in slot 1 of /dev/sg1.

Note: If a hard disk is inserted in the IO Unit of the PRIMEQUEST 520A/520/420, "none" is displayed instead of "Not Activated."

The following is an example of the display when the hard disk is inserted in slot 1 of /dev/sg1:

```
# /opt/FJSVpsa/bin/diskctrl -l  
/dev/sg1  
0 none  
1 none
```

Accordingly, identify the slot into which the hard disk is inserted by using the following procedure.

- (i) Use the the SAF-TE operation command location display function to cause the Fault LED to blink.

```
# /opt/FJSVpsa/bin/diskctrl -i /dev/sg1/1
```

- (ii) Confirm that the Fault LED for the slot into which the hard disk is inserted is blinking.

If the slot location is correct, execute the operation indicated in step (iv).

If the slot location is incorrect, execute the operation indicated in step (iii).

- (iii) Use the SAF-TE operation command location turnoff function to turn off the blinking Fault LED.

```
# /opt/FJSVpsa/bin/diskctrl -o /dev/sg1/1
```

Specify another slot and repeat steps (i) through (ii) until the correct slot locations have been verified.

- (iv) Use the SAF-TE operation command status display function verify that "Fault LED-Identify" is being displayed for a slot. Then proceed to the processing in step 3.

```
# /opt/FJSVpsa/bin/diskctrl -l  
/dev/sg1  
0 none  
1 none Power-Off Fault LED-Identify
```

- 3 Turn on the power with the SAF-TE operator command.

Power-on processing by the SAF-TE operator command turns on the power to the hard disk and requests the OS to scan the hard disk.

```
# /opt/FJSVpsa/bin/diskctrl -c /dev/sg1/1
```

Check the status of the added hard disk with the SAF-TE operator command.

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 /dev/sdc      Power-On      Fault LED-Off
  1 /dev/sdd      Power-On      Fault LED-Off
```

Note:

Manually execute the command below for PSA in the following cases:

- Hot maintenance of a hard disk is performed when using SUSE.
- Hot maintenance of a hard disk of PRIMECLUSTER GDS is performed when using Red Hat.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

1.3.1.2 Procedure for removal

This section explains the procedure, assuming that the removal of sdc is necessary.

- 1 If a hard disk to be removed includes a partition specified in each of the diskdump, raw, and swap devices, perform the operations described below.
Note: Because kdump instead of diskdump is used in Red Hat Enterprise Linux 5 (for Itanium), information on diskdump is not covered.

- When a diskdump device is included

If the hard disk to be removed includes a partition specified in the diskdump device, the following procedure is required before hot swapping.

- 1) Confirm that the diskdump service is active.

Execute the following command and confirm that "diskdump enabled" is displayed.

```
# service diskdump status
diskdump enabled
PRESERVEDUMP not enabled
```

- 2) Confirm that the partition included in the hard disk to be removed is specified in the diskdump dump device.

Execute the following command and confirm that the partition name (sdc1) included in the hard disk to be removed is displayed.

```
# cat /proc/diskdump

# sample_rate: 8
# block_order: 2
# fallback_on_err: 1
# allow_risky_dumps: 1
# dump_level: 0
# compress: 0
# total_blocks: 2095237
#
sdc1 4001792 18526208
```

3) Stop the diskdump service.

To stop the diskdump service, the fefpcl driver service, which is dependent on the diskdump service, must also be stopped. Stop both services by taking the following steps.

First, execute the following command to stop the fefpcl driver service.

```
# service y20FJSVfefpcl force-stop
Unloading panicforpcl driver: [ OK ]
Unloading fefpcl driver: [ OK ]
Force Stopping FJSVfefpcl:[ OK ]
```

Next, execute the following command to stop the diskdump service.

```
# service diskdump stop
```

4) Confirm that the diskdump service has stopped.

Execute the following command and confirm that "diskdump not enabled" is displayed.

```
# service diskdump status
diskdump not enabled
```

Note: While the diskdump service is inactive, bear in mind the following:

- If a system error such as panic occurs, dump collection by diskdump is not enabled because diskdump is inactive. Since the system error cannot be investigated in this state, reassign as soon as possible another disk as the dump device for diskdump, and then restart the diskdump service. For the procedure for reassigning the dump device for diskdump, see the *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN).
- Even if a system error such as panic occurs, the system partition status does not switch to "Panic," and cluster switching is delayed.
- When a raw device is included
If the hard disk to be removed includes a partition used in the raw device, first quit all applications that may raw-access that partition and then remove the hard disk.
- When a swap device is included
If the hard disk to be removed includes a partition specified in the swap device, remove the hard disk after shutting down the system.

- 2 Perform the following operations, depending on whether a hard disk to be removed has a mirroring configuration in the PRIMECLUSTER GDS.
 - With mirroring configuration in PRIMECLUSTER GDS
Select the DISK to be removed from the PRIMECLUSTER GDS and remove it. See the PRIMECLUSTER GDS manuals for details on operating PRIMECLUSTER GDS.
 - Without the mirroring configuration in PRIMECLUSTER GDS
Demount all the disk partitions that are mounted by the hard disk to be removed.

```
# umount /dev/sdc1
# umount /dev/sdc2
      .
      .
      .
```

Note: The partition used by each of the diskdump, raw, and swap devices does not need to be dismounted. However, the diskdump, raw device, and swap device settings for the removed device must be changed.

- 3 Turn off the power with the SAF-TE operator command. Power-off processing by the SAF-TE operator command turns off the power to the hard disk, turns on the Fault LED (amber), and requests the OS to delete "sdc."

```
# /opt/FJSVpsa/bin/diskctrl -e /dev/sdc
```

- 4 Remove the hard disk in the location where the Fault LED (amber) is ON. When the built-in hard disk of the PRIMEQUEST580A/540A/580/540/480/440 is removed, the Fault LED, which is located deep in the slot, starts blinking. The Fault LED remains on or continues blinking unless the partition is shut down or rebooted, or the power is turned off by using the SAF-TE operator command. To turn out the Fault LED, use the SAF-TE operation command as follows:
 - 1) Display the status of the hard disk with the SAF-TE operator command, and find the location where the Fault LED is ON.

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 none         Power-Off     Fault LED-On
  1 /dev/sdd      Power-On      Fault LED-Off
```

In the above example, the Fault LED is ON at slot 0 of /dev/sg1, where sdc was surveyed.

- 2) Turn off the Fault LED with the following SAF-TE operator command.

```
# /opt/FJSVpsa/bin/diskctrl -o /dev/sg1/0
```

The Fault LED is turned off, and when the status is displayed with the SAFTE operator command, "none" is displayed at slot 0 of /dev/sg1, indicating that the slot is empty.

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 none
  1 /dev/sdd      Power-On      Fault LED-Off
```

Note:

Manually execute the command below for PSA in the following cases:

- Hot maintenance of a hard disk is performed when using SUSE.
- Hot maintenance of a hard disk of PRIMECLUSTER GDS is performed when using Red Hat.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

1.3.1.3 Procedure for replacement (Except for failures in which the hard disk fails to respond)

If a hard disk failure occurs and the driver cannot perform recovery from the failure, the PSA turns on the Fault LED (amber).

- 1 If a hard disk to be swapped includes a partition specified in each of diskdump, raw, and swap devices, perform the operations described below.

Note: Because kdump is used instead of diskdump in Red Hat Enterprise Linux 5 (for Itanium), information on diskdump is not covered.

- When a diskdump device is included

If the hard disk to be removed includes a partition specified in the diskdump dump device, the following procedure is required before hot swapping.

- 1) Confirm that the diskdump service is active.

Execute the following command and confirm that "diskdump enabled" is displayed.

Remarks: If "diskdump not enabled" is displayed, proceed to the step 2.

```
# service diskdump status
diskdump enabled
PRESERVEDUMP not enabled
```

- 2) Confirm that the partition included in the hard disk to be removed is specified in the diskdump dump device.

Execute the following command and confirm that the partition name (sdc1) included in the hard disk to be removed is displayed.

```
# cat /proc/diskdump

# sample_rate: 8
# block_order: 2
# fallback_on_err: 1
# allow_risky_dumps: 1
# dump_level: 0
# compress: 0
# total_blocks: 2095237
#
sdc1 4001792 18526208
```


3) Stop the diskdump service.

To stop the diskdump service, the fefpcl driver service, which is dependent on the diskdump service, must also be stopped. Stop both services by taking the following steps.

First, execute the following command to stop the fefpcl driver service.

```
# service y20FJSVfefpcl force-stop
Unloading panicforpcl driver: [ OK ]
Unloading fefpcl driver: [ OK ]
Force Stopping FJSVfefpcl:[ OK ]
```

Next, execute the following command to stop the diskdump service.

```
# service diskdump stop
```

4) Confirm that the diskdump service has stopped.

Execute the following command and confirm that "diskdump not enabled" is displayed.

```
# service diskdump status
diskdump not enabled
```

- When a raw device is included

If the hard disk to be removed includes a partition used in the raw device, first quit all applications that may raw-access that partition and then remove the hard disk.

- When a swap device is included

If the hard disk to be removed includes a partition specified in the swap device, remove the hard disk after shutting down the system.

2 Perform the following operations, depending on whether a hard disk to be replaced has a mirroring configuration in the PRIMECLUSTER GDS.

1) With mirroring configuration in PRIMECLUSTER GDS

Select the DISK to be removed from the PRIMECLUSTER GDS and remove it. See the PRIMECLUSTER GDS manuals for details on operating PRIMECLUSTER GDS.

2) Without the mirroring configuration in PRIMECLUSTER GDS

Demount all the disk partitions that are mounted by the hard disk to be removed.

```
# umount /dev/sdc1
# umount /dev/sdc2
.
.
.
```

Note: The partition used by each of the diskdump, raw, and swap devices does not need to be dismounted.

- 3 Turn off the power with the SAF-TE operator command.
Power-off processing by the SAF-TE operator command turns off the power to the hard disk, turns on the Fault LED (amber), and requests the OS to delete the target hard disk.

```
# /opt/FJSPsa/bin/diskctrl -e /dev/sdc
```

Remove the hard disk at the location where the Fault LED (amber) is ON.

- 4 Display the status with the SAF-TE operator command and find the location where the Fault LED is ON.

```
# /opt/FJSPsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 --mount      Power-Off      Fault LED-On
  1 /dev/sdd      Power-On      Fault LED-Off
```

- 5 The Fault LED is ON at slot 0 of /dev/sg1, where the hard disk is inserted.
The power to the hard disk is turned on with the following SAF-TE operator command.

```
# /opt/FJSPsa/bin/diskctrl -c /dev/sg1/0
```

Confirm the location of the inserted hard disk by checking the status displayed by the SAF-TE operator command.

```
# /opt/FJSPsa/bin/diskctrl -l
/dev/sg0
  0 /dev/sda      Power-On      Fault LED-Off
  1 /dev/sdb      Power-On      Fault LED-Off
/dev/sg1
  0 /dev/sdc      Power-on      Fault LED-Off
  1 /dev/sdd      Power-on      Fault LED-Off
```

- 6 After the SAF-TE operator command is completed, mount the disk and, if it was in a mirroring configuration in PRIMECLUSTER GDS, add it to PRIMECLUSTER GDS.

Note:

Manually execute the command below for PSA in the following cases:

- Hot maintenance of a hard disk is performed when using SUSE.
- Hot maintenance of a hard disk of PRIMECLUSTER GDS is performed when using Red Hat.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

- 7 To restore all the diskdump and raw devices, perform the operations described below.

Note: Because kdump is used instead of diskdump in Red Hat Enterprise Linux 5 (for Itanium), information on diskdump is not covered.

- When a diskdump device is included

- 1) Initialize a partition specified in the diskdump dump device and check whether it is normal.

Mount the dump device in a proper directory. If mounting fails, the partition is initialized normally because it has no file system.

```
# mount /dev/sdb2 /mnt
FAT: bogus number of reserved sectors
mount: you must specify the filesystem type
```

When mounting succeeds, the partition specified in the dump device may be an unintended one. Check whether files in the mounted partition may be deleted. If no problem is found, dismount the partition.

```
# umount /dev/sdb2
```

- 2) Initialize the partition that is specified in the disk dump device.

```
# service diskdump initialformat
/dev/sdb2: [100.0%]
```

3) Start the diskdump service.

To start the diskdump service, the fefpcl driver service, which is dependent on the diskdump service, must also be started. Start both services by taking the following steps.

First, execute the following command to start the fefpcl driver service.

```
# service diskdump start
Starting diskdump: [ OK ]
```

Next, execute the following command to start the fefpcl driver service.

```
# service y20FJSVfefpcl start
Loading panicforpcl driver: [ OK ]
Loading fefpcl driver: [ OK ]
Wait until fefpcl driver is ready: [ OK ]
Setting fefpcl driver parameter: [ OK ]
Setting fefpcl driver additional parameter: [ OK ]
Starting FJSVfefpcl:[ OK ]
```

4) Confirm that the diskdump service has started.

Execute the following command and confirm that "diskdump enabled" is displayed.

```
# service diskdump status
diskdump enabled
PRESERVEDUMP not enabled
```

Note: While the diskdump service is inactive, bear in mind the following:

- If a system error such as a panic occurs, dump collection by diskdump is not enabled because diskdump is inactive. Since the system error cannot be investigated in this state, replace the hard disk as soon as possible, and then restart the diskdump service.
- Even if a system error such as a panic occurs, the system partition status does not switch to "Panic," and cluster switching is delayed.

- When a raw device is included

Make raw device settings according to the manual of an application that raw-accesses the post-swapping hard disk. After completing the settings, start the applications that were quit before the swapping.

Figure 1.1 shows the processing sequence for the preventive replacement of the hard disk.

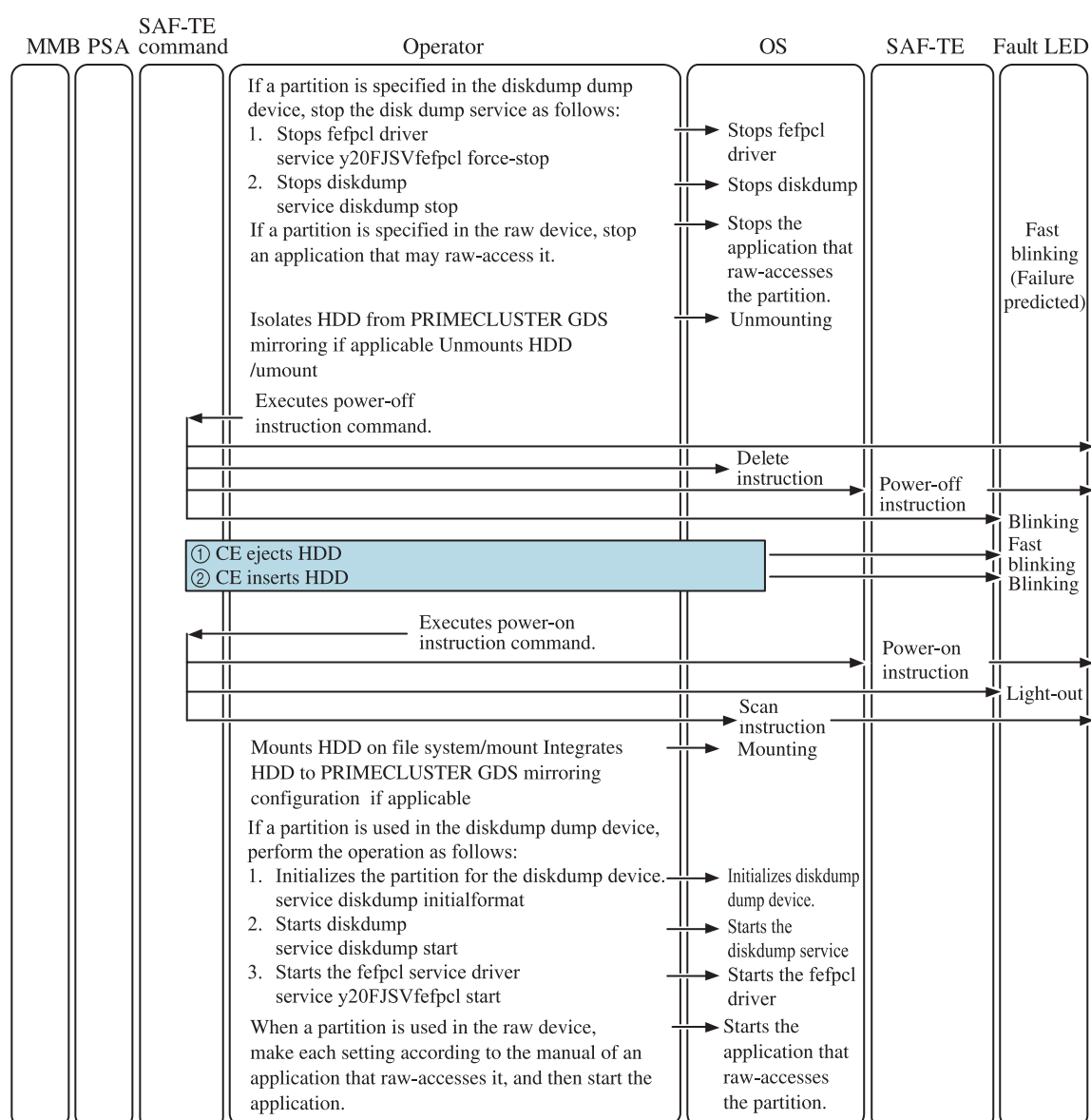


Figure 1.1 Preventive replacement of hard disk

1.3.1.4 Procedure for replacement (For failures in which the hard disk fails to respond)

This section explains the procedure for replacing the hard disk in cases where recovery using the driver is impossible owing to a non-responsive hard disk that has failed.

- 1 In the case of a hard disk no response error occurrence, the message below that is detected by the PSA is output, and the Fault LED goes on.
 - For Red Hat Enterprise Linux AS (v.4 for Itanium)
FJSVpsa: E 14056 IOU#n-HDD#n scsi:host %h channel %c id %i lun %l Device error (offlined) vendor=xxxxxxx model=xxxxxxx serial-no=xxxxxxxxxxx
 - For Red Hat Enterprise Linux 5 (for Itanium) and Novell SUSE LINUX Enterprise Server 10
FJSVpsa: E 14134 IOU#n-HDD#n scsi:host %h channel %c id %i lun %l Device error (offlined) vendor=xxxxxxx model=xxxxxxx serial-no=xxxxxxxxxxx
- * SCSI number: %h=host number, %c=channel number, %i=id number, %l=lun number
- 2 Confirm the disk state with the SAF-TE operator command. At this time, an offline error has occurred for a disk for which the Fault LED has gone on (*).

- RHEL4-AS4

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
    0 /dev/sda  Power-On  Fault LED-Off
    1 /dev/sdb  Power-On  Fault LED-Off
/dev/sg1
    0 --mount  Power-On  Fault LED-On    ← (*)
    1 /dev/sdd  Power-On  Fault LED-Off
```

- RHEL5/SUSE10

For PRIMEQUEST 580A/540A/580/540/480/440 IO unit built-in disk, or
PRIMEQUEST 520A/520/420 expansion file unit

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
    0 /dev/sda  Power-On  Fault LED-Off
    1 /dev/sdb  Power-On  Fault LED-Off
/dev/sg1
    0 /dev/sdc  Power-On  Fault LED-On    ← (*)
    1 /dev/sdd  Power-On  Fault LED-Off
```

For PRIMEQUEST 520A/520/420 IO unit built-in disk

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
    0 /dev/sda Power-On Fault LED-Off
    1 /dev/sdb Power-On Fault LED-Off
/dev/sg1
    0 --mount Power-On Fault LED-On ← (*)
    1 /dev/sdd Power-On Fault LED-Off
```

- 3 When replacing the PRIMEQUEST 520A/520/420 IO unit built-in disk, proceed to step 4. For any other cases, modify the offline state of the disk. Search for a directory on the basis of the SCSI number (host channel id lun) posted with the message in step 1, in the manner shown below.

cd/sys/class/scsi_host/host%h/device/target%h:%c:%i/%h:%c:%i:%l/
(*%h=host number, %c=channel number, %i=id number, %l=lun number)

```
Example: In the case of host0 channel0 id1 lun0
# cd /sys/class/scsi_host/host0/device/target0:0:1/0:0:1:0/

If the disk state is offline, place it in the running state.
Note that at this time, the disk will not enter the running state unless [running] is actually input.
# cat state                                ← state confirmation
offline
# echo running > state                     ← state change
# cat state
running
# cd                                       ← the path returns to default
```

- 4 If a hard disk to be swapped includes a partition specified in each of diskdump, raw, and swap devices, perform the operations described below.
Note: Because kdump is used instead of diskdump in Red Hat Enterprise Linux 5 (for Itanium), information on diskdump is not covered.

- When a diskdump device is included

If the hard disk to be removed includes a partition specified in the diskdump dump device, the following procedure is required before hot swapping.

- 1) Confirm that the diskdump service is active.

Execute the following command and confirm that "diskdump enabled" is displayed.

```
# service diskdump status
diskdump enabled
PRESERVEDUMP not enabled
```

- 2) Confirm that the partition included in the hard disk to be removed is specified in the diskdump dump device.

Execute the following command and confirm that the partition name (sdc1) included in the hard disk to be removed is displayed.

```
# cat /proc/diskdump

# sample_rate: 8
# block_order: 2
# fallback_on_err: 1
# allow_risky_dumps: 1
# dump_level: 0
# compress: 0
# total_blocks: 2095237
#
sdc1 4001792 18526208
```

- 3) Stop the diskdump service.

To stop the diskdump service, the fefpcl driver service, which is dependent on the diskdump service, must also be stopped. Stop both services by taking the following steps.

First, execute the following command to stop the fefpcl driver service.

```
# service y20FJSVfefpcl force-stop
Unloading panicforpcl driver: [ OK ]
Unloading fefpcl driver: [ OK ]
Force Stopping FJSVfefpcl:[ OK ]
```

Next, execute the following command to stop the diskdump service.

```
# service diskdump stop
```

- 4) Confirm that the diskdump service has stopped.

Execute the following command and confirm that "diskdump not enabled" is displayed.

```
# service diskdump status
diskdump not enabled
```

- When a raw device is included

If the hard disk to be removed includes a partition used in the raw device, first quit all applications that may raw-access that partition and then remove the hard disk.

- When a swap device is included

If the hard disk to be removed includes a partition specified in the swap device, remove the hard disk after shutting down the system.

- 5 Perform the following operations, depending on whether a hard disk to be replaced has a mirroring configuration in the PRIMECLUSTER GDS.
 - 1) With mirroring configuration in PRIMECLUSTER GDS
Select the DISK to be removed from the PRIMECLUSTER GDS and remove it. See the PRIMECLUSTER GDS manuals for details on operating PRIMECLUSTER GDS.
 - 2) Without the mirroring configuration in PRIMECLUSTER GDS
Demount all the disk partitions that are mounted by the hard disk to be removed.

```
# umount /dev/sdc1
# umount /dev/sdc2
.
.
.
```

Note: The partition used by each of the diskdump, raw, and swap devices does not need to be dismounted.

- 6 Turn off the power with the SAF-TE operator command. Specify the slot confirmed in step 1 and turn off the power.

```
# /opt/FJSVpsa/bin/diskctrl -e /dev/sg1/0
```

- 7 Confirm that the power is off. (*)

```
# /opt/FJSVpsa/bin/diskctrl -l

/dev/sg0
  0 /dev/sda  Power-On  Fault LED-Off
  1 /dev/sdb  Power-On  Fault LED-Off
/dev/sg1
  0 --mount   Power-Off Fault LED-On    ← (*)
  1 /dev/sdd  Power-On  Fault LED-Off
```

Note: For the PRIMEQUEST 520A/520/420 IO unit built-in disk, the "--mount" indication becomes "none."

- 8 Replace the hard disk where Fault LED (Amber) is on.
- 9 In the above example, you can confirm that the Fault LED of slot 0 for /dev/sg1 goes on and the hard disk is mounted there.

Turn on the power by using the following SAF-TE operator command.

```
# /opt/FJSVpsa/bin/diskctrl -c /dev/sg1/0
```

- 10 Confirm the location where the hard disk is mounted with the SAF-TE operator command state indication.

```
# /opt/FJSVpsa/bin/diskctrl -l
/dev/sg0
      0    /dev/sda    Power-On    Fault LED-Off
      1    /dev/sdb    Power-On    Fault LED-Off
/dev/sg1
      0    /dev/sdc    Power-On    Fault LED-Off
      1    /dev/sdd    Power-On    Fault LED-Off
```

- 11 After the SAF-TE operator command is completed, mount the disk and, if it was in a mirroring configuration in PRIMECLUSTER GDS, add it to PRIMECLUSTER GDS.

Note:

Manually execute the command below for PSA in the following cases:

- Hot maintenance of a hard disk is performed when using SUSE.
- Hot maintenance of a hard disk of PRIMECLUSTER GDS is performed when using Red Hat.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

- 12 To restore all the diskdump and raw devices, perform the operations described below.

Note: Because kdump is used instead of diskdump in Red Hat Enterprise Linux 5 (for Itanium), information on diskdump is not covered.

- When a diskdump device is included

- 1) Initialize a partition specified in the diskdump dump device and check whether it is normal.

Mount the dump device in a proper directory. If mounting fails, the partition is initialized normally because it has no file system.

```
# mount /dev/sdb2 /mnt
FAT: bogus number of reserved sectors
mount: you must specify the filesystem type
```

When mounting succeeds, the partition specified in the dump device may be an unintended one. Check whether files in the mounted partition may be deleted. If no problem is found, dismount the partition.

```
# umount /dev/sdb2
```

- 2) Initialize the partition that is specified in the disk dump device.

```
# service diskdump initialformat  
/dev/sdb2: [100.0%]
```

- 3) Start the diskdump service.

To start the diskdump service, the fefpcl driver service, which is dependent on the diskdump service, must also be started. Start both services by taking the following steps.

First, execute the following command to start the diskdump service.

```
# service diskdump start  
Starting diskdump: [ OK ]
```

Next, execute the following command to start the fefpcl driver service.

```
# service y20FJSVfefpcl start  
Loading panicforpcl driver: [ OK ]  
Loading fefpcl driver: [ OK ]  
Wait until fefpcl driver is ready: [ OK ]  
Setting fefpcl driver parameter: [ OK ]  
Setting fefpcl driver additional parameter: [ OK ]  
Starting FJSVfefpcl:[ OK ]
```

- 4) Confirm that the diskdump service has started.

Execute the following command and confirm that "diskdump enabled" is displayed.

```
# service diskdump status  
diskdump enabled  
PRESERVEDUMP not enabled
```

Note: While the diskdump service is inactive, bear in mind the following:

- If a system error such as a panic occurs, dump collection by diskdump is not enabled because diskdump is inactive. Since the system error cannot be investigated in this state, replace the hard disk as soon as possible, and then restart the diskdump service.
- Even if a system error such as a panic occurs, the system partition status does not switch to "Panic," and cluster switching is delayed.
- When a raw device is included
Make raw device settings according to the manual of an application that raw-accesses the post-swapping hard disk. After completing the settings, start the applications that were quit before the swapping.

1.4 REMCS Service

This section provides an overview of the REMCS service. Items to use the REMCS service are made by the certified service engineer. See [CHAPTER 7, "REMCS"](#) for details on operating the REMCS agent.

1.4.1 Overview of REMCS service

REMCS function

REMCS (remote customer support system) connects a user server to the REMCS Center via the Internet, sends server configuration information, and then automatically reports an error to promptly respond to and solve the trouble.

The REMCS functions in the PRIMEQUEST are implemented with the following components.

- MMB: Collection of server system hardware configuration information, error detection, and reporting to REMCS Center
- PSA: Collection of configuration information of the PCI cards and SCSI devices recognized in a partition and error detection
- SIRMS: Linux (Red Hat): Collection of software configuration information
Windows: Collection of software configuration information, collection of trouble-shooting information on a software error
(SIRMS support Windows in Japan only.)

The MMB communicates with the REMCS Center. The MMB collects information from the individual partitions and sends it to the REMCS Center.

To receive the REMCS service, the user has to sign the SupportDesk Product Basic Service contract. Without signing the contract, the user can register in the REMCS Center but cannot receive the service. For the SupportDesk Product Basic Service, ask your service representatives.

REMCS functions

- Configuration information monitoring
REMCS detects changes in the hardware and software configurations, and reports the latest configuration information to the REMCS Center.
- Error report
If a server hardware error occurs, REMCS automatically reports the error to the REMCS Center and simultaneously transfers error information, including a log, to the center. REMCS does not perform automatic monitoring for software errors. Once a hardware error is detected and reported, any errors detected in the same unit are not reported to the REMCS Center. This suppression of reporting for PSA-detected events is canceled when the operating system is rebooted or when PSA is stopped and restarted. If an error with a notification level higher than an event that is being suppressed in the same location occurs during notification suppression, the system is notified even it is within the suppression interval. In this case, the notification suppression continues with the suppression interval reduced to 0.
- Periodic connection
REMCS automatically connects to the REMCS Center as scheduled (see [Item \(4\)](#), "[Setting up a periodic connection schedule](#)," in [Section 7.1.2](#)) to verify the communication path, and check whether REMCS Agent is alive.

Installing the REMCS function

The REMCS function (REMCS Agent) of the PRIMEQUEST consists of PSA and SIRMS that are installed on the MMB and partition. The PRIMEQUEST is shipped with the REMCS Agent function installed on the MMB. For the PSA and SIRMS installation procedures, see the *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN). SIRMS is automatically installed when PSA is installed.

1.4.2 Supported connection modes

PRIMEQUEST supports only the following connection modes, each of which uses only SMTP to communicate with the REMCS Center.

- Internet connection (e-mail)
Mode to communicate with the REMCS Center via the Internet
- P-P connection (ISDN: e-mail)
Mode to communicate with the REMCS Center in a point-to-point (P-P) connection method using ISDN
- P-P connection (VPN: e-mail)
Mode to communicate with the REMCS Center in a point-to-point (P-P) connection using broadband, such as ADSL

1.5 Collecting Maintenance Data (Linux)

The fjsnap tool collects system information (hardware and software configuration information, environment settings, operation information, definition information, etc.) required for troubleshooting. The system administrator is requested to send the system information file collected with fjsnap to a Fujitsu certified service engineer. Fujitsu uses that information to locate the cause of the system trouble.

The following shows an outline of using fjsnap to collect system information.

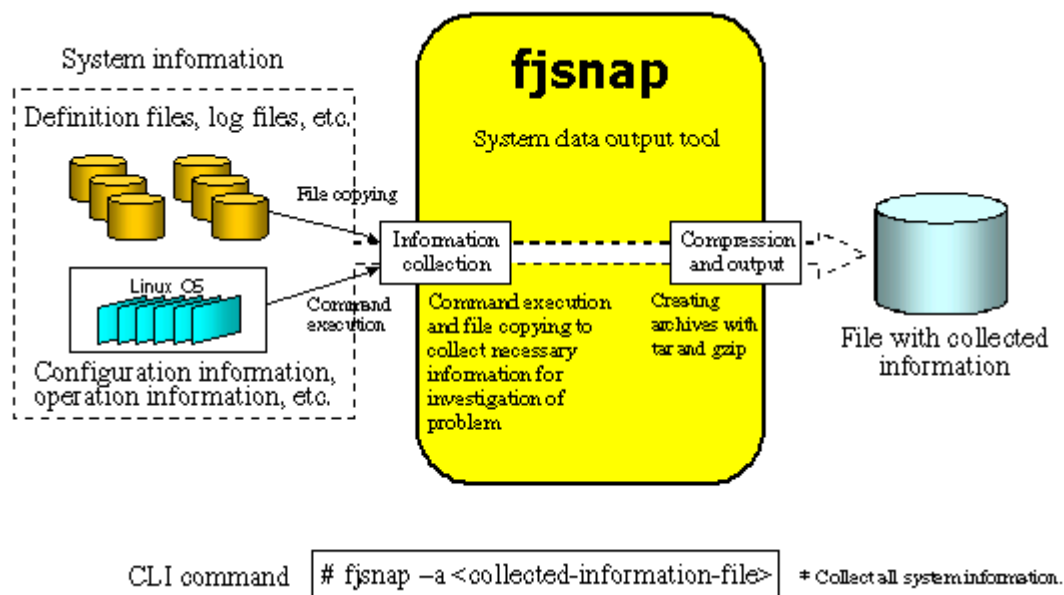


Figure 1.2 Outline of system information collection by fjsnap

The system administrator logs in to the partition with super-user privilege and executes the following command to collect the system information. (When the collected information file is output to /tmp/fjsnap.tar.gz)

```
# /usr/sbin/fjsnap -a /tmp/fjsnap.tar.gz
```

See the *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs* (C122-E004EN) for details on using the fjsnap tool.

1.6 Collecting Maintenance Data (Windows Server 2003)

1.6.1 Early troubleshooting [DSNAP]

DSNAP is software that quickly collects accurate information at one time from examinations after the Windows OS encounters a problem. If a problem occurs in your system, your Fujitsu certified engineer uses this software to correctly find out your system software configuration and setting states and conduct smooth examinations of processes.

- Installation method

See Section 3.3.4, "High-reliability Tools," in Chapter 3, "Operating System Installation," in the *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN).

- Use method

Refer to [OS Install Drive]: \DSNAP README.TXT file.

1.6.2 Software Support Guide

Software Support Guide is a set of software used to quickly and securely collect troubleshooting information at one time if a software error occurs in the Windows operating system.

If a problem occurs in the customer's system, a Fujitsu certified service engineer uses such information to get an exact understanding of the customer's system software configuration and settings and promote a smooth investigation.

Software Support Guide uses accompanying tools to collect the following types of information to enable quick troubleshooting.

Table 1.1 Tools available to Software Support Guide and information collected by the tools.

Tool name	Collected information
Quick Support System (QSS)	Registries, event log, system files, Watson log, mini dumps, and MSCS cluster log
Event Trace for Windows (ETW)	OS standard trace function Process/thread, disk, and network traces can be used. (ETW must be started after installation of Software Support Guide.)
User Mode Process Dumper	Application (snapshot) dump
Desktop Heap Monitor	Information on the size of the desktop heap, which is a system resource

Start Software Support Guide to check for further details.

1.6.2.1 Collecting information with Software Support Guide

Software Support Guide is an aggregate set of troubleshooting tools including QSS. This section first explains the Software Support Guide functions and then uses an example of a software problem to explain how to collect information.

(1) Software Support Guide functions

Software Support Guide uses the following tools and functions to provide quick solutions to system problems:

- 1 Quick Support System (QSS), a collection tool
QSS collects basic information required for quick troubleshooting.

Table 1.2 Information collection

Collected information		Description
1	Event log	An application log and system log are collected in EVT or CSV format.
2	Registry information	System registry information is collected.
3	System file information	System file list information is collected.
4	System information	System information (such as the size of installed memory) is collected.
5	Minimum memory dump	A minimum memory dump is collected only if it has been created.
6	Microsoft Cluster Service (MSCS) information	MSCS log information is collected.
7	PRIMEQUEST Server Agent (PSA) information	A PSA log is collected.

- 2 Dr. Watson
Dr. Watson is a tool for collecting an OS standard user mode dump.
- 3 Event Trace for Windows (ETW)
ETW is an OS standard trace/logging function that can collect the types of data listed below. Enable the function to collect data as needed when the relevant event occurs.
 - Data related to process creation and termination
 - Data related to thread creation and termination
 - Data related to disk I/O operations
 - Data related to TCP/IP transmission/reception requests

(2) Collecting information when a software problem has occurred

This section explains an example of collecting information when a software problem has occurred.

Forcibly collecting a memory dump

A forced memory dump has very useful information when there is one of the following symptoms:

- Frozen desktop screen
The entire Windows system hangs (the desktop screen is frozen, and mouse and keyboard operation is disabled) during system operation.
- Extremely poor responsiveness of the mouse and keyboard
System performance deteriorates greatly during system operation, with poor responsiveness of the mouse and keyboard. These conditions continue.

Collect a forced memory dump in the following procedure.

- 1 Establish a connection to the MMB Web-UI.
- 2 Search for the Windows partition in which a failure occurred.
From the MMB Web-UI window, click [Partition] → [Power Control].
- 3 Issue INIT.
From the pulldown menu of the applicable partition, specify [INIT], and then click the [Apply] button.
- 4 A memory dump starts.
The system automatically reboots during the memory dump. Depending on the settings, the system may need to be rebooted manually.

Notes:

- Server operation is stopped during the forced memory dump.
 - Depending on the environment, the memory dump may take a long time to complete.
 - If the KVM is connected to the partition in which Windows Server 2003 Enterprise Edition is installed, the screen may not be displayed normally during the memory dump.
- 5 After startup, log on with the administrator privilege to the partition.
 - 6 Execute QSS to collect system information.
Execute QSS as shown below (in this example, Software Support Guide is installed in c:\supportguide):
 - 7 Start the command prompt.
Click [Start] → [Run], specify "cmd.exe" in the [Name] field, and then click the [OK] button.
 - 8 Enter the following command at the command prompt (specify the data output path for output_path):

`c:\supportguide\qss\qss_pq.exe <output_path>`

9 Collect data.

When the following message appears for the command prompt, enter [Y] key, and press the [Enter] key.

Type Y to start, or type N to cancel (default = N):

10 QSS execution starts, and QSS collects information.

11 Check the collected information.

- Memory dump
For the dump file location, see "Memory dump/paging file setting."
- QSS-collected information
Folder specified during collection

(3) Information checklist

Use the following checklist to confirm that the collected information is adequate.

Table 1.3 Information check list

Check item	Description
Collect information including dump files.	
Collect information by using QSS. (Required)	<p>Information collection using QSS is always required when a problem occurs. For an example of executing QSS, see step 6 and subsequent steps in , "Forcibly collecting a memory dump."</p> <p>Notes:</p> <ul style="list-style-type: none"> • Do not click [X] in the window while QSS is being executed. Canceling QSS execution by clicking [X] will leave a temporary work file on the server. • To cancel QSS execution, press the [C] key while holding down the [Ctrl] key.
Record information on the problem occurrence. (Required)	<ul style="list-style-type: none"> • Time that the problem occurred • Any particularities of the problem Does the problem occur frequently? Does the problem occur regularly? • Specific event that occurred immediately before the problem occurred Example: A patch was applied.
Check the server configuration. (Required)	<p>Check the following items:</p> <ul style="list-style-type: none"> • Model name and type name of the server • Hardware configuration <p>Types and locations of mounted internal options:</p> <ul style="list-style-type: none"> • Version and level of the OS used, and whether service packs have been applied • LAN/WAN system configuration

1.7 Setting Dump Environments (Windows Server 2003)

In Windows Server 2003, a dump can be collected with an OS standard function. A system area must be allocated in advance to save a dump. For details on allocating the area, see the following manuals:

- *PRIMEQUEST 580A/540A/580/540/480/440 System Design Guide* (C122-B001EN)
- *PRIMEQUEST 520A/520/420 System Design Guide* (C122-B009EN)

This section explains how to set the dump environment in Windows Server 2003. For details on dump related operations, See the *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs* (C122-E004EN). To recover the system after a system failure occurs, see and set the following items before starting the operation.

- [Memory dump/paging file](#) (→ 1.7.1)
- [Early troubleshooting \[DSNAP\]](#) (→ 1.6.1)

1.7.1 Memory dump/paging file

The memory dump file is used to save debug information when a STOP error (fatal system error) occurs in the system. The settings required for a memory dump must be made after the operating system and applications used for operation are installed.

1.7.1.1 Different information that can be collected with a memory dump

The following three types of memory dumps can be set up on the PRIMEQUEST device, with each having a different scope of collectable information.

Before starting a memory dump, make sure that the hard disk has enough free space.

- Complete memory dump
Records all the contents of the physical memory when the system has stopped. The boot volume must have free space equivalent to approximately the physical memory size plus 1 megabyte. It can save only one dump. If the specified save location already has a dump file, the dump file is overwritten.

- **Kernel memory dump (recommended)**
Records the information for the kernel space only. The boot volume must have 50 megabytes to several hundred megabytes (up to the physical memory size plus 128 megabytes) of free space. The size depends on the operating status. The boot volume can store only one dump. If the specified save location already has a dump file, the dump file is overwritten.
- **Minimum memory dump**
Records a minimum of information that helps identify a problem. When this option is specified, a new file is created every time the system stops unexpectedly.

Table 1.4 Modes and sizes of memory dump

Memory dump mode	Memory dump file size	
Complete memory dump	Physical memory size + 1 MB	Overwrite (*2)
Kernel memory dump	Depends on the size of memory space when the OS is operating (usually 50 to several hundred MB). Maximum: Physical memory installed + 128 MB (*1)	Overwrite (*2)
Small memory dump	64 KB or 128 KB	Create a new file.

*1 The value shown is the maximum size and depends on the size of memory space.

*2 By default, an existing file is overwritten. The default setting can be changed so that an existing file is not overwritten. However, note that no new file would be created, unlike in a "minimum memory dump."

Remarks: Select the setting mode appropriate for system operation by considering the following:

- If the PRIMEQUEST Software Installer is executed, the mode is automatically set to kernel memory dump. Because a kernel memory dump does not include user mode information, the cause of a problem may not always be determined.
- Depending on the size of mounted memory, a complete memory dump takes longer to create a dump and keeps business stopped longer accordingly. In addition, more space is required for saving a dump file on the hard disk.

1.7.1.2 Setting a memory dump

Setting a complete memory dump

Complete memory dump cannot be set from the system dump setting window. It can be set by changing the following registry value:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl

"CrashDumpEnabled" (type: REG_DWORD, data: 0x1)

After changing the setting, restart the system. For details on the dump file save path and overwrite settings, see ["Setting a kernel memory dump/minimum memory dump."](#)

Setting a kernel memory dump/minimum memory dump

Set the memory dump file in the following procedure.

- 1 Log on to the server with the administrator privilege.
- 2 Check the amount of free space on the drive on which the memory dump file is to be stored.
- 3 Click [Control Panel] → [System].
The [System Property] dialog box appears.
- 4 Click the [Detail Setting] tab, and click [Set] button at [Startup and Recovery].
The [Startup and Recovery] dialog box appears.

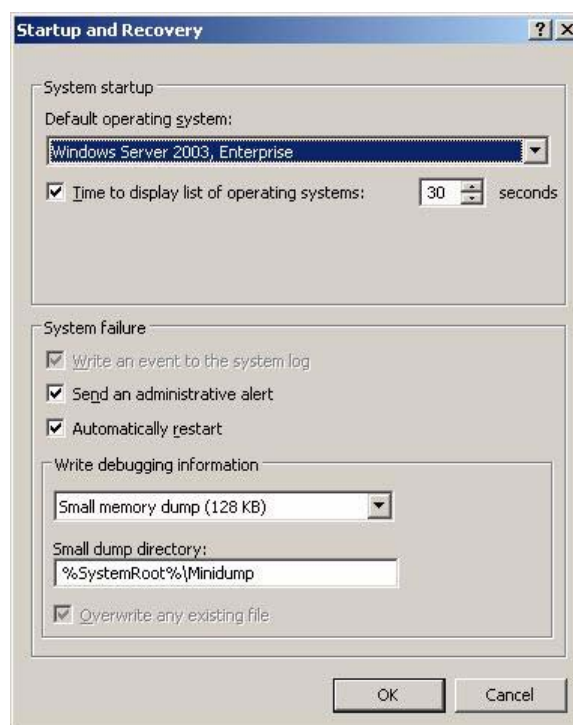


Figure 1.3 Startup and Recovery dialog box

- 5 Do the following settings:
 - 1) Select the type of memory dump file from [Write debugging information].
 - Kernel memory dump (recommended)

Only kernel memory is logged to the memory dump file.

In [Dump file], specify the full path of the directory to which a memory dump file is saved. If the [Overwrite any existing file] check box is selected for kernel memory dump, debug information is always written to the specified file.
 - Small memory dump (64KB or 128KB)

Minimum information is logged in the memory dump file. Every time an unrecoverable error occurs, a new file is created in the directory specified in [Small dump directory].
- 6 Click [OK] button to close the [Startup and Recovery] dialog box.
- 7 Click [OK] button to exit from the [System Property] dialog box.
- 8 Reboot the partition.

The settings are validated after the partition reboot.

1.7.1.3 Verifying the memory dump settings

Perform a memory dump in advance to make sure that memory information is dumped normally. In addition, measure the time taken till dump is output actually and the time taken for a system restart in order to estimate the time required till business can be restarted. Based on that result, reconsider the dump mode as needed.

To implement a dump, specify INIT for the target partition by selecting [Partition] → [Power Control] from the MMB Web-UI. For details, see Chapter 5, "MMB Web-UI," in the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

1.7.1.4 Setting paging files

Set the paging file by following the procedure below. Unless otherwise instructed, use the values that are automatically assigned during Windows installation for the paging file.

- 1 Log on to the server with administrator privilege.
- 2 Click [Control Panel] → [System].
The [System Properties] dialog box is displayed.
- 3 Click the [Detail Settings] tab and then click [Settings] of [Performance].
The [Performance Options] dialog box is displayed.
- 4 Click the [Detail Settings] tab.



Figure 1.4 Detail Settings dialog box

- 5 Click the [Change] button of [Virtual Memory].
The [Virtual Memory] dialog box is displayed.

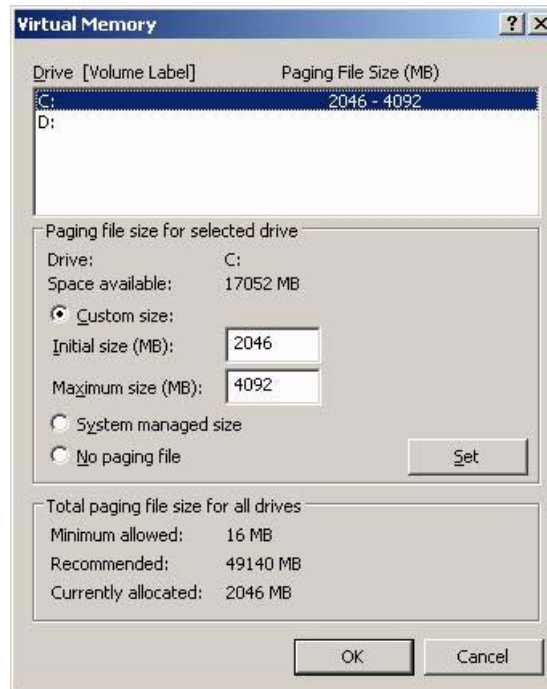


Figure 1.5 Virtual Memory dialog box

- 6 Specify the drive where a paging file is created.
Select from the [Drive] list the drive in which the system is installed. The selected drive is displayed in [Drive] of [Paging File Size of Selected Drive].
- 7 Select [Custom Size] and enter a value in [Initial Size].
To search for a minimum value, perform the following procedure.
 1. Under Custom Size, enter the minimum value for Initial Size (MB) (if the dialog box shown in [Figure 1.5, "Virtual Memory dialog box,"](#) is displayed, this value is 16 megabytes, which is the minimum value of the total paging file size for all drives), and enter the minimum value + 2 megabytes for Maximum Size (MB) (if the dialog box shown in [Figure 1.5, "Virtual Memory dialog box,"](#) is displayed, this value is 18 megabytes). Then, click the [Set] button.
 2. Unless the following message is displayed, make the setting with the entered values.
If the following message is displayed, set the minimum value as the displayed value. (200 megabytes in this case)
Generally, values automatically assigned by the OS should be used.

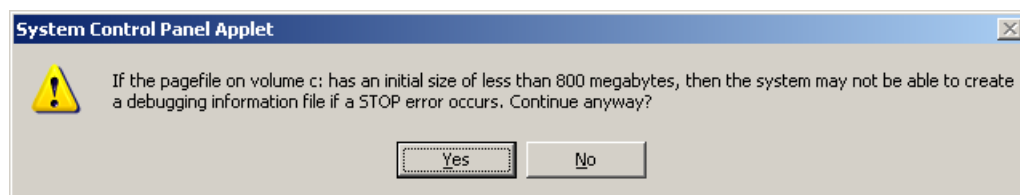


Figure 1.6 [System Control Panel Applet] dialog box

- 8 Enter a value for [Maximum Size].
Set a value that is larger than [Initial Size].
- 9 Click the [Settings] button of [Paging File Size of Selected Drive].
The setting is saved, and the set value is displayed in [Paging File Size] of the [Drive] list.
- 10 Click the [OK] button to close the [Virtual Memory] dialog box.
- 11 Click the [OK] button to close the [Performance Option] dialog box.
- 12 Click the [OK] button to close the [System Properties] dialog box.
- 13 Reboot the partition.
After the partition is rebooted, the settings are enabled.

1.7.1.5 Note

Note that if the paging file is allocated to a partition other than the system partition (usually drive C), no dump file is generated when a stop error occurs. Unless otherwise instructed, do not move the paging file.

1.8 Backup and Restoration

This section describes how to back up and restore the system volume on the partition in which Linux (Red Hat) or Windows is installed. For details of how to back up and restore the system volume on the partition in which SUSE is installed, refer to the SUSE manual.

1.8.1 Backup Requirements

PRIMEQUEST uses reliable components and hardware and duplicates many devices to ensure a high reliability. If trouble occurs and the system is damaged, or server internal data is deleted because of an operator error, the data must have been backed up so it can be restored to its original state.

If the server data has been backed up, the system can be recovered from the backup data even if internal data on the hard disk has been destroyed because of an operator error and subsequent hardware failure. Unless a backup is created, important data can be lost. To safely operate the system, be sure to make a periodic backup.

The required operations are explained in the following order.

- [Linux \(Red Hat\) backup](#) (→ 1.8.2)
- [Linux \(Red Hat\) restoration](#) (→ 1.8.3)
- [Windows backup](#) (→ 1.8.4)
- [Windows restoration](#) (→ 1.8.5)

1.8.2 Linux (Red Hat) backup

This section explains in the following order the procedures for backing up the system volume in the partition where the Linux OS (Red Hat) is installed. An example of Red Hat Enterprise Linux AS (v.4 for Itanium) is provided.

- Using the standard OS utilities
- Using SystemcastWizard Lite

This section explains in the following order the procedures for backing up the system volume in the partition where the Linux OS is installed.

- When PRIMECLUSTER GDS is not used
- When PRIMECLUSTER GDS is used

Note:

Prepare a single unit tape device for the backup device

Remarks:

The OS console is used for backup and restore operation. Either the KVM console or serial console can be used.

For details on use of SystemcastWizard Lite for Linux backup, see the *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

1.8.2.1 Backup when PRIMECLUSTER GDS is not used

This section explains the applicable backup procedure when PRIMECLUSTER GDS is not used.

The example of operation shown below assumes the following disk configuration:

```
/dev/sda1 : /boot/efi  
/dev/sda2 : /  
/dev/sda3 : swap  
/dev/sda4 : /work
```

Preparation

First, check the operation environment (system and disk configurations) of the objective system. The contents checked here are required for restoration when the disk fails.

(1) Check the system setup.

- 1 Check IDE and SCSI card types and IRQ and I/O port operating status.

```
# dmesg
```

or

```
# more /var/log/messages
```

- 2 Check driver file names.

```
# lsmod
```

- 3 Check device names, device types, and major and minor numbers.

```
# ls -al /dev/sda*
```

(2) Check the disk configuration.

- 1 Check the mount status.

```
# cat /etc/fstab
```

- 2 Keep a record of the configuration information of a partition.

Due to disk failure, it may be necessary to restore data on a new disk. Therefore, it is necessary to prepare for restoration by recording the current partition configuration in advance by using the parted command.

Proceed to the work according to the following example.

Example:

```
# parted
(parted) unit s
(parted) print

Disk /dev/sdb: 71390319s
Sector size (logical/physical): 512B/512B
Partition table: gpt

No.      Start       End         Size        File system  Name      Flag
  1       34s        204833s     204800s     fat16        Primary   msftres
  2      204834s    42147873s   41943040s   ext2         Primary
  3      42147874s   46228383s   4080510s    linux-swaps  Primary
  4      46228384s   67199903s   20971520s   ext2         Primary
(parted) quit
```

Remarks: In Red Hat Enterprise Linux 5 (for Itanium), the print subcommand of parted briefly indicates numeric values with such units as "MB" added; therefore, the difference with the actual size may increase.

To reduce the difference with the backup size at partition reconfiguration, keep a record of the partition and reduce the size of the display unit before executing the print subcommand.

In the example above, "unit s" is used to display the size in sectors (s).

- 3 Check file system label names.

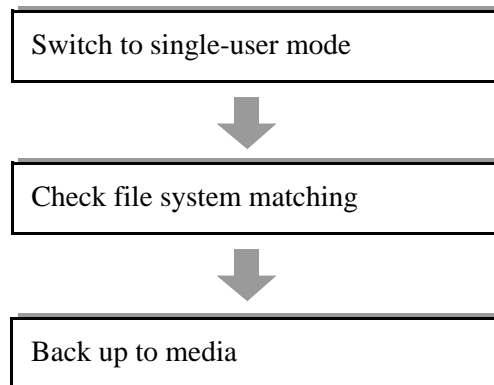
```
# e2label /dev/sda2
```

Remarks:

Specifying the device mounted on /boot/efi will result in an error, this error occurs because the file system is different. That does not cause a problem because "boot/efi" is not defined as a label name, checking it is not required.

Backup

Perform the backup in the following procedure.



The following explains each step.

(1) Switch to single-user mode

To perform the backup, the user must deactivate all processes except those required to perform it. This is to secure file matching.

To enter this state, switch to single-user mode.

- When the system is already active
 - 1 Log in with the root directory.
 - 2 Stop running applications.
 - 3 Switch to run level 1 (single-user mode).

```
# init 1
```

- When the system is in a stopped state

- 1 Start the system.

When the EFI boot manager menu appears, select the name of the system to be started (such as Red Hat Enterprise Linux).

Note:

Advance settings are required to start the EFI boot manager menu. See Section 3.3.2.4, "Boot control of partition" in the *PRIEMQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN) for details on the setting method.

- 2 Enter the command shown below following the "ELILO boot:" prompt.

- When a KVM console is used

```
Kernel-Label-Name 1
```

- When a serial console is used

```
Kernel-Label-Name 1 console=ttyS0,19200n8r
```

When the switchover to single-user mode is completed, the command line mode is entered and the prompt is displayed.

Remarks: To check the current Kernel-Label-Name, see the default entry in the following config file:

/boot/efi/efi/redhat/elilo.conf

(2) Check file system matching

To check whether the file system to be backed up is normal, check its match.

The file system that needs to be checked is ext3 (or ext2). "/boot/efi" and swap need not be checked.

- For location other than "/" (root), "/boot/efi," and swap

- 1 Demount the file system to be backed up.

```
# cd /  
# umount /work
```

- 2 Check the matching of the demounted file system.

```
# e2fsck -pfv /dev/sda4
```

Note:

Do not execute the e2fsck command if the umount command produces an error.

If the e2fsck command is executed with the file system mounted, the selected volume may be damaged.

- For "/" (root)

- 1 Remount the "/" file system in Read-Only mode.

```
# mount -r -n -o remount /
```

- 2 Check the matching of the file system.

```
# e2fsck -pfv /dev/sda2
```

- 3 Remount the file in normal state.

```
# mount -w -n -o remount /
```

Note:

Do not execute the e2fsck command if the mounting in Read-Only mode fails.

If the e2fsck command is executed with the file system mounted as write-enabled, the selected volume may be damaged.

(3) Back up to media

Back up to backup media for each partition of the disk.

The dump command is used for backup, but it supports the ext2 and ext3 file systems only. Use the tar command to back up /boot/efi of a different file system.

Note:

Be careful when different tape units are used for backup and restoration because the default block sizes of the tape units may be different. Execute backup and restoration based on the same block size. Restoration fails if the block size used for restoration differs from that used for backup.

- Using a locally connected tape unit:

- 1 Prepare a tape unit.

See "mt" command manuals for details.

- Display status information on the tape unit.

```
# mt -f /dev/nst0 status
```

- Rewind tape.

```
# mt -f /dev/nst0 rewind
```

- 2 Back up.

- For location other than /boot/efi

Back up with the dump command.

```
# dump 0uf /dev/nst0 /dev/sda2
```

- For /boot/efi

Back up with the tar command.

```
# cd /boot/efi
# tar czvf /dev/nst0 .
```

- When a tape unit connected to the remote host is used

- 1 Start the network.

```
# /etc/rc.d/init.d/network start
```

- 2 Activate the network.

```
# ifconfig eth0 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx broadcast \
xxx.xxx.xxx.xxx
```

\: Indicates that no line feeds should be inserted.

Remarks:

Set values such as the IP address according to your system.

3 Prepare a tape unit.

Use the `mt` command with the `ssh` command for operation with a remote tape unit.

For details, see the `mt` command manual.

- Rewind tape.

```
# ssh remote-host-name mt -f /dev/nst0 rewind
```

Enter the password in response to the password prompt.

4 Back up.

Use the `ssh` command for the backup operation.

- For a file system other than `/boot/efi`

Back up with the `dump` command.

```
# dump 0f - /dev/sda2 | ssh remote-host-name dd of=/dev/nst0
```

Enter the password in response to the password prompt.

- For `/boot/efi`

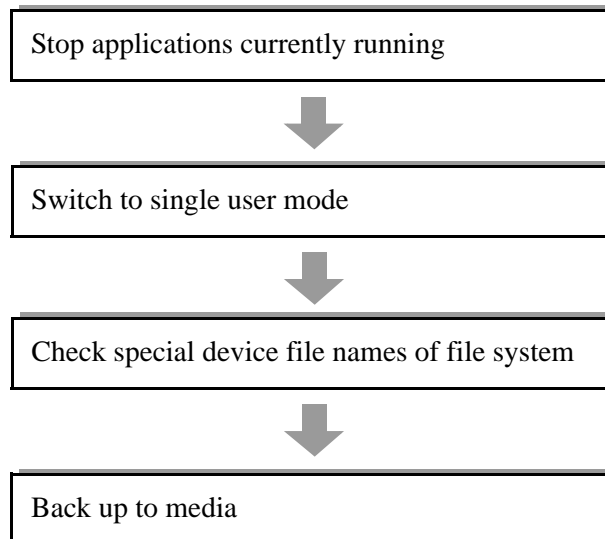
Back up with the `tar` command.

```
# cd /boot/efi
# tar czvf - . | ssh remote-host-name dd of=/dev/nst0
```

Enter the password in response to the password prompt.

1.8.2.2 Backup when PRIMECLUSTER GDS is used

Use the following procedure for the backup when PRIMECLUSTER GDS is used.



Remarks:

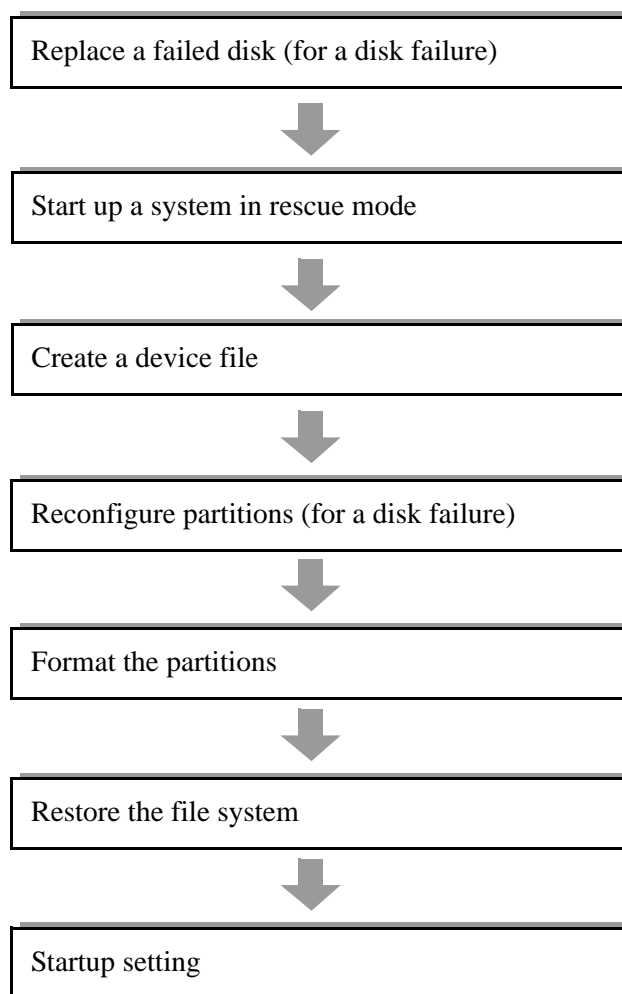
See the *PRIMECLUSTER Global Disk Services Configuration and Administration Guide (Linux)* for details.

1.8.3 Linux (Red Hat) restoration

This section explains the procedures for restoring the system volume from the partition where the Linux OS (Red Hat) is installed, using an example of Red Hat Enterprise Linux AS (v.4 for Itanium).

1.8.3.1 Restoration when PRIMECLUSTER GDS is not used

Perform the restoration in the following procedure.



The following explains each step.

An input example for the following disk configuration is provided.

```
/dev/sda1 : /boot/efi  
/dev/sda2 : /  
/dev/sda3 : swap  
/dev/sda4 : /work
```

(1) Replace the disk (for a disk failure)

Replace the failed disk.

(2) Start up the system in rescue mode

By activating the installation CD in rescue mode, the system can be booted with the CD-ROM only instead of booting it from the system hard disk drive. This allows the user to access a file stored on the system hard disk drive even if Linux (Red Hat) cannot actually be executed directly from the hard disk drive.

- 1 Insert the installation CD1 in the CD-ROM drive and start up the system.
The EFI boot manager menu is displayed.

Note:

To display the EFI boot manager menu, it must be set in advance. See Section 3.3.2.4, "Boot control of partition" in the *PRIEMQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN) for details on the setting method.

- 2 Select the DVD-ROM drive in the boot option and press the [Enter] key.

`DVD/Acpi(PNP0A03,0)/Pci(1D|1)Usb(0, 0) ← Select this.`

- 3 Enter the following after the "ELILO boot:" prompt to boot the system.

- When a KVM console is used

`linux rescue`

- When a serial console is used

`linux rescue console=ttyS0,19200n8r`

Several minutes may be required until the window in 4 is displayed.

- 4 Select the following in the [Choose Language] window and click [OK].

`English`

- 5 Select the following in the [Keyboard Type] window and click [OK].
(for the KVM console)

`us`

Note:

To use a different keyboard, select it here.

- 6 Set up a network in the [Setup Networking] window.
Select [Yes] for the setup; otherwise, select [No].
Select [Yes] to display the window to set the LAN card IP address that is current recognized as eth0. Set the IP address according to the instructions in the window.
- 7 In the [Rescue] window, the user is asked whether to automatically mount an existing partition. Select [Skip].
- 8 The following command prompt is displayed when the system booting in rescue mode is completed.

```
- /bin/sh-3.00#
```

(3) Create a device file

If there is no device that corresponds to the /dev directory, load the necessary SCSI system device drivers into the system and create the special files (disks and partitions).

Because these special files are valid while the rescue system is active, if the rescue system is rebooted to divide a partition, they must be created again.

- 1 Check whether the necessary drivers are included.

```
- /bin/sh-3.00# lsmod
```

Confirm that the drivers checked in "Preparation" include the necessary ones.

- 2 Check the special files of the device names, device types, and major and minor numbers that are checked in "Preparation."

```
- /bin/sh-3.00# cd /dev  
- /bin/sh-3.00# ls -al sda*
```

If the necessary drivers are not created, create them with the mknod command.

```
- /bin/sh-3.00# mknod sda b 8 0  
- /bin/sh-3.00# mknod sda1 b 8 1  
- /bin/sh-3.00# mknod sda2 b 8 2  
- /bin/sh-3.00# mknod sda3 b 8 3  
- /bin/sh-3.00# mknod sda4 b 8 4
```

(4) Reconfigure partitions (for a disk failure)

When a new disk is used due to disk failure, its partitions must be reconfigured. To create the same partition configuration as that at backup time, see the configuration information that was recorded in Preparation (2), "[Check the disk configuration.](#)," in [Section 1.8.2.1](#).

Example of disk configuration information:

Disk /dev/sdb: 71390319s						
Sector size (logical/physical): 512B/512B						
Partition table: gpt						
No.	Start	End	Size	File system	Name	Flag
1	34s	204833s	204800s	fat16	Primary	msftres
2	204834s	42147873s	41943040s	ext2	Primary	
3	42147874s	46228383s	4080510s	linux-swap	Primary	
4	46228384s	67199903s	20971520s	ext2	Primary	

If the configuration information recorded in advance is as shown above, create the partition configuration by using procedure shown in the example below.

Example:

```
-/bin/sh-3.00# parted
:
(parted) print                ← Confirm that the partitions are not created.
(parted) mklabel gpt          ← Set the disk label to "gpt".
(parted) unit s                ← Change the unit to sectors.
(parted) mkpartfs primary fat16 34 204833
:
(parted) mkpartfs primary ext2 204834 42147873
:
(parted) mkpartfs primary linux-swap 42147874 46228383
(parted) print                ← Confirm that the partitions are created.
(parted) quit                  ← Quit the parted command.
```

(5) Format the partitions

Format the partitions (vfat, ext3(ext2), and swap) on the disk.

The following indicates a format example for each partition type.

- vfat format

```
-/bin/sh-3.00# mkfs.vfat /dev/sda1
```


- ext3 format

After the file system is formatted, set the label name of the file system.

```
- /bin/sh-3.00# mkfs.ext3 /dev/sda2  
- /bin/sh-3.00# e2label /dev/sda2 /
```

- ext2 format

After the file system is formatted, set the label name of the file system.

```
- /bin/sh-3.00# mkfs.ext2 /dev/sda2  
- /bin/sh-3.00# e2label /dev/sda2 /
```

- For swap partition

```
- /bin/sh-3.00# mkswap /dev/sda3
```

(6) Restore the file system

Restore all directories, starting from the "/" (root) directory.

Note:

When backup and restoration are performed with different tape units, the default block sizes of those tape units may differ. Perform the backup and restoration with the same block size. If the block size for the restoration differs from that for the backup, the restoration fails.

- 1 Create a mount point.

Create a mount point as a work directory.

```
- /bin/sh-3.00# mkdir /mnt/work1  
- /bin/sh-3.00# mkdir /mnt/work2
```

- 2 Mount the configured partitions.

```
- /bin/sh-3.00# mount -t vfat /dev/sda1 /mnt/work1  
- /bin/sh-3.00# mount -t ext3 /dev/sda2 /mnt/work2  
- /bin/sh-3.00# df -k
```

Check that the partition is correctly mounted.

The following section explains the restoration procedures of the file system when using the tape unit connected locally and when using the tape unit connected to the remote host.

- Using a locally connected tape unit:

- 1 Prepare the tape unit.

See the `mt` command manuals for details.

- Tape unit state information display

```
- /bin/sh-3.00# mt -f /dev/nst0 status
```

- Tape rewind

```
- /bin/sh-3.00# mt -f /dev/nst0 rewind
```

- Move the head to the first block of the next file.

```
- /bin/sh-3.00# mt -f /dev/nst0 fsf
```

- 2 Perform the restoration.

- For a location other than `/boot/efi`

Perform the restoration with the `restore` command.

```
- /bin/sh-3.00# cd /mnt/work2  
- /bin/sh-3.00# restore rf /dev/nst0 .
```

- For `/boot/efi`

Perform the restoration with the `tar` command.

```
- /bin/sh-3.00# cd /mnt/work1  
- /bin/sh-3.00# tar xzvf /dev/nst0
```

Note:

When `/tmp` is specified as an independent partition, the `/tmp` permission is changed from 1777 when the backup and restoration are performed, and a specific service using `/tmp` may not be started.

After the restoration is performed, return the `/tmp` permission to 1777.

- Procedure for changing `/tmp` permission

```
- /bin/sh-3.00# cd /mnt/work2  
- /bin/sh-3.00# ls -l | grep tmp  
drwxr-xr-x  7 root root    4096  Feb 24 15:44 tmp  
- /bin/sh-3.00# chmod 1777 tmp  
- /bin/sh-3.00# ls -l | grep tmp  
drwxrwxrwt  7 root root    4096  Feb 24 15:44 tmp
```

- 3 Exit the rescue mode and reboot the system.

```
- /bin/sh-3.00# exit
```

- Using a tape unit connected to a remote host

- 1 Activate the network.

```

-/bin/sh-3.00# ifconfig eth0 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx broadcast \
xxx.xxx.xxx.xxx

```

\: Indicates that no line feeds should be inserted.

Note:

The ifconfig command does not support the -a option. Check the network with the ping command.

Remarks:

Set values such as IP addresses appropriately for the system.

- 2 Prepare a tape unit.

Use the ssh command to operate the remote tape unit with the mt command.

For details, see mt command manual.

- 3 Perform the restoration.

- Not under /boot/efi

Perform the restoration with the restore command.

```

-/bin/sh-3.00# cd /mnt/work2
-/bin/sh-3.00# ssh remote-host-name dd if=/dev/nst0 |
restore rf -

```

When you are prompted for the password, enter it.

- Under /boot/efi

Perform the restoration with the tar command.

```

-/bin/sh-3.00# cd /mnt/work1
-/bin/sh-3.00# ssh remote-host-name dd if=/dev/nst0 |
tar xzvf -

```

When you are prompted for the password, enter it.

Note:

When /tmp is specified as an independent partition, the /tmp permission is changed from 1777 when the backup and restoration are performed, and a specific service using /tmp may not be started.

After the restoration is performed, return the /tmp permission to 1777.

- Procedure for changing /tmp permission

```

-/bin/sh-3.00# cd /mnt/work2
-/bin/sh-3.00# ls -l | grep tmp
drwxr-xr-x    7 root root      4096  Feb 24 15:44 tmp
-/bin/sh-3.00# chmod 1777 tmp
-/bin/sh-3.00# ls -l | grep tmp
drwxrwxrwt    7 root root      4096  Feb 24 15:44 tmp

```

- 4 Exit the rescue mode and reboot the system.

```
-/bin/sh-3.00# exit
```

(7) Startup setting

- When a hard disk is replaced

- 1 Add an EFI boot manager menu.

- (1) Select [Boot Option Maintenance Menu] in the boot manger menu.

```
EFI Boot Manager ver 1.10 [0.3]

Please select a boot option
  Red Hat Enterprise Linux AS
  EFI Shell [Built-in]
  DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)
  Floppy/Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0604,0)
  Boot Option Maintenance Menu      ← Select this.
  Setup Menu

Use ^ and v to change option(s). Use Enter to
select an option
```

Note:

To display the EFI boot manger menu, it must be set in advance. See Section 3.3.2.4, "Boot control of partition" in the *PRIEMQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN) for details on the setting method.

- (2) Select [Add a Boot Option] in the boot option maintenance menu.

```
Boot Option Maintenance Menu

Main Menu. Select an Operation
  Boot From a File
  Add a Boot Option      ← Select this.
  Delete Boot Option(s)
  Change Boot Order
  Set Auto Boot Timeout
  Reset System
  Exit
```

(3) Select a boot device.

Select [NO VOLUME LABEL].

```

Boot Option Maintenance Menu

Add a Boot Option.  Select a Volume
NO VOLUME LABEL [Acpi(PNP0A03,0)/Pci(9|1)/Pci(0|2)/Pci(1|0)/Scsi ← Select this.
Removable Media Boot [Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)]
Load File [Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B5D6E0043)]
Load File [EFI Shell [Built-in]]
Exit

```

(4) Specify a directory and a file.

Select [efi] → [redhat] → [elilo.efi].

```

Boot Option Maintenance Menu

Select file or change to new directory:
    03/16/05  09:31p <DIR>          8,192 efi ← Select this.
    [Treat like Removable Media Boot]
Exit

```

Note:

If the directory is not displayed, return to step (3) and specify another device.

```

Boot Option Maintenance Menu

Select file or change to new directory:
    03/30/05  05:56p <DIR>          8,192 .
    03/30/05  05:56p <DIR>           0 ..
    03/16/05  09:31p <DIR>          8,192 Intel Firmware
    03/16/05  09:48p <DIR>          8,192 redhat ← Select this.
Exit

```

```

Boot Option Maintenance Menu

Select file or change to new directory:
    03/30/05  05:56p <DIR>          8,192 .
    03/30/05  05:56p <DIR>          8,192 ..
    09/21/04  08:13p              333,276 elilo.efi ← Select this.
Exit

```

(5) Set a menu name.

When "Enter New Description:" is displayed, set a character string such as "Red Hat Enterprise Linux" to be used in the EFI boot manager menu.

(6) Set an option.

Enter [N] after "Enter BootOption Data Type [A-Ascii U-Unicode N-No BootOption]:."

Also enter [N] after "Save [Y-Yes N-No]: " (confirmation of writing to NVRAM).

Return to "Boot Option Maintenance Menu."

(7) Select [Exit] to return to the Boot Option Maintenance Menu.

2 Change the boot priority order in the EFI boot manager menu.

- (1) Select [Change Boot Order] in the boot option maintenance menu.

```
Boot Option Maintenance Menu

Main Menu. Select an Operation
  Boot From a File
  Add a Boot Option
  Delete Boot Option(s)
  Change Boot Order      ← Select this.
  Set Auto Boot Timeout
  Reset System
  Exit
```

- (2) Select the menu name that is set in (1), and raise its priority order.
Select the menu name with the arrow keys and raise its priority by [U] or [u].

```
Boot Option Maintenance Menu

Change Boot Order. Select an Operation
  Red Hat Enterprise Linux AS 4
  EFI Shell [Built-in]
  DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)
  Floppy/Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0604,0)
  Red Hat Enterprise Linux AS ← Select this and move it
                               to the top.

  Save
  Help
  Exit
```

- (3) Save the setting.

```
Boot Option Maintenance Menu

Change Boot Order. Select an Operation
  Red Hat Enterprise Linux AS
  Red Hat Enterprise Linux AS 4
  EFI Shell [Built-in]
  DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)
  Floppy/Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0604,0)
  Save      ← Select this.
  Help
  Exit
```

- (4) Select [Exit] to return to the Boot Option Maintenance Menu.
(5) Select [Exit] and return to the boot manager menu.

3 Start the system.

Select the set menu name in the boot manager menu.

● When a hard disk is not replaced

Follow the same procedure up to step 6 in "(2) Start up the system in rescue mode."

1 In the [Rescue] window, the user is asked whether to automatically mount an existing partition. Click [Continue].

If the existing root partition ("/") of the Linux system can be mounted in /mnt/sysimage, the result is displayed in the [Rescue] window. Click [OK].

2 When the prompt is displayed, change the root path to the hard disk.

```
# chroot /mnt/sysimage
```

3 Execute efibootmgr to rewrite the startup/boot menu.

```
# /usr/sbin/efibootmgr -c -w -L "Red Hat Enterprise Linux AS 4 for Itanium" \
-d /dev/sda -p /dev/sda1 -l "EFI\\redhat\\elilo.efi"
```

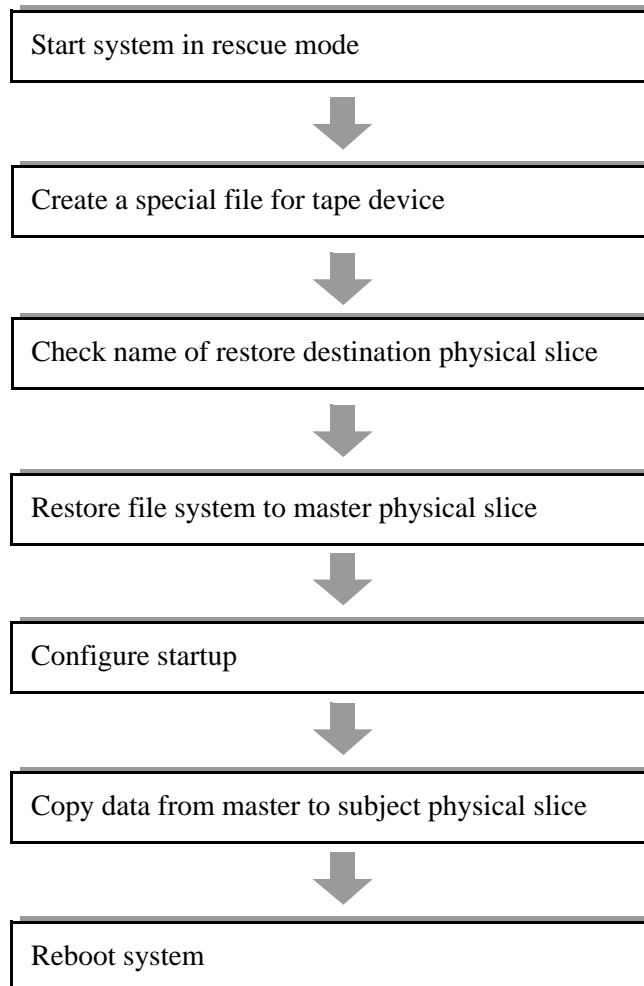
\\: Indicates that no line feeds should be inserted.

4 Escape from the rescue menu and start up the system.

```
# exit      ← Escape from chroot environment.
# exit      ← Escape from rescue mode.
```

1.8.3.2 Restoration when PRIMECLUSTER GDS is used

When PRIMECLUSTER GSD is used, perform the restoration in the following procedure.



Remarks:

See the *PRIMECLUSTER Global Disk Services Configuration and Administration Guide (Linux)* for details.

1.8.4 Windows backup

Use SystemcastWizard Lite to back up Windows partitions.

For details on backup with SystemcastWizard Lite, see the *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

1.8.5 Windows restoration

Use SystemcastWizard Lite to back up Windows partitions.

For details on backup with SystemcastWizard Lite, see the *PRIMEQUEST SystemcastWizard Lite User's Guide* (C122-E010EN).

1.9 Notes on Setting a Device Name (Linux: Red Hat)

Linux (Red Hat) assigns device names to various devices such as hard disk drives in the order they are recognized when the system is started up. Therefore, if the system is rebooted after a failure occurs on a hard disk drive or controller, the hard disk drive cannot be recognized, so that the device names may change. This is also true for network devices. If the system is rebooted after a failure occurs in an NIC (Network Interface Controller), the failed device cannot be found, so that the device names may change.

Example:

When hard disk drives are connected to SCSI ID=1, 2, and 3, device names, /dev/sda, /dev/sdb, and /dev/sdc, are assigned. If /dev/sdb fails in this state, after the system is rebooted, /dev/sdc is moved up and recognized as /dev/sdb. The unexpected change of a device name may make it impossible to reboot the system and, in the worst case, the data of a file system may be destroyed .

In the latest Linux (Red Hat), the above problem is solved by assigning the same device name even if the system is rebooted after the hardware device configuration is changed. Be sure to take this measure because the unexpected change of a device name may make it impossible to reboot the system or may destroy the file system data. Note that the device names assigned by the OS may not directly be used, but those defined and created by middleware may be used for the operation. Therefore, see the manual of each middleware product for details. For details on the device names assigned when an ETERNUS multipath driver is used, see the *ETERNUS Multipath Driver Installation Guide* or Manual.

Note that the method of using device names differs between the disk system devices such as hard disks and network devices.

The following explains how the disk system devices and network devices are handled.

1.9.1 Disk system devices

Linux (Red Hat) assign two types of device name beginning with /dev/disk in addition to the device names (example: /dev/sda) that are normally used in the /dev directory.

Figure 1.7 shows the configuration example device names.

/dev/disk/by-path/xxxxxxx: xxxxxxxx is information to be created from disk location information.

/dev/disk/by-id/yyyyyyy: yyyyyyyy is information to be created from the identification information set on a disk.

The following refers to a device name beginning with /dev/disk/by-path as a by-path name and a device name beginning with /dev/disk/by-id as a by-id name. Also, the device names that are normally used are referred to as compatible device names.

Because the by-path and by-id names are created from physical information such as path numbers and device identifiers, they remain unchanged if the hardware configuration is changed. Although the device names become long, they are used in the same way as conventional ones. The by-path name should be specified because it is superior in disk maintenance such as identifying a faulty location. However, specify the by-id name for an ETERNUS disk array device. For details on this specification, refer to "Supported OSs and models, and connection requirements" at the following URL:

<http://www.fujitsu.com/global/support/computing/storage/system/>

/dev/	
	sda
	sda1
	sda2
disk/	
	by-path/
	pci-0000:00:00.1-scsi-0:0:1:0
	pci-0000:00:00.1-scsi-0:0:1:0p1
	:
	:
	by-id/
	SSEAGATE_ST373307LC_3HZ1NBK500007403WPKR
	SSEAGATE_ST373307LC_3HZ1NBK500007403WPKR1
	:

Figure 1.7 Configuration example of device names

1.9.1.1 Details on device names

This section explains in detail the three types of device name (compatible, by-path, and by-id names).

(1) Compatible device name

This name is normally used and may change if the system is rebooted after a hardware change.

(2) by-path name

This name is created from information on a location with a disk connected (PCI bus address + SCSI address). If the disk is replaced, but the location where the PCI card is inserted is unchanged, the same device name can be used. The format is as follows.

<code>/dev/disk/by-path/pci-xxxx:xx:xx.x-scsi-y:y:y:y[pn]</code>	
<code>xxxx:xx:xx.x:</code>	PCI bus address (segment number + PCI bus number + device number + function number)
<code>y:y:y:y:</code>	SCSI card internal device identification information (CH number + SCSI-ID + LUN)
<code>pn:</code>	Added for partition. "n" indicates a partition number.

Figure 1.8 By-path name format

(3) by-id name

This name is created from the unique identification information (serial number) that is set on a hard disk. It changes if the hard disk is replaced because of a failure.

1.9.1.2 Commands and files with awareness of device names

[Table 1.5](#) lists the main commands and files that require action regarding device names.

Table 1.5 Commands and files with awareness of device names

Purpose of operation	Command and file
Partition setting	parted, fdisk command
File system operation	mkfs, mke2fs, fsck, e2fsck, tune2fs, mount command /etc/fstab, etc/auto.master file
LVM operation	lvextend, pvchange, pvcreate, pvmove, vgcreate, vgextend command /etc/lvm/.cache, /etc/lvm/lvm.conf file
Raw device operation	raw command /etc/sysconfig/rawdevices file
Swap file operation	mkswap, swapon command

1.9.1.3 Notes on using new devices

(1) Device names output by kernel

Compatible device names are displayed as the device names that are contained in the messages and error logs output by kernel. See the procedure indicated in (3), ["Checking the correlation between device names"](#) for details on the correlation with the by-path names or by-id names.

(2) Command response messages

A response message of a command and utility to collect device information contains compatible device names. See the procedure indicated in (3), ["Checking the correlation between device names"](#) for details on the correlation with the by-path names or by-id names.

(3) Checking the correlation between device names

1 Finding by-path and by-id names from compatible device names

By-path and by-id names for a compatible device name can be displayed with the `udevinfo` command. The following provides an example of displaying the `/dev/sda` by-path and by-id names.

```
# udevinfo -q symlink -p `udevinfo -q path -n /dev/sda`  
disk/by-path/pci-0000:02:08.0-scsi-0:0:0:0  
disk/by-id/SFUJITSU_MAP3367NC_UPP4P4307J95
```

2 Finding compatible device names from by-path and by-id names

The by-path and by-id names are symbolic links to the corresponding compatible device names, which can be checked with the `ls` command. The following provides a display example.

```
# ls -l /dev/disk/by-path/pci-0000:02:08.0-scsi-0:0:0:0  
lrwxrwxrwx 1 root root 9 Mar 11 2005  
/dev/disk/by-path/pci-0000:02:08.0-scsi-0:0:0:00 → ../../sda
```

1.9.2 Network Devices

The network devices are managed by the `ifcfg-eth<x>` file (`eth<x>` indicates a network device name, and `x` is an integer, which represents file names such as `ifcfg-eth0` and `ifcfg-eth1`) in the `/etc/sysconfig/network-scripts` directory. By defining the hardware address (physical MAC address) of a network device in this file, the network device name (`eth<x>`) can be fixed.

Note that by using a network management tool, the network devices can be set with the GUI.

Specifically, the following line is added to the `ifcfg-eth<x>` file.

HWADDR=MAC-address

MAC-address specifies an Ethernet device hardware address in

```
DEVICE=eth1                .....Network device name
BOOTPROTO=static
BROADCAST=192.168.101.255
HWADDR=00:0E:0C:70:C3:B6   .....Hardware address
IPADDR=192.168.101.101
NETMASK=255.255.255.0
NETWORK=192.168.101.0
ONBOOT=yes
TYPE=Ethernet
```

Figure 1.9 Example of ifcfg-eth<x> file

CHAPTER 2 Physical Locations of Components

2.1 Component, LED, and Interface Locations (PRIMEQUEST 580A/540A/580/540/480/440)

This section shows the physical locations of individual components, LEDs, and interfaces.

Remarks: Only the PRIMEQUEST 580A/540A/580/540 supports BMM#1.

OP-panel

The figure below shows the locations of the OP-Panel and LEDs.

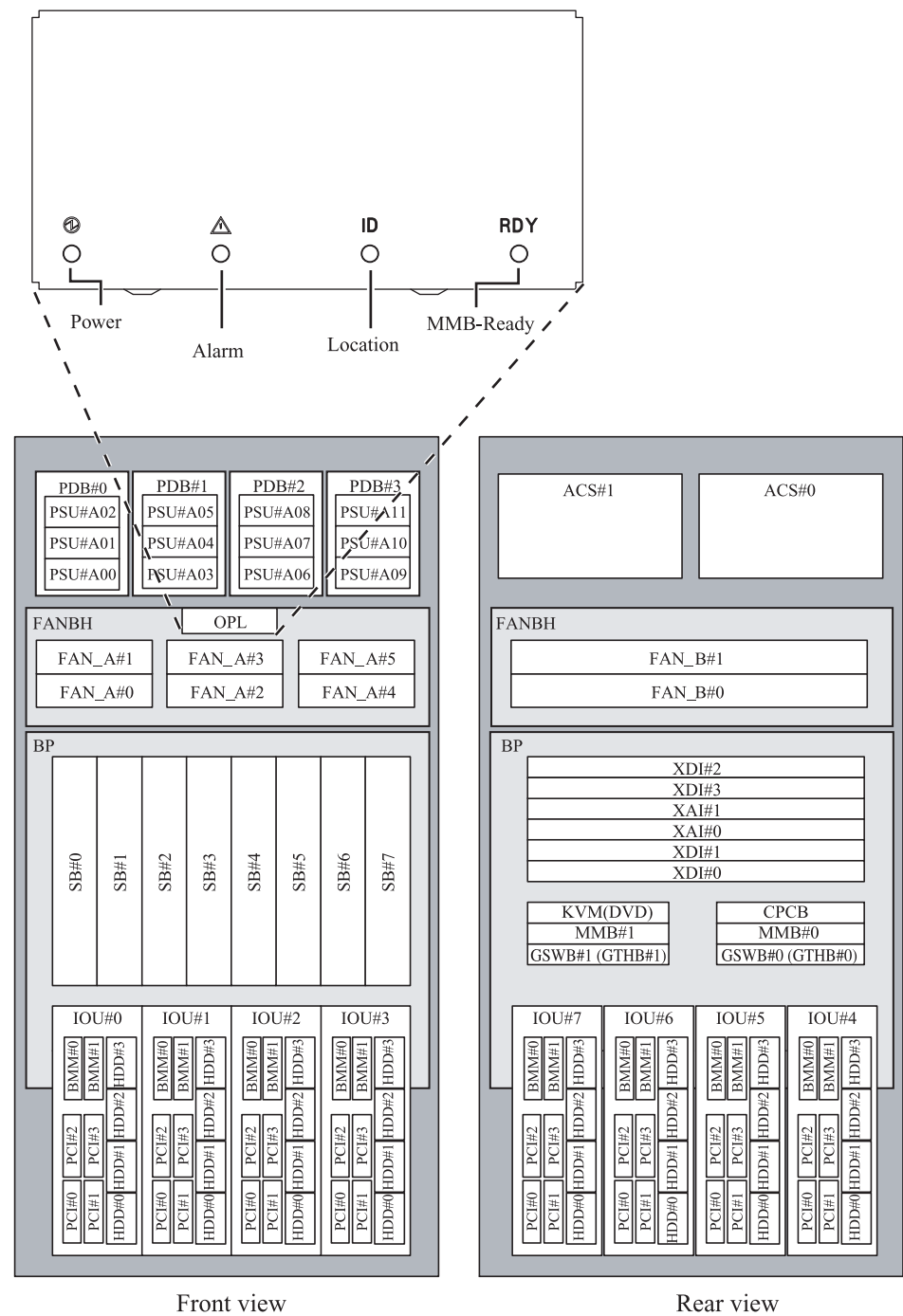


Figure 2.1 OP-Panel location (PRIMEQUEST 580A/540A/580/540/480/440)

SB

The figure below shows the locations of the system boards (SB) and the LEDs on an SB.

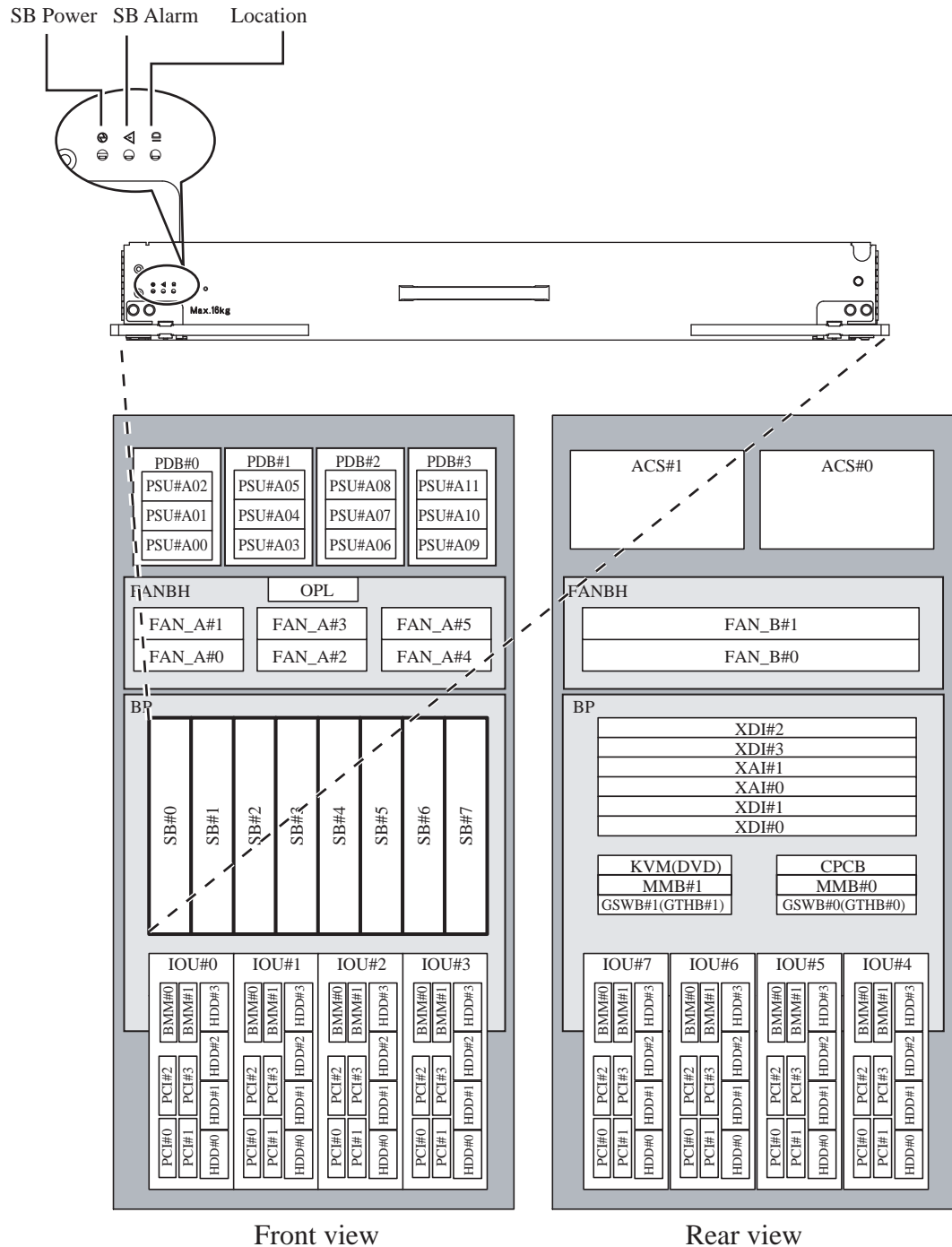


Figure 2.2 SB locations (PRIMEQUEST 580A/540A/580/540/480/440)

MMB

The figure below shows the locations of the management boards (MMB), and the external interfaces and LEDs on an MMB.

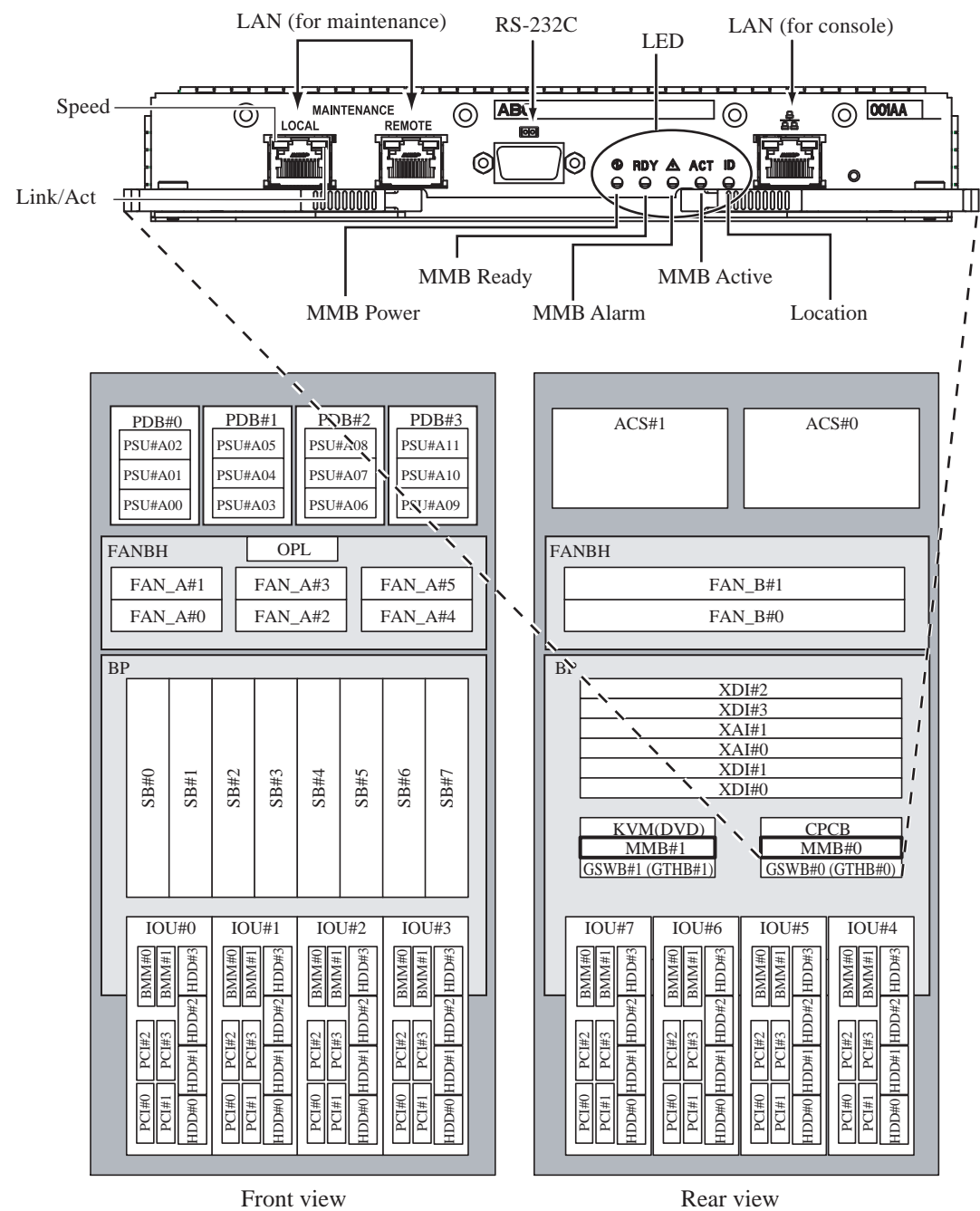


Figure 2.3 MMB location (PRIMEQUEST 580A/540A/580/540/480/440)

GSWB

The figure below shows the locations of the GSWBs, and the external interfaces and LEDs on a GSWB.

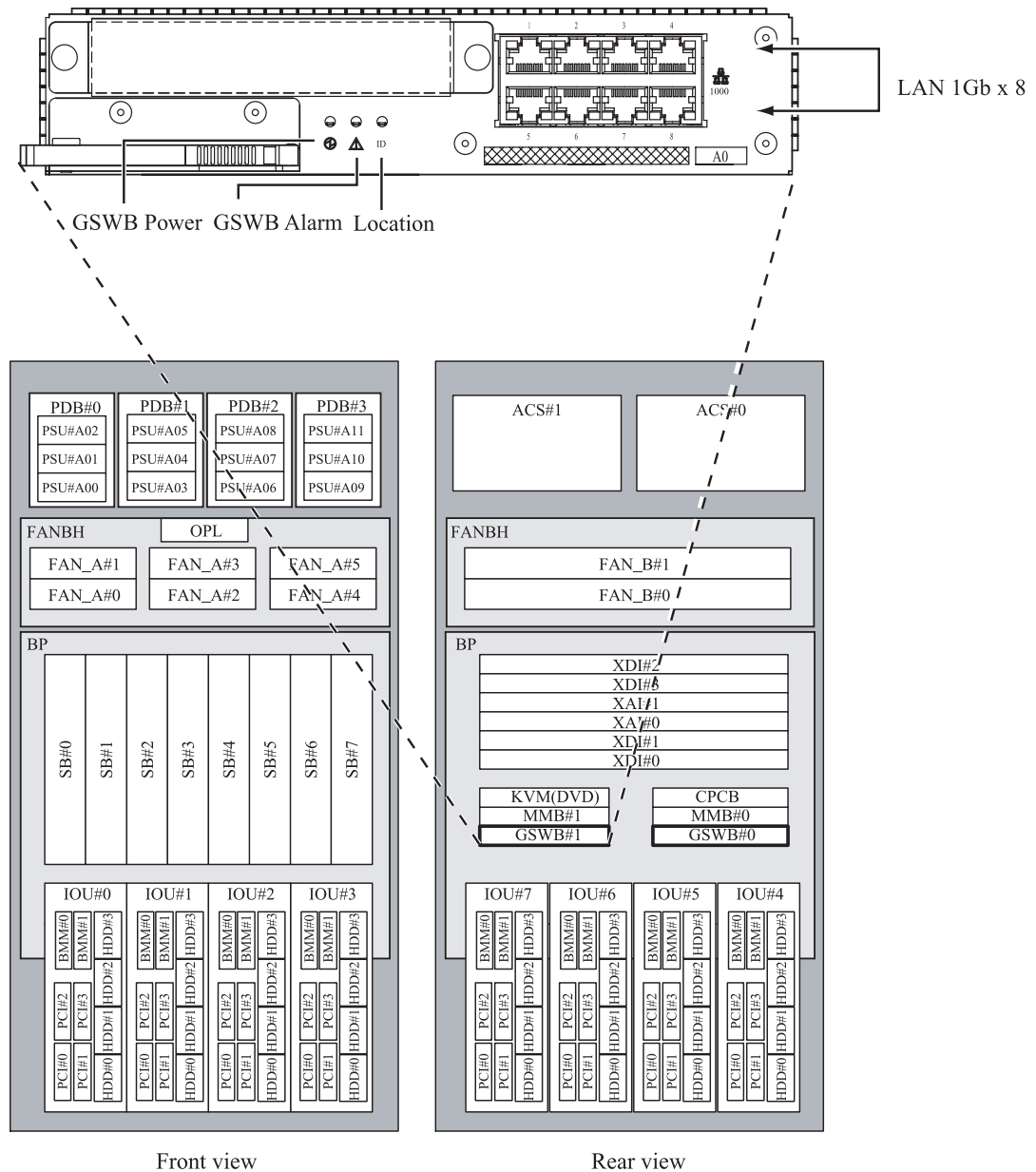


Figure 2.4 GSWB location (PRIMEQUEST 580A/540A/580/540/480/440)

GTHB

The figure below shows the locations of the GTHBs, and the external interfaces and LEDs on a GTHB.

Remarks: The GTHB can be mounted only in PRIMEQUEST 580A/540A/580/540 servers.

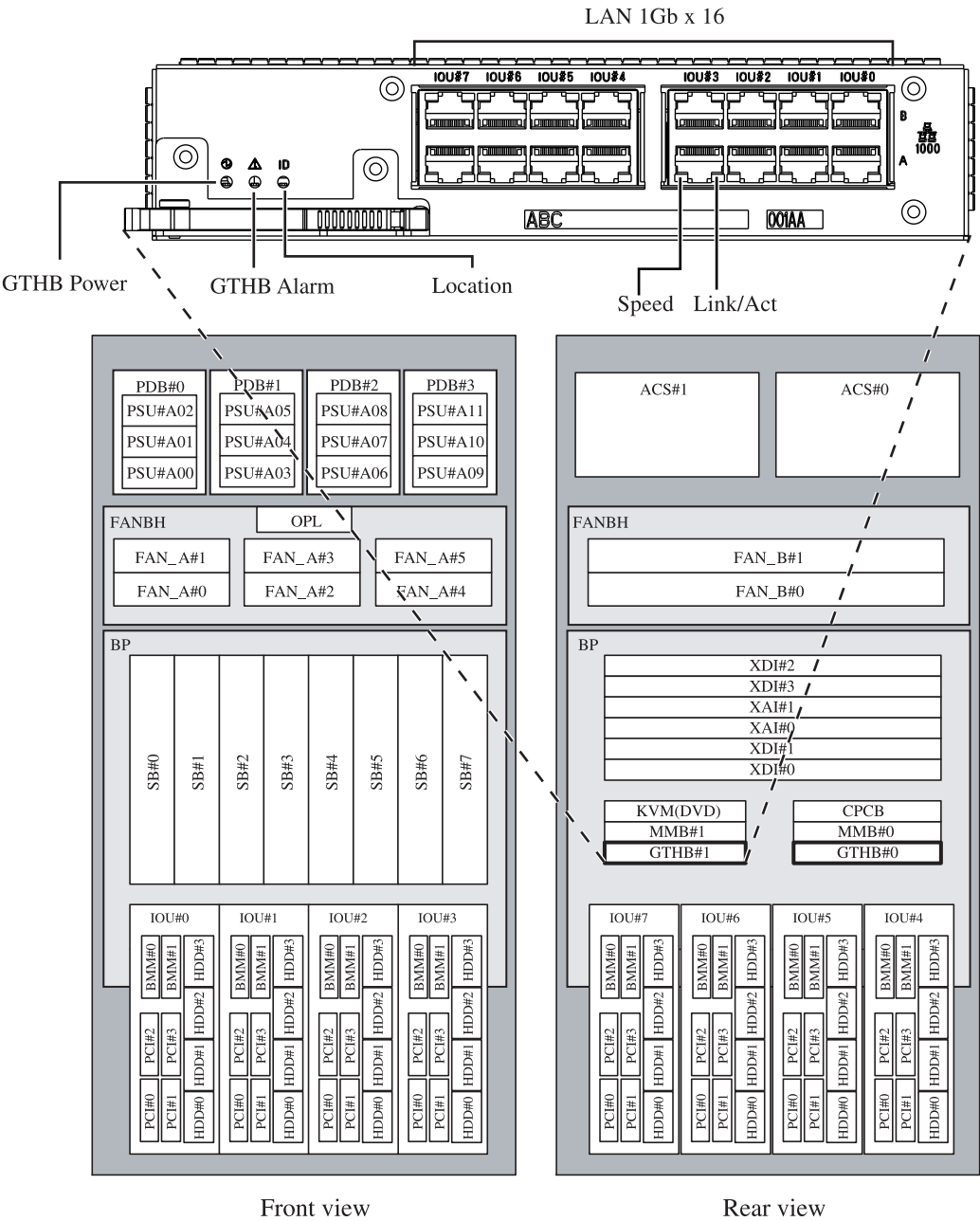


Figure 2.5 GTHB location (PRIMEQUEST 580A/540A/580/540)

IO Unit

The figure below shows the locations of the IO Units, and the external interfaces and LEDs on an IO Unit.

Remarks:

- As shown in [Figure 2.7](#), the locations of the USB ports are different between BMM A and BMM B, but the ports have the same functions.
- BMM A is mounted in the PRIMEQUEST 580/540/480/440.
BMM A or B is mounted in the PRIMEQUEST 580A/540A.

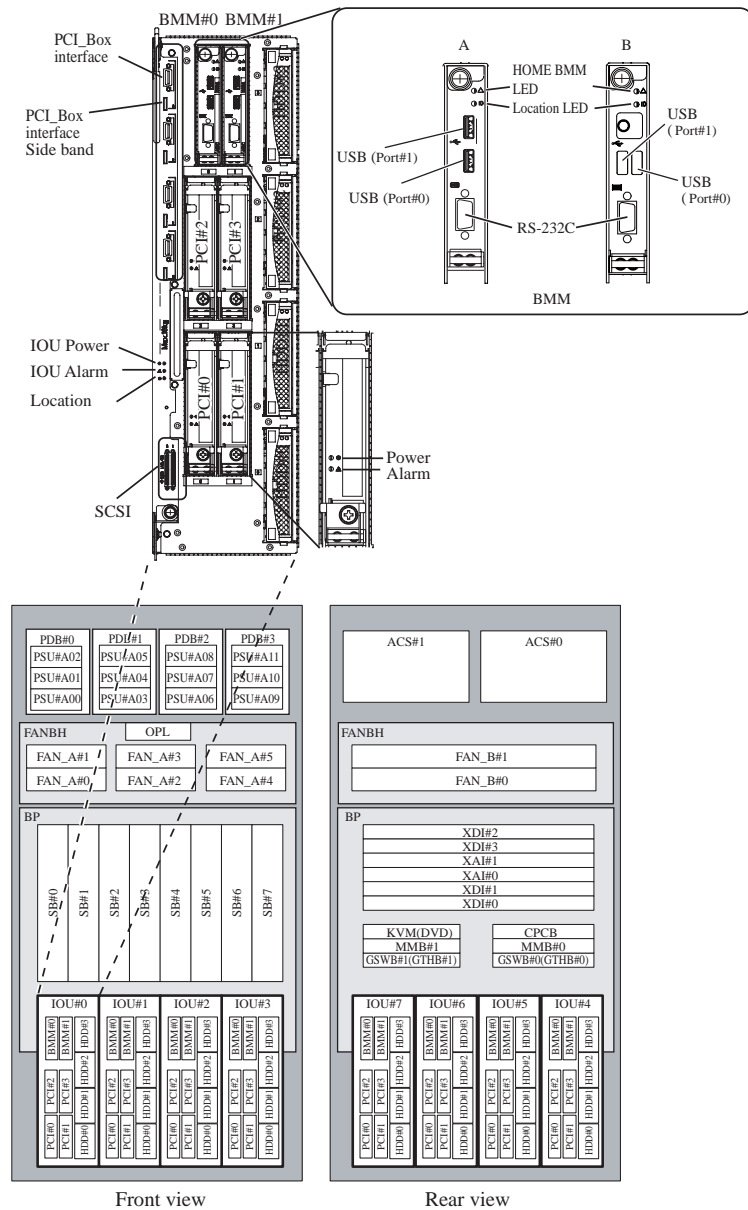


Figure 2.6 IO Unit location (PRIMEQUEST 580A/540A/580/540/480/440)

XAI

The figure below shows the locations of the XAI and LEDs on an XAI.

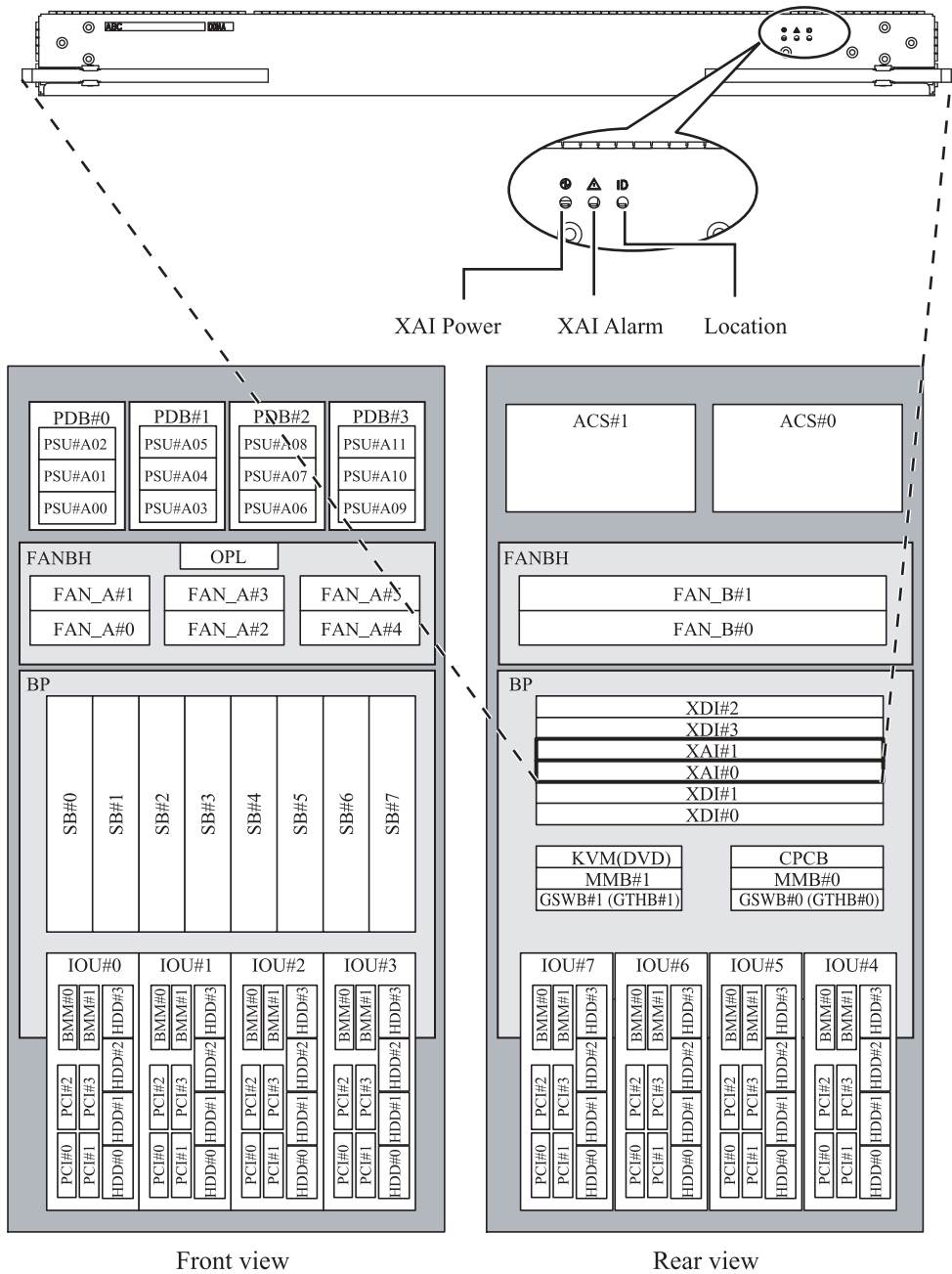


Figure 2.7 XAI location (PRIMEQUEST 580A/540A/580/540/480/440)

XDI

The figure below shows the locations of the XDIs and LEDs on an XDI.

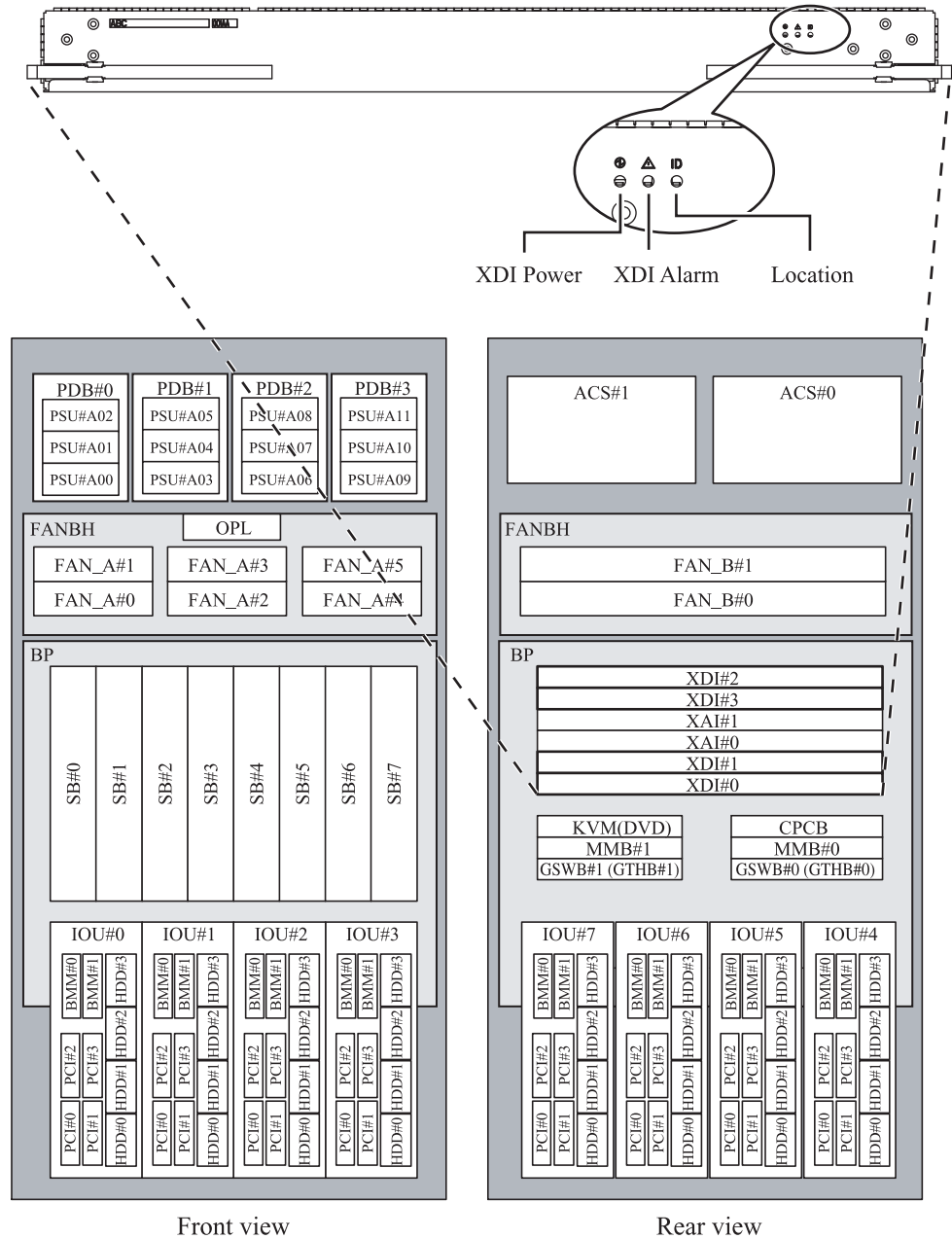


Figure 2.8 XDI location (PRIMEQUEST 580A/540A/580/540/480/440)

CPCB

The figure below shows the CPCB location, and the locations of the external interfaces and LEDs on a CPCB.

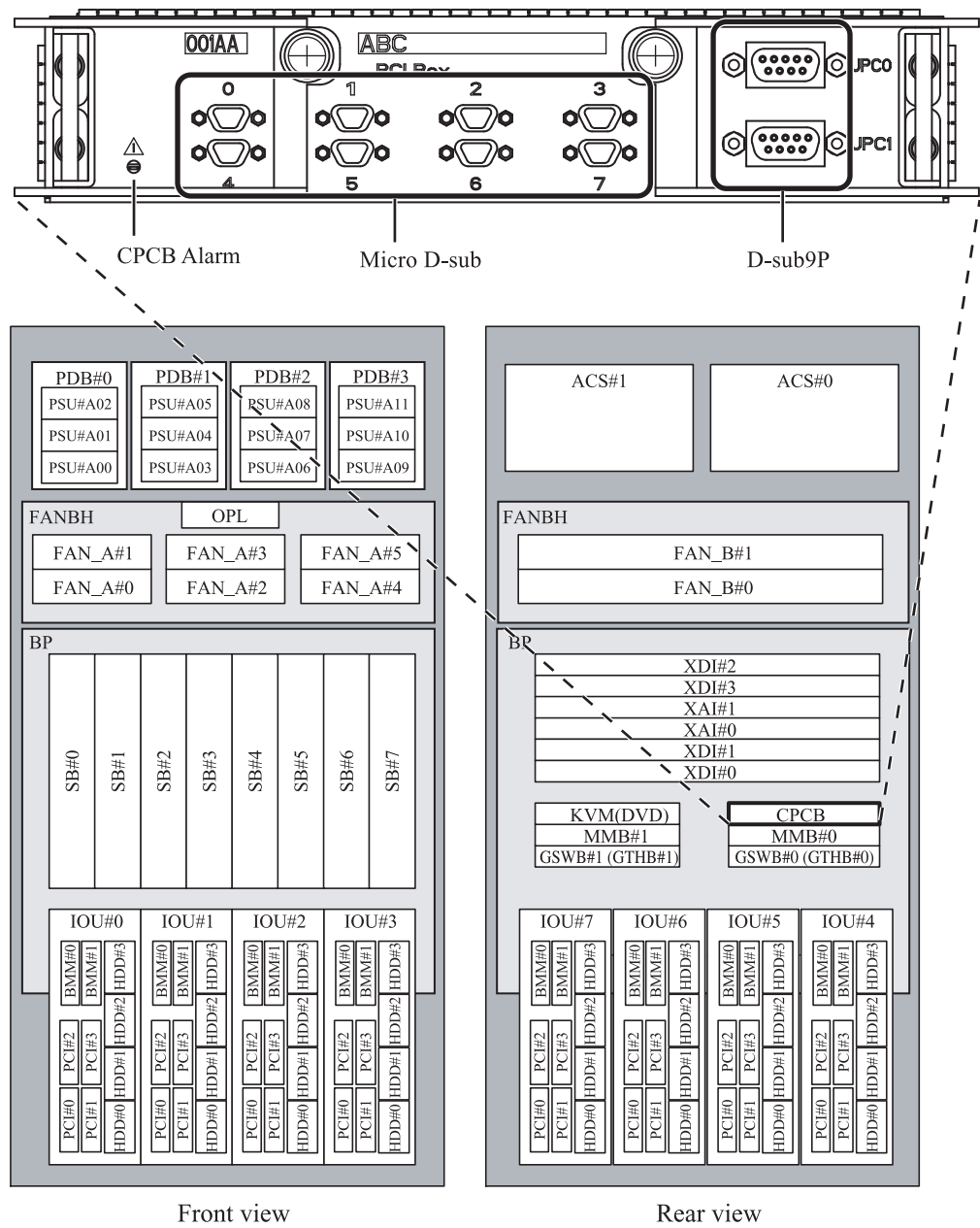


Figure 2.9 CPCB location (PRIMEQUEST 580A/540A/580/540/480/440)

KVM interface unit

The figure below shows the KVM interface unit location, and the external interfaces and LEDs on a KVM.

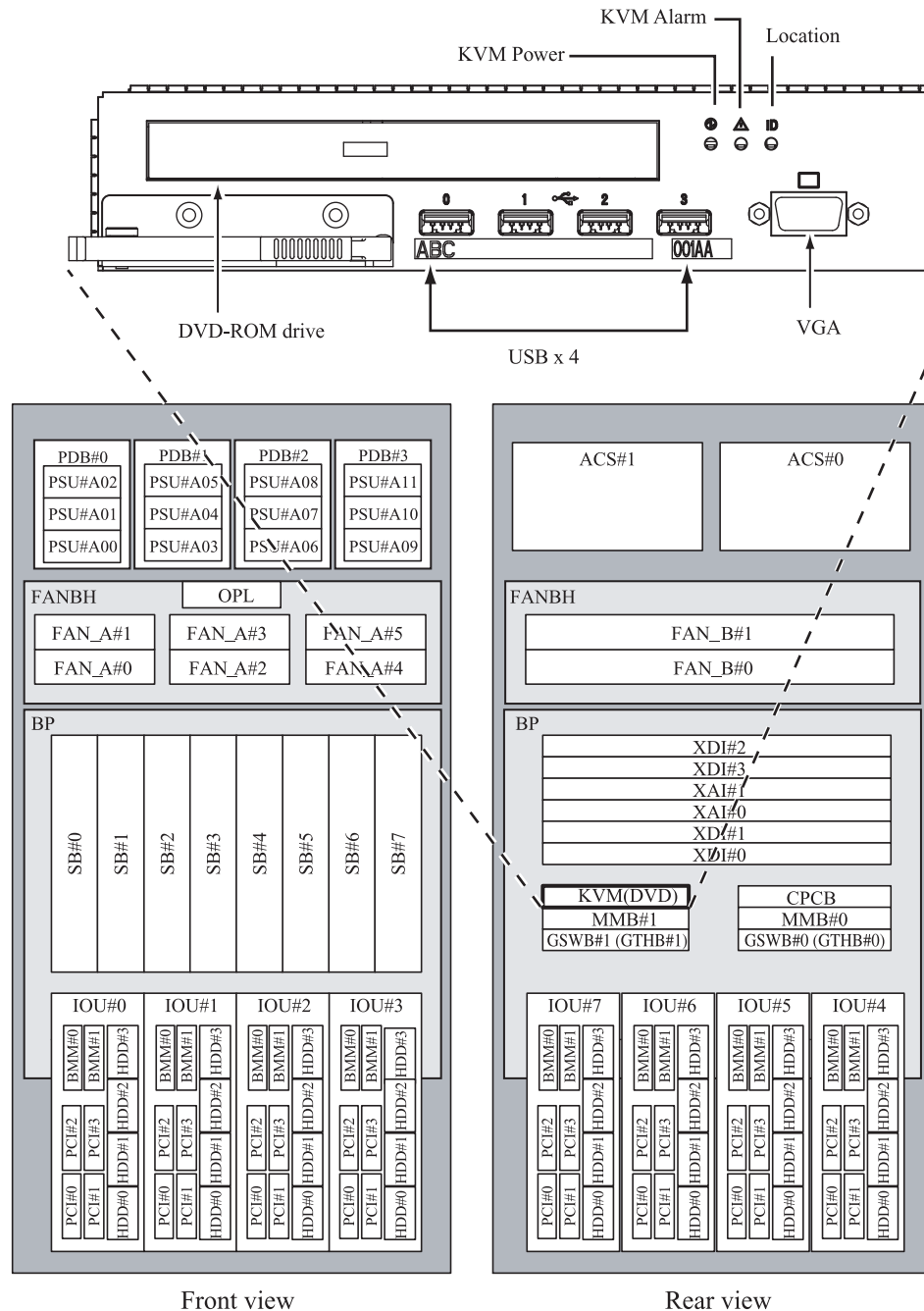


Figure 2.10 KVM location (PRIMEQUEST 580A/540A/580/540/480/440)

2.2 Component, LED, and Interface Locations (PRIMEQUEST 520A/520/420)

This section shows the physical locations of individual components, LEDs, and interfaces.

Remarks:

- Only the PRIMEQUEST 520A/520 supports BMM#1.
- Only the PRIMEQUEST 520A/520 can use PCI#2 and PCI#3.

OP-panel

The figure below shows the locations of the OP-Panel and LEDs.

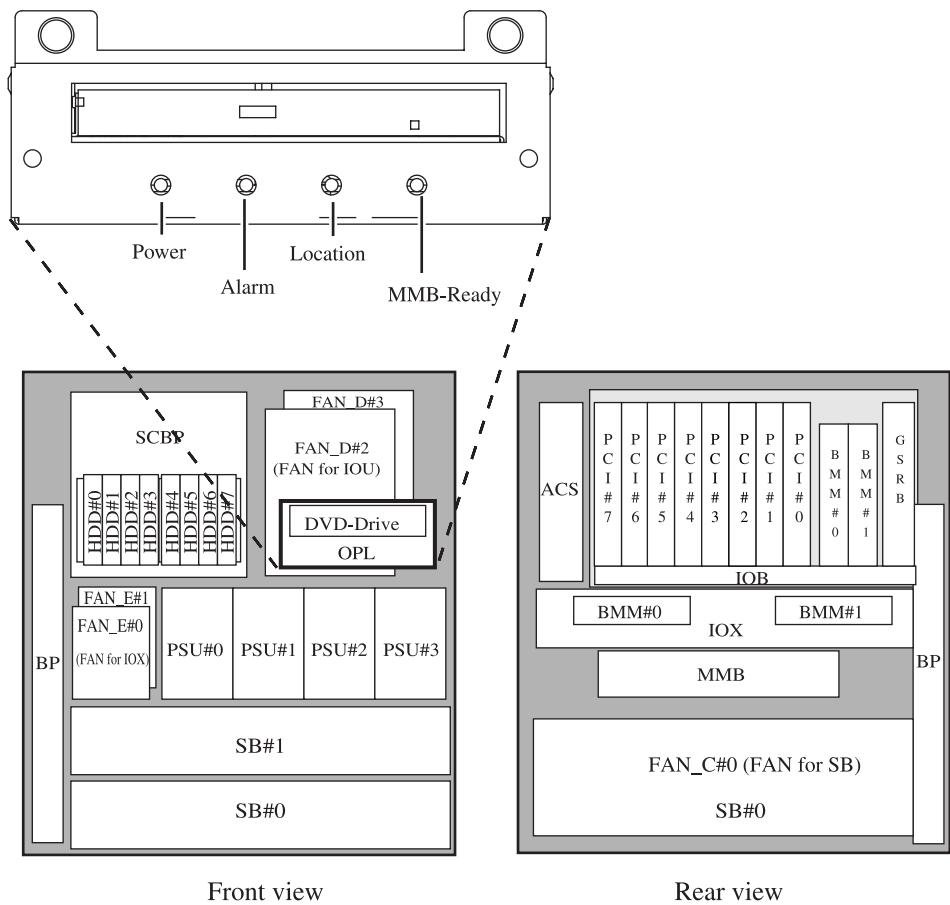


Figure 2.11 OP-Panel location (PRIMEQUEST 520A/520/420)

SB

The figure below shows the locations of the system boards (SB) and the LEDs on an SB.

Note: The LEDs on an SB can be checked from the left side of the main unit.

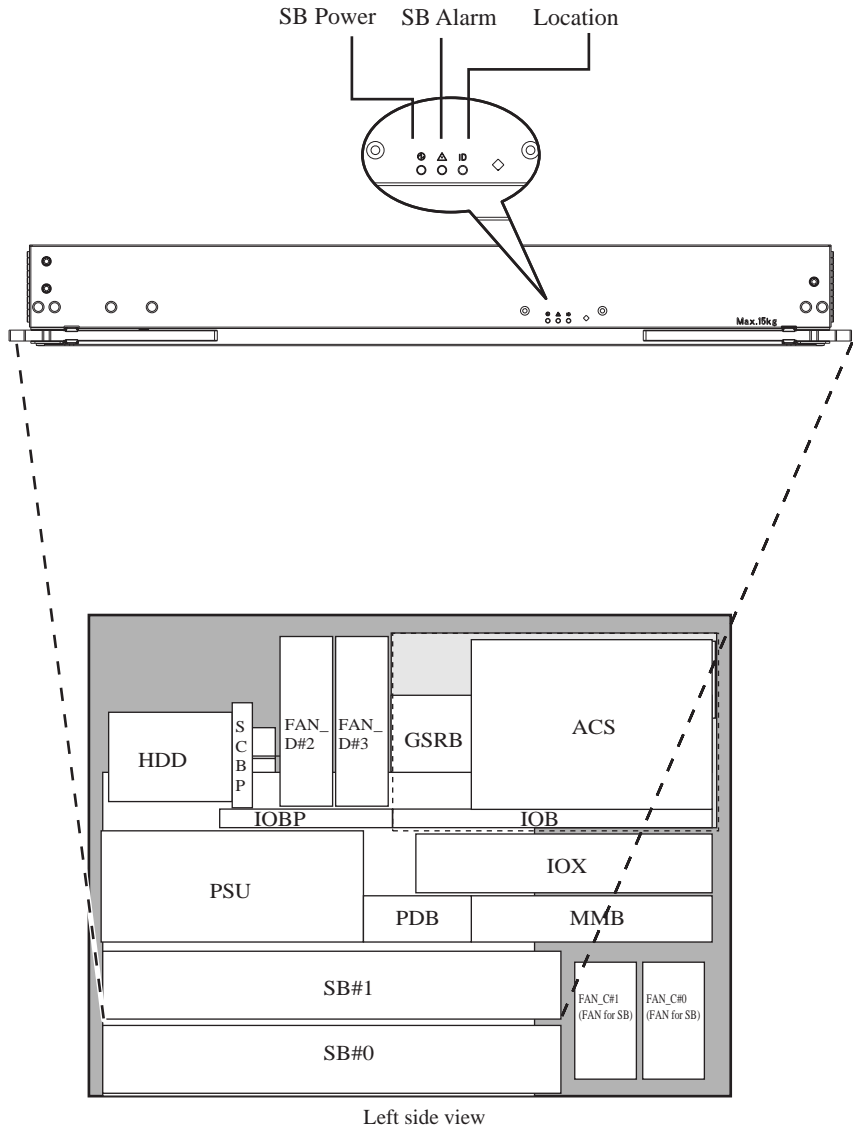


Figure 2.12 SB locations (PRIMEQUEST 520A/520/420)

MMB

The figure below shows the locations of the management boards (MMB), and the external interfaces and LEDs on an MMB.

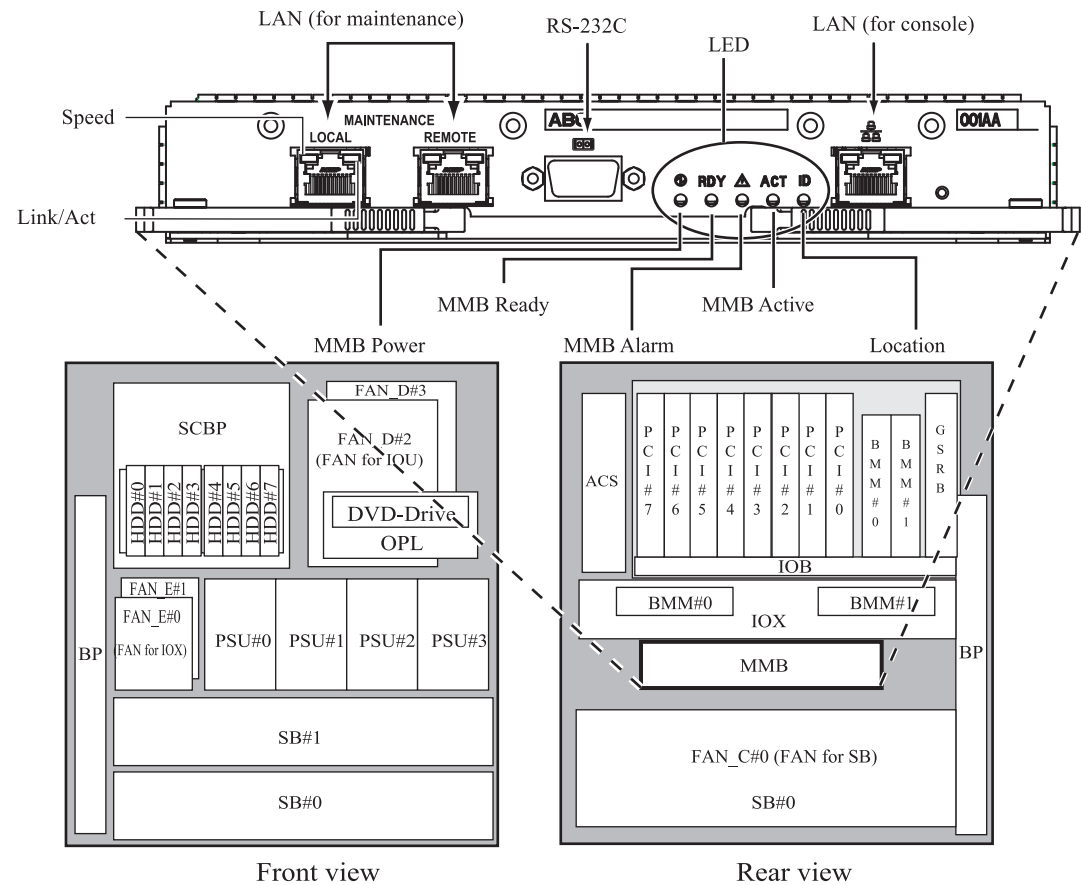


Figure 2.13 MMB location (PRIMEQUEST 520A/520/420)

IO Unit

The figure below shows the locations of the IO Units, and the external interfaces and LEDs on an IO Unit.

Remarks:

- Only the PRIMEQUEST 520A/520 supports BMM#1.
- Only the PRIMEQUEST 520A/520 can use PCI#2 and PCI#3.

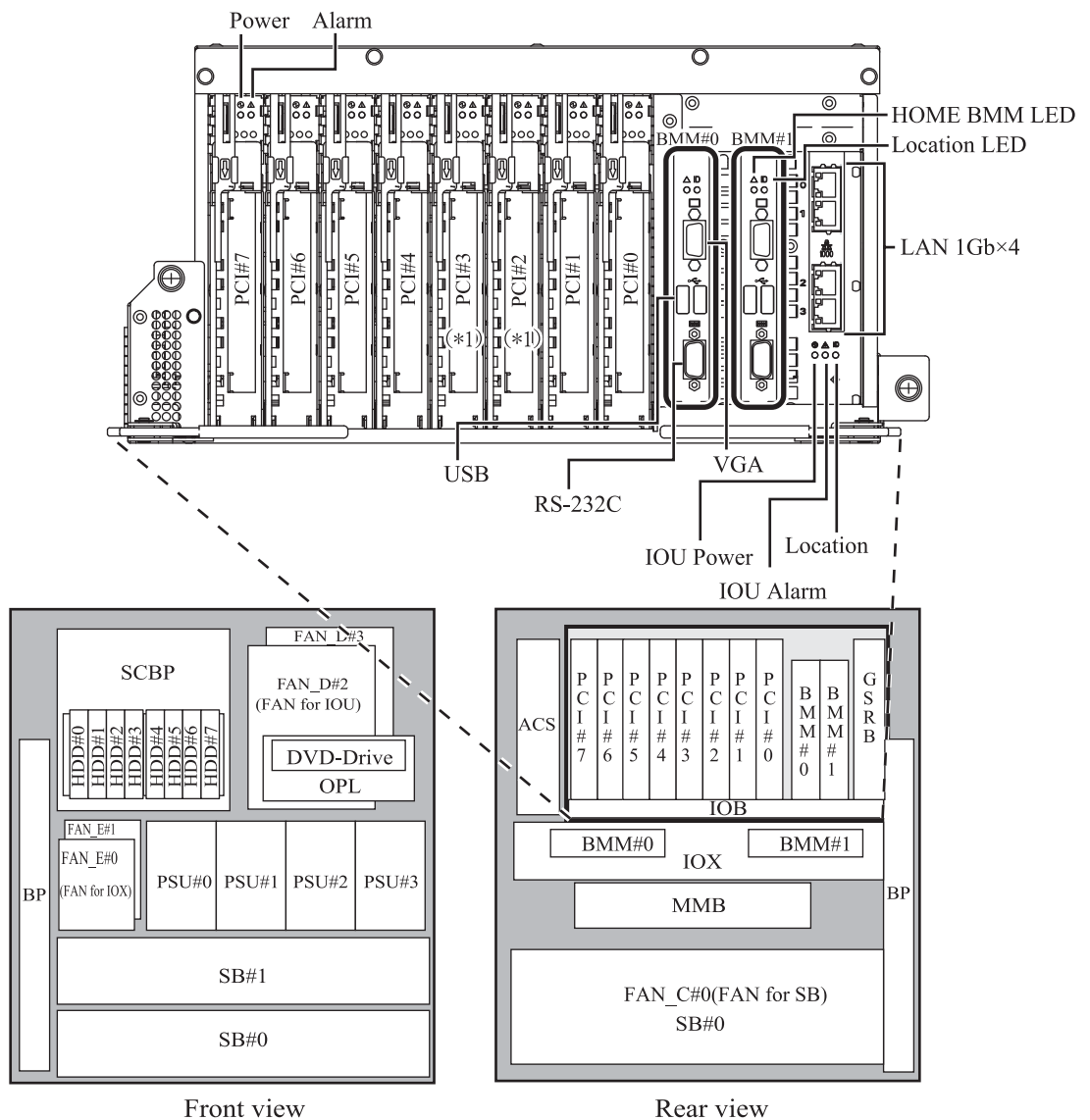


Figure 2.14 IO Unit location (PRIMEQUEST 520A/520/420)

IOX

The figure below shows the location of the IOX, and the external interfaces and LEDs on an IOX.

Remarks:

- Only the PRIMEQUEST 520A/520 supports BMM#1.
- Only the PRIMEQUEST 520A/520 can use PCI#2 and PCI#3.

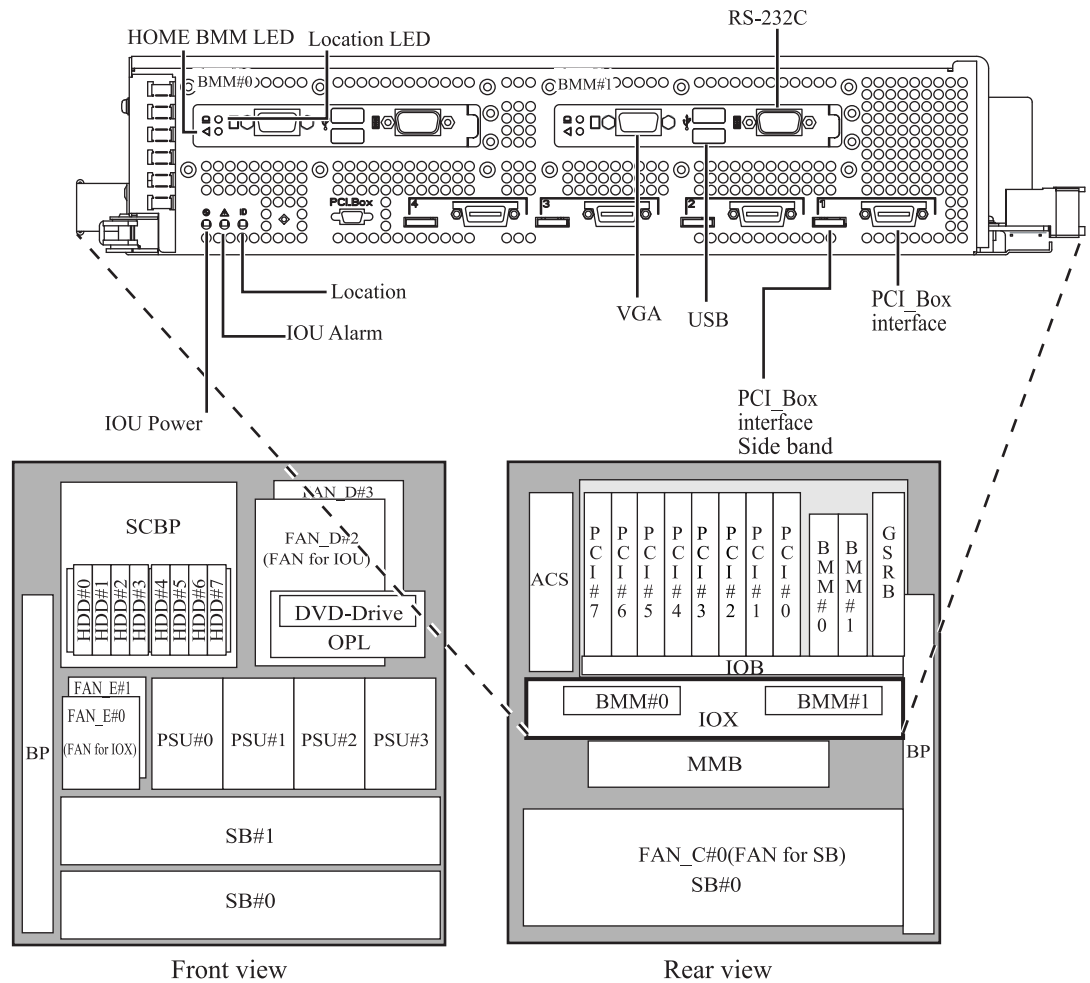


Figure 2.15 IOX location (PRIMEQUEST 520A/520/420)

CHAPTER 3 Hot Plug

3.1 Overview of Hot Plugging

This appendix describes procedures for hot plugging PCI cards in the PRIMEQUEST-series machine. The hot plugging procedures include parts that are common to every type of card and parts that require additional steps depending on the functions of the card or driver used.

The appendix describes the operations required for every type of card (e.g. power supply unit operations) and the operations applicable to specific combinations of card types and software. For details on card and software products not covered in the appendix, see the respective product manuals.

Remarks:

- This section explains hot plugging in Linux.
- Windows Server 2008: See the PRIMEQUEST 500A/500 Series Microsoft Windows Server 2008 User's Guide (C122-E087EN).
- Windows Server 2003: Hot swapping of PCI cards is not supported.

General workflow

This section provides the OS and subsystem instructions (commands and editing of setup files) that are necessary for adding, removing, and swapping cards and physical manipulation of hardware.

Before performing work according to the OS and subsystem instructions (commands and editing of setup files) described in the section, be sure to see the related product manuals, check the command syntax, and confirm the effect of the work on the system.

- [General workflow](#) (→ 3.2.1)

Common hot plugging procedure

This section describes the common procedures for adding, deleting, and swapping PCI cards of every type. In addition to these common procedures, additional steps are required for specific types of cards, and the procedures with these steps are described in "Hot plugging particular cards."

- [Common Procedures for Hot Plugging PCI Cards \(→ 3.3\)](#)

Hot plugging particular cards

This section describes procedures with the additional steps required for specific types of cards. The section describes the procedures for NICs and FC cards (also referred to as HBAs).

- [Hot Plugging a Network Card \(→ 3.4\)](#)
- [Hot Plugging a SCSI Card \(FC Card\) \(→ 3.5\)](#)

For details on the work for other types of cards that require their own procedures, see the related hardware and software manuals as well as the other portions of this appendix. The cards covered in this section (NICs and FC cards) are usually used in combination with duplication software (PRIMECLUSTER GLS (GLS), PRIMECLUSTER GDS (GDS), ETERNUS multipath driver). The section describes procedures for these cards used in combination with the duplication software and procedures for these cards used independently.

Note:

The procedures contain names of commands for manipulating software. As described above, however, different operands may be specified and additional operations may be required, depending on the configuration.

Therefore, when actually performing the operations, be sure to refer to the related product manuals.

3.2 Hot Plugging Procedure

3.2.1 General workflow

This section shows the general workflow in hot plugging for adding, removing, and swapping cards.

The following procedures are the general procedures required for every type of card compatible with the current version of PCI Hot Plug supported by Linux. (Cards for which no match can be found in the framework of this document may be supported in the future. When actually performing the operations, be sure to refer to the related product manuals.) An operation in parentheses is a required one for a specific type of PCI card, and the details of each operation vary depending on the combination of the card type and software used.

Addition procedure

- 1 (Preparation for adding a card)
- 2 Make sure that power to the target slot is off.
- 3 Insert the card into the slot.
- 4 Turn on power to the slot.
- 5 (Post-addition processing)

Removal procedure

- 1 (Preparation for removing a card)
- 2 Turn off power to the target slot.
- 3 Remove the card from the slot.
- 4 (Post-removal processing)

Swapping procedure

- 1 (Preparation for swapping a card)
- 2 Turn off power to the target slot.
- 3 Swap the card.
- 4 Turn on power to the slot.
- 5 (Post-swap processing)

3.2.2 Installation of a PCI Hot Plug driver

Before hot plugging of a specific type of card, a Hot Plug driver must be installed on the system. The power operation procedure is a common one. Among other things, the next section also describes the power operation procedure.

First, the PCI Hot Plug function must be enabled as a prerequisite for hot plugging.

For hot plugging of the PCI-X card, execute the command below to install the shpchp module. This operation is required only once before hot plugging the PCI-X card.

```
# modprobe shpchp
```

For hot plugging of the PCI-Express card, execute the command below to install the pciehp module. This operation is required only once before hot plugging the PCI-Express card.

```
# modprobe pciehp
```

The modprobe command also automatically incorporates the modules required for incorporating the specified module.

3.2.3 Power operation procedure

When a PCI card is physically added, removed, or swapped, power to its slot must be controlled via the OS.

First, determine the target slot number based on the physical location of the slot of the PCI card.

The following description assumes that the target slot number is 7. The bus numbers in the procedure are examples. When actually performing this operation, replace these numbers with the actual bus numbers.

Confirm the target slot numbers according to [Tables 5.4 to 5.6 in CHAPTER 5, "Physical Locations and Bus Numbers."](#) For the mounting locations, see [Figure 2.6, "IO Unit location \(PRIMEQUEST 580A/540A/580/540/480/440\)."](#) or [Figure 2.14, "IO Unit location \(PRIMEQUEST 520A/520/420\)."](#) in [CHAPTER 2, "Physical Locations of Components."](#)

3.2.3.1 Checking the power status

Check for the following directory, which corresponds to the target slot.

```
/sys/bus/pci/slots/0 - n : slot number
```

Note: For Red Hat Enterprise Linux 5 or SUSE LINUX Enterprise Server 10, the directory name under `/sys/bus/pci/slots` is "BUS_no._slot_no". The BUS and slot numbers are indicated as four decimal digits.

Whether or not the PCI card in the slot is enabled can be checked by displaying the contents of the file named "power" in this directory.

```
# cat /sys/bus/pci/slots/7/power
```

If 0 is displayed, the PCI card is disabled. If 1 is displayed, it is enabled.

3.2.3.2 Power-on and power-off procedures

If 0 is written to "power" in the directory corresponding to the target slot, the PCI card in the slot is disabled and the slot can be disconnected as shown below. This operation turns off the associated LED.

```
# echo 0 > /sys/bus/pci/slots/7/power
```

The above operation excludes devices connected to an adapter, if applicable, from the system at the same time.

Note:

Be sure to control power via the OS.

When 1 is written to "power" in the directory corresponding to the disabled slot, the slot becomes enabled and can be used again.

```
# echo 1 > /sys/bus/pci/slots/7/power
```

This operation incorporates devices (and drivers) connected to an adapter, if applicable, into the system at the same time.

Note:

The card and its driver must be checked to confirm that the card has been correctly incorporated after power is turned on. Since this procedure varies depending on the specified card and driver to be incorporated, see the manuals for the card and driver.

3.3 Common Procedures for Hot Plugging PCI Cards

This section describes procedures for adding, removing, and swapping PCI cards that do not require any additional steps, including editing setting files and issuing commands (as described in [3.4](#) and [3.5](#)). Be sure to use OS commands for power operations.

3.3.1 Addition procedure

- 1 Make sure that power to the target PCI slot is off.
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 2 Add a PCI card.
- 3 Turn on power to the PCI slot.
For details, see [Section 3.2.3, "Power operation procedure."](#)

3.3.2 Removal procedure

- 1 Turn off power to the target PCI slot.
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 2 Remove the PCI card.

3.3.3 Swapping procedure

- 1 Turn off power to the target PCI slot.
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 2 Swap the PCI card.
- 3 Turn on power to the PCI slot.
For details, see [Section 3.2.3, "Power operation procedure."](#)

Note: A precaution on PSA with SUSE

When SUSE is used, PSA cannot automatically recognize added and deleted devices. Therefore, after adding or deleting a card, you must execute the command below for PSA so that it can recognize the added or deleted device. After deleting a card to be replaced, execute said command and wait at least 30 seconds before adding a new card since PSA requires about 30 seconds to recognize a device.

```
/opt/FJSPsa/sh/force_search.sh -a
```

3.4 Hot Plugging a Network Card

Hot plugging a network card (referred to as a network interface controller (NIC), in this document) requires additional steps as well as the procedures described in [Section 3.3](#).

This section describes the procedures applicable to a NIC used in combination with GLS and procedures applicable to a NIC used without GLS. (For the common procedures, see [Section 3.3, "Common Procedures for Hot Plugging PCI Cards."](#))

The section covers the following topics:

- [Hot plugging a network card used independently \(used without GLS\)](#) (→ [3.4.1](#))
- [Hot plugging a network card under GLS control](#) (→ [3.4.2](#))

Their common methods for editing the necessary setting files, applying them in the system, and verifying installation are described in the following sections:

- [Handling kudzu](#) (→ [3.4.3](#))
- [Installation verification procedure](#) (→ [3.4.5](#))

Remarks: The only maintenance mode supported for network cards in cluster interconnects is rolling maintenance.

3.4.1 Hot plugging a network card used independently (used without GLS)

This section describes procedures for hot plugging a network card used independently (used without GLS).

The "*" symbol at the end of a step indicates the step is the same as that in the corresponding common procedure for PCI cards. The target NIC of hot plugging is assumed to have the ethX interface.

3.4.1.1 Addition procedure

The addition procedure varies depending on whether RedHat or SUSE is used. See the procedure for the respective operating system.

Note: When adding two or more NICs, be sure to add them one by one; otherwise, they may be set incorrectly.

RedHat

- 1 Confirm that a PCI hot plug driver is installed.
If not installed, install it according to [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

```
# /sbin/lsmmod | grep shpchp
shpchp                206984    0
```

- 2 Check the existing interface names.
Execute the following command and check the interface names.

```
# /sbin/ifconfig -a
```

- 3 Insert the NICs into the PCI slots.
- 4 Turn on the power of the PCI slots.
For details, see [Section 3.2.3.2, "Power-on and power-off procedures"](#).

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: Slot number

- 5 Conform the hardware addresses.
When the power is turned on, an interface (ethX) is created for each of the added NICs. Execute the following command, compare the result with that in Step 2, and then check the names of the created interfaces.

```
# /sbin/ifconfig -a
```

Use the ifconfig (8) command to check the hardware address (HWaddr) of a created interface. When one NIC includes two or more interfaces, confirm the hardware address of each interface created.

In the example below, dev32084 and eth0 are assigned as temporary interface names.

```
Example: # /sbin/ifconfig -a
...
dev32084  Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:41
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab20000-8ab40000

eth0      Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:40
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab00000-
...

```

6 Create an interface setting file.

Set the interface setting file (/etc/sysconfig/network-scripts/ifcfg-ethX) as shown below. In "HWADDR," set the hardware address that was checked in Step 5. When adding two or more NICs, or an NIC including two or more interfaces, create the file for each interface.

```
Example:
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:0E:0C:70:C3:40
BROADCAST=192.168.16.255
IPADDR=192.168.16.1
NETMASK=255.255.255.0
NETWORK=192.168.16.0
ONBOOT=yes
TYPE=Ethernet

```

Remarks: The interface setting file is required to automatically activate an interface at system startup.

- 7 Add the created interfaces to the modprobe.conf file.

This correlates the interfaces and drivers to each other. An example of /etc/modprobe.conf is shown below.

```
Example:
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias eth0 e1000 ← Added
```

- 8 Activate the created interfaces.

Execute the following command to activate the interfaces. Activate all necessary interfaces.

```
# /sbin/ifup ethX
```

SUSE

- 1 Confirm that a PCI Hot Plug driver is installed.

If not installed, install it according to [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

```
Example: # /sbin/lsmo d | grep shpchg
shpchg           212056  0
```

- 2 Check the existing interface names.

Execute the following command, and check the existing interface names.

```
# /sbin/ifconfig -a
```

- 3 Insert each NIC into a PCI slot.

- 4 Turn on the power to the PCI slots.

For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: Slot number

- 5 Confirm the hardware addresses.

When the power is turned on, an interface (ethX) is created for each added NIC. Execute the following command, compare the results with those in step 2, and confirm the hardware addresses (HWaddr) of the created interfaces.

```
# /sbin/ifconfig -a
```

For each NIC that includes two or more interfaces, confirm the hardware addresses (HWaddr) of all the interfaces.

In the example below, 00:0E:0C:70:C3:41 and 00:0E:0C:70:C3:40 are the hardware addresses (HWaddr) of the interfaces.

```
Example: # /sbin/ifconfig -a
...
eth0  Link encap:Ethernet HWaddr 00:0E:0C:70:C3:41
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
      Memory:8ab20000-8ab40000
eth1   Link encap:Ethernet HWaddr 00:0E:0C:70:C3:40
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
      Memory:8ab00000-
...
```

- 6 Activate YaST to configure the network.

Activate YaST. From the menu, select [Network Devices] -> [Network Card] to go to the network card selection window. Select the NICs with the hardware addresses (HWaddr) confirmed in step 5, reconfigure the settings required, and then exit YaST.

3.4.1.2 Removal procedure

The removal procedure varies depending on whether RedHat or SUSE is used. See the procedure for the respective operating system.

Note: To remove two or more NICs, be sure to remove them one by one; otherwise, they may be set incorrectly.

RedHat

- 1 Confirm that a PCI hot plug driver is installed.

If not installed, install it according to [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

Checking procedure:

```
# /sbin/lsmmod | grep shpc
shpchp                206984    0
```

- 2 Check the PCI slot numbers that have interfaces installed.

Use the information of the setting file and OS to check where the interfaces are installed (because the interface names specified by users may differ from those managed by the OS).

First, check the hardware address of an interface to be removed.

```
Example: # grep HWADDR /etc/sysconfig/network-scripts/ifcfg-eth0
HWADDR=00:0E:0C:70:C3:40
```

Check the interface name that has this hardware address and is managed by the OS.

```
Example: # grep -il "00:0E:0C:70:C3:40" /sys/class/net/*/address
/sys/class/net/eth0/address
```

This recognizes the interface name managed by the OS. Next, check the bus address of the PCI slot where this interface is installed.

```
Example: # ls -l /sys/class/net/eth0/device
lrwxrwxrwx 1 root root 0 Sep 29 09:26
                /sys/class/net/eth0/device ->
                ../../../../devices/pci0000:00/0000:00:01.2/
0000:08:00.2/0000:0b:01.0
```

See [Table 5.4](#) to [Table 5.6](#), "Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines" and check the slot number. The table to be referenced depends on the PRIMEQUEST model and PCI address mode. For details, see [Section 3.2.3, "Power operation procedure."](#)

When an NIC includes two or more interfaces, all of them must be removed. Use the procedure described below to check all interfaces that have the same bus address.

```
Example: # ls -l /sys/class/net/*/device | grep "0000:0b:01"
lrwxrwxrwx 1 root root 0 Sep 29 09:26
                /sys/class/net/eth0/device
                -> ../../../../devices/pci0000:00/0000:00:01.2/
0000:08:00.2/0000:0b:01.0
lrwxrwxrwx 1 root root 0 Sep 29 09:26
                /sys/class/net/eth1/device
                -> ../../../../devices/pci0000:00/0000:00:01.2/
0000:08:00.2/0000:0b:01.1
```

When two or more interfaces are indicated as shown in the example, all of them are included in the same NIC. If only one interface is shown, the following procedure is not required. In such case, proceed to Step 3.

Check the hardware address from the interface names managed by the OS.

```
Example: # cat /sys/class/net/eth1/address
00:0e:0c:70:c3:41
```

Check the interface name that has this hardware address.

```
Example: # grep -il "00:0e:0c:70:c3:41" /etc/sysconfig/network-scripts/
ifcfg-eth*
/etc/sysconfig/network-scripts/ifcfg-eth1
```

These operations indicate that the interface that exists in the same NIC as eth0 is eth1.

3 Deactivate the NIC.

Note: Deactivate all interfaces that were checked in Step 2.

```
# /sbin/ifdown ethX
```

4 Turn off the power of the PCI slots (*).

When the power is turned off, the interfaces (ethX) are removed. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

n: Slot number

5 Remove the NIC from each PCI slot.

6 Remove the interface setting file..

```
# rm /etc/sysconfig/network-scripts/ifcfg-ethX
```

7 Remove the interface settings of each interface removed from modprobe.conf..
Remove the correspondence between the interfaces and drivers that is no longer required.

Example:

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias eth0 e1000 ← Removed
```

SUSE

- 1 Confirm that a PCI Hot Plug driver is installed.

If not installed, install it according to [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

```
Example: # /sbin/lsmmod | grep shpchp
shpchp          212056  0
```

- 2 Check the slot numbers of PCI slots that have interfaces installed.

Execute the following command, and check the bus addresses of the PCI slots in which the interfaces (ethX) to be removed are installed.

```
Example: # ls -l /sys/class/net/ethX/device
lrwxrwxrwx 1 root root 0 Sep 29 09:26 /sys/class/net/eth0/device ->
../../../../devices/pci0000:00/0000:00:01.2/ 0000:08:00.2/0000:0b:01.0
```

See [Table 5.4](#) to [Table 5.6](#), which show the correspondence between physical mounting locations and bus numbers in PRIMEQUEST-series machines, and check the slot numbers. The table to be referenced depends on the PRIMEQUEST model and PCI address mode. For details, see [Section 3.2.3, "Power operation procedure."](#)

For each NIC that includes two or more interfaces, all the interfaces must be removed. Use the procedure described below to check for all interfaces that have the same bus address. The example below shows that the same NIC includes eth0 and eth1.

```
Example: # ls -l /sys/class/net/*/device | grep "0000:0b:01"
lrwxrwxrwx 1 root root 0 Sep 29 09:26 /sys/class/net/eth0/device
-> ../../../../devices/pci0000:00/0000:00:01.2/0000:08:00.2/0000:0b:01.0
lrwxrwxrwx 1 root root 0 Sep 29 09:26 /sys/class/net/eth1/device
-> ../../../../devices/pci0000:00/0000:00:01.2/0000:08:00.2/0000:0b:01.1
```

3 Confirm the hardware addresses.

Execute the following command, and confirm the hardware addresses (HWaddr) of the interfaces to be removed.

```
# /sbin/ifconfig
```

For each NIC that includes two or more interfaces, confirm the hardware addresses (HWaddr) of all the interfaces.

In the example below, 00:0E:0C:70:C3:41 and 00:0E:0C:70:C3:40 are the hardware addresses (HWaddr) of the interfaces.

```
Example: # /sbin/ifconfig
...
eth0  Link encap:Ethernet HWaddr 00:0E:0C:70:C3:41
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
      Memory:8ab20000-8ab40000
eth1  Link encap:Ethernet HWaddr 00:0E:0C:70:C3:40
      BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
      Memory:8ab00000-
...
```

4 Deactivate the NIC.

Note: Deactivate all the interfaces that were confirmed in step 2.

```
# /sbin/ifdown ethX
```

5 Turn off the power to the PCI slots.

When the power is turned off, the interfaces (ethX) are removed. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

6 Remove each target NIC from its PCI slot.**7 Activate YaST to configure the network.**

Activate YaST. From the menu, select [Network Devices] → [Network Card] to go to the network card selection window. Select the NICs with the hardware addresses (HWaddr) confirmed in step 3, remove the NICs, and then exit YaST.

3.4.1.3 Swapping procedure

The swapping procedure varies depending on whether RedHat or SUSE is used. See the procedure for the respective operating system.

Note: To swap two or more NICs, be sure to swap them one by one; otherwise, they may be set incorrectly.

RedHat

- 1 Confirm that a PCI hot plug driver is installed.
If not installed, install it according to [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

Checking procedure:

```
# /sbin/lsmmod | grep shpchp
shpchp                206984    0
```

- 2 Check the PCI slot numbers with the interfaces installed.
Use the information of the setting file and OS to check where the interfaces are installed (because the interface names specified by users may differ from those managed by the OS).
First, check the hardware address of an interface to be removed.

```
Example: # grep HWADDR /etc/sysconfig/network-scripts/ifcfg-eth0
HWADDR=00:0E:0C:70:C3:38
```

Check the interface name that has this hardware address and is managed by the OS.

```
Example: # grep -il "00:0E:0C:70:C3:38" /sys/class/net/*/address
/sys/class/net/eth0/address
```

This recognizes the interface name managed by the OS. Next, check the bus address of the PCI slot where this interface is installed..

```
Example: # ls -l /sys/class/net/eth0/device
lrwxrwxrwx 1 root root 0 Sep 29 10:17 /sys/class/net/eth0/device
-> ../../../../devices/pci0000:00/0000:00:01.2/0000:08:00.2/0000:0b:01.0
```

See [Table 5.4](#) to [Table 5.6](#), "Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines" and check the slot number. The table to be referenced depends on the PRIMEQUEST model and PCI address mode. For details, see [Section 3.2.3, "Power operation procedure."](#)

When an NIC includes two or more interfaces, all of them must be removed. Use the procedure given below to check all interfaces that have the same bus address.

```
Example: # ls -l /sys/class/net/*/device | grep "0000:0b:01"
lrwxrwxrwx 1 root root 0 Sep 29 10:17 /sys/class/net/eth0/device
-> ../../../../devices/pci0000:00/0000:00:01.2/0000:08:00.2/0000:0b:01.0
lrwxrwxrwx 1 root root 0 Sep 29 10:17 /sys/class/net/eth1/device
-> ../../../../devices/pci0000:00/0000:00:01.2/0000:08:00.2/0000:0b:01.1
```

When two or more interfaces are indicated as shown in the example, all of them are included in the same NIC. If only one interface is shown, the following procedure is not required. In such case, proceed to Step 3.

Check the hardware address from the interface names managed by the OS.

```
Example: # cat /sys/class/net/eth1/address
00:0e:0c:70:c3:39
```

Check the interface name that has this hardware address.

```
Example: # grep -il "00:0e:0c:70:c3:39" /etc/sysconfig/network-scripts/
ifcfg-eth*
/etc/sysconfig/network-scripts/ifcfg-eth1
```

These operations indicate that the interface that exists in the same NIC as eth0 is eth1.

3 Deactivate the NIC.

Execute the following command to deactivate all the interfaces that were checked in Step 2.

```
# /sbin/ifdown ethX
```

Note: Deactivate all interfaces that were checked in Step 2.

4 Turn off the power of the PCI slots (*).

When the power is turned off, the interfaces (ethX) are removed. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

5 Check the existing interface names.

Execute the following command and check the interface names.

```
# /sbin/ifconfig -a
```

6 Swap each NIC.

The subsequent procedures vary with the product (RHEL-AS4 [IPF] / RHEL5 [IPF]).

- In RHEL-AS4 (IPF)

- 7 Turn on the power of the PCI slots (*).

For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: Slot number

- 8 Check the hardware addresses.

When the power is turned on, an interface (ethX) is created for each of the swapped NICs. Execute the following command, compare the result with that in Step 2, and then check the created interface name.

```
# /sbin/ifconfig -a
```

Execute the ifconfig (8) command and check the hardware address (HWaddr) of a swapped interface. When one NIC include two or more interfaces, check the hardware address of each interface.

```
Example: # /sbin/ifconfig -a
...
eth0      Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:40
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab00000-8ab20000

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:41
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab20000-8ab40000
...
```

- 9 Edit the interface setting file.

Edit the interface setting file (/etc/sysconfig/network-scripts/ifcfg-ethX) with the new hardware addresses as follows. In "HWADDR," set the hardware addresses that were checked in Step 8.

```
Example:
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:0E:0C:70:C3:40
BROADCAST=192.168.16.255
IPADDR=192.168.16.1
NETMASK=255.255.255.0
NETWORK=192.168.16.0
ONBOOT=yes
TYPE=Ethernet
```

- 10 Activate all swapped interfaces.

Activate the interfaces by executing the following command. Activate all necessary interfaces.

```
# /sbin/ifup ethX
```

- In RHEL5 (IPF)

- 7 Save /etc/ modprobe.conf.

Execute the following command to save /etc/ modprobe.conf.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
```

- 8 Save the interface setting file.

Execute the following command to save the interface setting files of all the interfaces that were checked in Step 2.

```
# mv /etc/sysconfig/network-scripts/ifcfg-ethX /etc/
sysconfig/network-scripts/ifcfg-ethX.bak
```

- 9 Turn on the power of the PCI slots (*).

For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: Slot number

- 10 Collect the latest hardware information.

Since NICs have been added, execute the following command to collect the latest hardware information.

```
# /sbin/kudzu
```

11 Restore the saved /etc/ modprobe.conf.

Execute the following command to restore the saved /etc/ modprobe.conf.

```
# mv /etc/modprobe.conf.bak /etc/modprobe.conf
```

12 Check the hardware addresses.

When the power is turned on, an interface (ethX) is created for each of the swapped NICs. Execute the following command, compare the result with that in Step 5, and then check the created interface name.

```
# /sbin/ifconfig -a
```

Execute the ifconfig(8) command and check the hardware address (HWaddr) of a swapped interface. When one NIC includes two or more interfaces, check the hardware address of each interface.

```
Example: # /sbin/ifconfig -a
...
eth0      Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:40
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab00000-8ab20000

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:70:C3:41
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Memory:8ab20000-8ab40000

...
```

13 Restore the saved interface setting file.

Execute the following command to restore the saved /etc/sysconfig/network-scripts/ifcfg-ethX.

```
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak /etc/
  sysconfig/network-scripts/ifcfg-ethX
```

14 Edit the interface setting file.

Replace the hardware addresses with the new ones. In "HWADDR," set the hardware addresses that were checked in step 12.

```
Example:
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:0E:0C:70:C3:40
BROADCAST=192.168.16.255
IPADDR=192.168.16.1
NETMASK=255.255.255.0
NETWORK=192.168.16.0
ONBOOT=yes
TYPE=Ethernet
```

15 Activate the swapped interfaces.

Execute the following command to activate the interfaces. Activate all necessary interfaces.

```
# /sbin/ifup ethX
```

SUSE

Remove the target NIC according to [3.4.1.2, "Removal procedure,"](#) and add a NIC according to [3.4.1.1, "Addition procedure."](#)

3.4.2 Hot plugging a network card under GLS control

This section describes the procedure for hot plugging for a network card that is made redundant using a GLS. A procedure that ends with an asterisk [*] is the same as that described in [Section 3.4.1, "Hot plugging a network card used independently \(used without GLS\)."](#)

For details on the GLS setting procedure and command, refer to the latest GLS manual *PRIMECLUSTER Global Link Services Configuration and Administration Guide 4.1: Redundant Line Control Function (for Linux)*. Note that the setting procedure described in this manual is for PRIMECLUSTER GLS 4.1A40. If a different GLS version is used, execute the command by checking with the GLS manual.

GLS hot plugging is supported as shown below. This manual contains a procedure for hot plugging during GLS operation (Y in the table below). In some configurations, GLS operation must be stopped before hot plugging (P in the table below). The procedure used after stopping GLS operation is the same as that described in the GLS manual.

Table 3.1 GLS hot plug support

Duplicated system	Configuration	Addition	Removal	Swapping
Fast switching system	Single configuration	Y	Y	Y
	Cluster configuration	P (*1)	P (*2)	Y
NIC switching system	Single configuration	Y	Y	Y
	Cluster configuration	P (*1)	P (*2)	Y

Y: Hot plugging possible during GLS operation

P: Hot plugging possible after stopping GLS operation

- *1 The addition procedure in the cluster configuration is as follows: add NICs according to [Section 3.4.1.1, "Addition procedure,"](#) and add virtual interface settings according to Section 5.2, "Addition Procedure for Cluster Environment Settings," in the GLS manual.
- *2 The removal procedure in the cluster configuration is as follows: remove virtual interface settings according to Section 5.4, "Procedure for Removing Cluster Environment Settings," in the PRIMECLUSTER GLS manual, and remove NICs according to [Section 3.4.1.2, "Removal procedure."](#)

If the system is rebooted after NIC addition, removal, or swapping, the tool (kudzu (8)) used to inspect hardware changes may be executed. Respond to this in the procedure described below. The following table lists the optional items in the kudzu (8) window for NIC addition, removal, or swapping.

Table 3.2 Optional item in kudzu (8) window

	Optional item in kudzu (8) window
NIC addition	Ignore
NIC removal	Keep Configuration
NIC swapping	Keep Configuration and Ignore

- 1 When adding NICs
The kudzu (8) displays a window to specify whether to add device information to the system for the added interfaces. Among "Configure," "Ignore," and "Do Nothing," select "Ignore."
- 2 When removing NICs
The kudzu (8) displays a window to specify whether to remove device information from the system for the removed interfaces. Among "Remove Configuration," "Keep Configuration," and "Do Nothing," select "Keep Configuration."
- 3 When swapping NICs
The kudzu (8) displays a window to specify whether to remove device information from the system for the removed interfaces. Because the device information is used by the added interfaces, leave it on the system. Among "Remove Configuration," "Keep Configuration," and "Do Nothing," select "Keep Configuration." Later, the kudzu (8) displays a window to specify whether to add device information to the system for the added interfaces. Among "Configure," "Ignore," and "Do Nothing," select "Ignore."

3.4.2.1 Addition procedure

This section describes the procedure for adding NICs and creating a virtual interface to make the added NICs redundant.

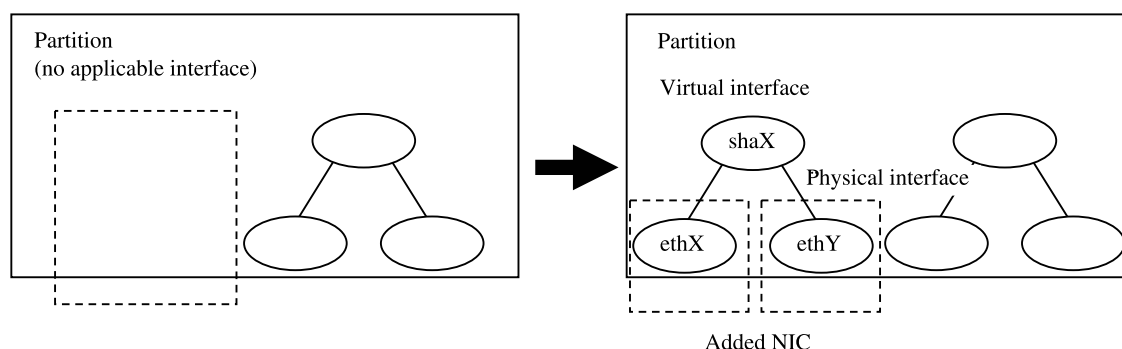


Figure 3.1 Addition of a virtual interface for making the added NICs (ethX, ethY) redundant

For a high-speed switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816  0
```

- 2 Make sure that power to the target PCI slot is off (*).
For details, see [Section 3.2.3.1, "Checking the power status."](#)

```
# cat /sys/bus/pci/slots/n/power
0
```

n: slot number

- 3 Add a NIC to the PCI slot (*).
- 4 Turn on power to the PCI slot (*).
For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: slot number

5 Check the hardware address (*).

An interface (ethX) is created for an added NIC when power is turned on.

Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. For details, see [Section 3.4.1.1, "Addition procedure."](#) To add two or more NICs, repeat Steps 2 to 5.

6 Perform post-addition processing.

- 1) To enable the GLS to use the interfaces at system startup, edit the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). In "HWADDR," set the hardware address that was checked in Step 5. Also, set "HOTPLUG=no" and "ONBOOT=yes" in the interface setting file for the NIC to be made redundant.

ifcfg-ethX

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet
```

ifcfg-ethY

```
DEVICE=ethY
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
BROADCAST=YYY:YYY:YYY:YYY
IPADDR=YYY:YYY:YYY:YYY
NETMASK=YYY:YYY:YYY:YYY
NETWORK=YYY:YYY:YYY:YYY
ONBOOT=yes
TYPE=Ethernet
```

- 2) Add the added interfaces to the `/etc/modprobe.conf` file (*).

This correlates the interfaces and drivers to each other. An example of `/etc/modprobe.conf` is shown below.

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 ← Added
alias ethY e1000 ← Added
```

- 3) Activate the interface of an added NIC (*).

```
# /sbin/ifup ethX
# /sbin/ifup ethY
```

- 4) If necessary, specify subnet mask information for the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask create -i <network_address>
-m <netmask>
```

- 5) Set virtual interfaces (specify `ethX` and `ethY`).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX -m
t -i <ipaddress> -t ethX,ethY
```

- 6) Activate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n shaX
```

For a NIC switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#) For details, see [Section 3.2.3.1, "Checking the power status."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816    0
```

- 2 Make sure that power to the target PCI slot is off (*).
For details, see [Section 3.2.3.1, "Checking the power status."](#)

```
# cat /sys/bus/pci/slots/n/power
0
```

n: slot number

- 3 Add a NIC to the PCI slot (*).
- 4 Turn on power to the PCI slot (*).
For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: slot number

- 5 Check the hardware address (*).
An interface (ethX) is created for an added NIC when power is turned on.
Execute the `ifconfig (8)` command to check the hardware address (HWaddr) of the created interface. For details, see [Section 3.4.1.1, "Addition procedure."](#) To add two or more NICs, repeat Steps 2 to 5.
- 6 Perform post-addition processing.
 - 1) To enable the GLS to use the interfaces at system startup, edit the interface setting file (`/etc/sysconfig/network-scripts/ifcfg-eth<x>`). In "HWADDR," set the hardware address that was checked in Step 5. Also, set "HOTPLUG=no" and "ONBOOT=yes" in the interface setting file for the NIC to be made redundant.

ifcfg-ethX

```

DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet

```

ifcfg-ethY

```

DEVICE=ethY
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=no
TYPE=Ethernet

```

- 2) Add the added interfaces to the /etc/modprobe.conf file (*).

This correlates the interfaces and drivers to each other. An example of /etc/modprobe.conf is shown below.

```

alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 ← Added
alias ethY e1000 ← Added

```

- 3) Change the interface names of the added NICs to the names specified in the interface setting files (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the same interface names and MAC addresses in the nameif (8) command as those in DEVICE and HWADDR in the ifcfg-ethX and ifcfg-ethY files that were set in 1) of step 6. When the nameif (8) command is executed, the specified interface must be deactivated.

```
# /sbin/nameif ethX XX:XX:XX:XX:XX:XX
# /sbin/nameif ethY YY:YY:YY:YY:YY:YY
```

- 4) If necessary, specify subnet mask information for the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask create -i
<network_address> -m <netmask>
```

- 5) Set virtual interfaces (specify ethX and ethY)

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX
-m d -i <ipaddress1> -e <ipaddress2> -t ethX,ethY
```

- 6) Specify hub monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n shaX -p
<ipaddr1>,<ipaddr2>
```

- 7) If necessary, set the standby patrol function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaY
-m p -t shaX
```

- 8) Restart GLS to enable the changed settings.

This restart also activates the virtual interface and starts its monitoring.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

3.4.2.2 Removal procedure

This section describes the procedure for removing NICs whose virtual interface makes them redundant.

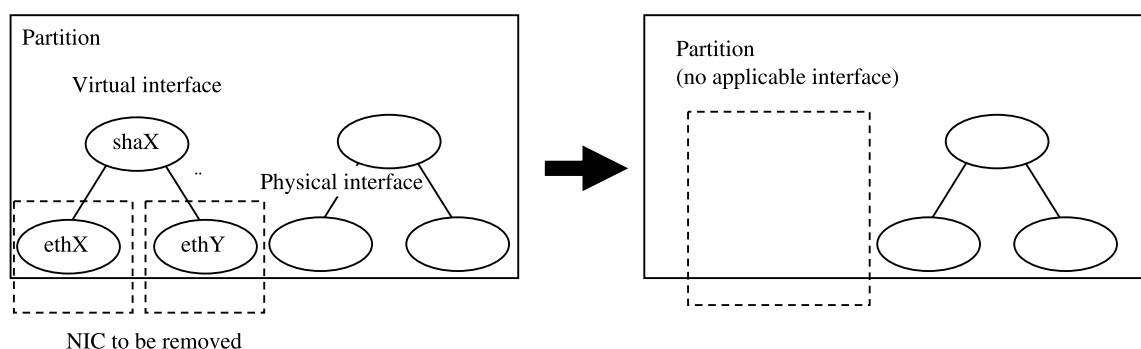


Figure 3.2 Removing NICs whose virtual interface makes them redundant (ethX, ethY)

For a high-speed switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#) For details, see [Section 3.2.3.1, "Checking the power status."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816  0
```

- 2 Prepare for removing a card.

- 1) Deactivate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n shaX
```

- 2) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

- 3) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i
<network_address>
```

- 4) Check the number of a PCI slot that contains the NIC to be removed (*).
For details, see procedure 2 in [Section 3.4.2.1, "Addition procedure."](#)

- 5) Deactivate the interface of the NIC to be removed (*).

```
# /sbin/ifdown ethX
# /sbin/ifdown ethY
```

- 3 Turn off power to the target PCI slot (*).

The interface (ethX) is deleted when power is turned off. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

- 4 Remove the NIC from the PCI slot. To remove more NICs, repeat steps 2 to 4.
- 5 Perform post-removal processing.

- 1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

```
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-ethX
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-ethY
```

- 2) Remove the settings of the removed interfaces from /etc/modprobe.conf (*).
Remove the correspondence between the interfaces and drivers that is no longer required.

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 ← Removed
alias ethY e1000 ← Removed
```


For a NIC switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#) For details, see [Section 3.2.3.1, "Checking the power status."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816    0
```

- 2 Prepare for removing a card.

- 1) Deactivate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n shaX
```

- 2) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

- 3) Stop hub monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

- 4) Delete the hub monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll delete -n shaXf
```

- 5) Delete the standby patrol function. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaY
```

- 6) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

- 7) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i
<network_address>
```

- 8) Check the number of a PCI slot that contains the NIC to be removed.
For details, see procedure 2 in [Section 3.4.2.1, "Addition procedure."](#) (*)

- 9) Deactivate the interface (*).

```
# /sbin/ifdown ethX
# /sbin/ifdown ethY
```

- 3 Turn off power to the target PCI slot (*).

The interface (ethX) is deleted when power is turned off. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

n: slot number

- 4 Remove the NIC from the PCI slot. To remove more NICs, repeat steps 2 to 4.
- 5 Perform post-removal processing.

- 1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

```
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-ethX
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-ethY
```

- 2) Remove the settings of the removed interfaces from /etc/modprobe.conf (*). Remove the correspondence between the interfaces and drivers that is no longer required.

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 ← Removed
alias ethY e1000 ← Removed
```

- 3) Restart GLS to enable the changed settings.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

3.4.2.3 Swapping procedure

This section describes the procedure for swapping a NIC whose virtual interface makes it redundant.

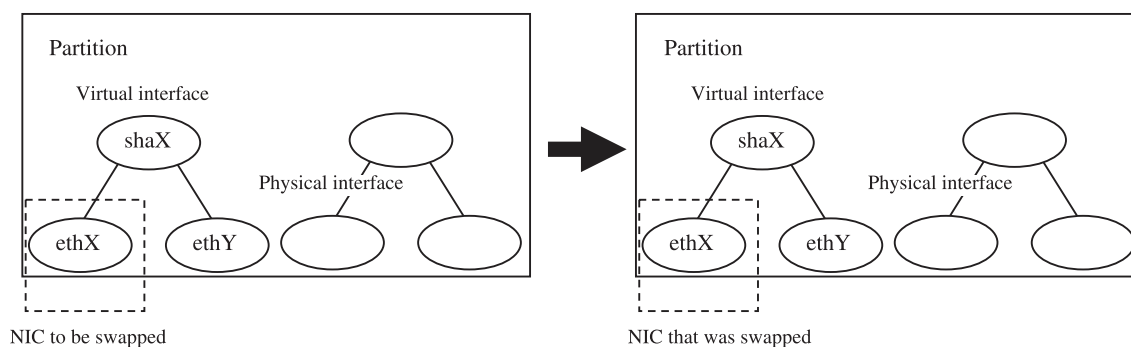


Figure 3.3 Swapping a NIC whose virtual interface make it redundant (ethX)

For a high-speed switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#) For details, see [Section 3.2.3.1, "Checking the power status."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816    0
```

- 2 Prepare for swapping a card.
 - 1) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped. (Specify the interface name of the NIC to be swapped as ethX.)

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i
ethX
```

- 2) Enter the dsphanet command to confirm that the device status of the NIC (interface name: ethX) is CUT.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4, Patrol]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
shaX      Active   t    OFF  ethX(CUT), ethY(ON)
```

- 3) Deactivate the interface (*).

```
# /sbin/ifdown ethX
```

- 3 Turn off power to the target PCI slot (*).

The interface (ethX) is deleted when power is turned off. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

n: slot number

- 4 Swap the NIC in the PCI slot (*).

- 5 Turn on power to the PCI slot (*).

For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: slot number

- 6 Check the hardware address (*).

An interface (ethX) is created for the swapped NIC when power is turned on.

Execute the ifconfig (8) command to check hardware address of the swapped NIC (HWaddr). For details, see [Section 3.4.1.3, "Swapping procedure."](#)

- 7 Perform post-swap processing.

- 1) Change the specified value of HWADDR in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 6.

ifcfg-ethX

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet
```

- 2) Activate the interface of the swapped NIC (*).

```
# /sbin/ifup ethX
```

- 3) Restore the NIC definition (interface name: ethX) that was temporarily deleted prior to swapping in 1) of Step 2).

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

- 4) Enter the dsphanet command to confirm that the device status of the swapped NIC is ON.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name           Status      Mode CL  Device
+-----+-----+-----+----+-----+
shaX           Active      t    OFF  ethX(ON),ethY(ON)
```

For a NIC switching system

- 1 Confirm that the PCI Hot Plug driver is installed (*).
If it is not installed, install the driver by following the procedure in [Section 3.2.2, "Installation of a PCI Hot Plug driver."](#) For details, see [Section 3.2.3.1, "Checking the power status."](#)

Confirmation procedure

```
# /sbin/lsmmod | grep shpchp
shpchp                203816    0
```

- 2 Prepare for swapping a card.

- 1) Stop hub monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

- 2) Stop standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

- 3) Enter the dsphanet command to check the status of the NIC (interface name: ethX) to be swapped. The NIC must be in a different state from that of an active NIC (the NIC must be in the OFF or STOP state). If the NIC is active, follow Step 4 to switch its state to standby.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4, Patrol]
Name           Status      Mode CL  Device
+-----+-----+-----+----+-----+
shaX           Active      d    OFF  ethX(ON),ethY(OFF)
```

- 4) If the NIC is an active NIC, switch its state to standby. After the switch, enter the dsphanet command to confirm that the NIC is a standby NIC (OFF).

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4, Patrol]
Name          Status    Mode CL  Device
+-----+-----+-----+-----+-----+
shaX          Active    d    OFF  ethX(OFF),ethY(ON)
```

- 5) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

- 6) Deactivate the interface of the NIC to be swapped (*).

```
# /sbin/ifdown ethX
```

- 3 Turn off power to the target PCI slot (*).

The interface (ethX) is deleted when power is turned off. For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 0 > /sys/bus/pci/slots/n/power
```

n: slot number

- 4 Swap the NIC in each PCI slot (*).

- 5 Turn on power to the PCI slot (*).

For details, see [Section 3.2.3.2, "Power-on and power-off procedures."](#)

```
# echo 1 > /sys/bus/pci/slots/n/power
```

n: slot number

- 6 Check the hardware address (*).

An interface (ethX) is created for the swapped NIC when power is turned on.

Execute the ifconfig (8) command to check hardware address of the swapped NIC (HWaddr). For details, see [Section 3.4.1.3, "Swapping procedure."](#)

7 Perform post-swap processing.

- 1) Change the specified value of HWADDR in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 6.

```
ifchg-ethX
```

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet
```

- 2) Change the interface name of the swapped NIC to the name specified in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the same interface name and hardware address in the nameif (8) command as those in DEVICE and HWADDR in the ifcfg-ethX file that was set in 1) of step 7. When the nameif (8) command is executed, the specified interface must be deactivated.

```
# /sbin/nameif ethX ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
```

- 3) Set the state of the swapped NIC interface to that of a standby NIC of GLS. Confirm that an IPv4 address is not assigned and the UP and NOARP flags are set.

```
# /sbin/ifconfig ethX 0 -arp up
# /sbin/ifconfig ethX
ethX      Link encap:Ethernet  HWaddr ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
           inet6 addr: fe80::XXXXXXXXXXXXXXXX/64 Scope:Link
           UP BROADCAST NOARP MULTICAST  MTU:1500  Metric:1
```

- 4) If necessary, disconnect the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

- 5) Start standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/strptl -n shaY
```

- 6) Restart hub monitoring.

```
# /opt/FJShanet/usr/sbin/hanetpoll on
```

- 7) Restart interface status monitoring.

```
# /bin/rm /var/opt/FJShanet/tmp/disable_watchif
```

3.4.3 Handling kudzu

When the system is rebooted with NICs added, removed, or swapped, the tool (kudzu (8)) used to inspect hardware changes may be executed. Respond to this in the following procedure.

- 1 When adding NICs

The kudzu (8) displays a window to specify whether to add device information to the system for the added interfaces. The device information is added to the system when the interfaces are added. Among "Configure," "Ignore," and "Do Nothing," select "Ignore."

- 2 When removing NICs

The kudzu (8) displays a window to specify whether to remove device information from the system for the removed interfaces. The device information is removed from the system when the interfaces are removed. Among "Remove Configuration," "Keep Configuration," and "Do Nothing," select "Keep Configuration."

- 3 When swapping NICs

The kudzu (8) displays a window to specify whether to remove device information from the system for the removed interfaces. Because the device information is used by the added interfaces, leave it on the system. Among "Remove Configuration," "Keep Configuration," and "Do Nothing," select "Keep Configuration." Later, the kudzu (8) displays a window to specify whether to add device information to the system for the added interfaces. Among "Configure," "Ignore," and "Do Nothing," select "Ignore."

3.4.4 Assigning a specific interface name to an interface

For hot plugging, a fixed device name must be assigned to each NIC. (By default, the OS assigns interface names in the order that it detects hardware devices. Therefore, the assigned values vary as hardware is added and removed. This causes problems with GLS and other programs that handle interface names directly). To use fixed interface names, manually edit the naming file (interface setting file). The interface setting file and the method of editing it vary depending on the OS used, which is either Red Hat, SUSE9, or SUSE10. See the explanation for each OS.

"MAC-address" in the subsequent explanations indicates the hardware address of an interface represented in the AA:BB:CC:DD:EE:FF format.

Red Hat

Interface in Red Hat is managed with an ifcfg-eth<X> file in the /etc/sysconfig/network-scripts directory. By specifying the hardware address of a network device (MAC address) in such a file, the interface name can be fixed.

HWADDR=MAC-address

A specific interface name is valid only for an activated interface. To assign the specific interface name at system startup, specify ONBOOT=yes.

```
<<Example of the ifcfg-eth<x> file>>
DEVICE=eth1.....Network device name
BOOTPROTO=static
BROADCAST=192.168.101.255
HWADDR=00:0E:0C:70:C3:B6.....Hardware address
IPADDR=192.168.101.101
NETMASK=255.255.255.0
NETWORK=192.168.101.0
ONBOOT=yes
TYPE=Ethernet
```

This file is automatically read when interface is to be activated. Therefore, the hardware address must be specified before interface is activated.

SUSE9

Interfaces in SUSE9 are managed with the `ifcfg-eth-id-<MAC-address>` file in the `/etc/sysconfig/network` directory. By defining an interface name in this file, the interface name can be fixed. To do so, write the following line in the `ifcfg-eth-id-<MAC-address>` file:

```
PERSISTENT_NAME = 'interface-name'
```

In SUSE9, a name automatically assigned by the kernel cannot be used as a fixed interface name (the names `eth*`, `tr*`, `wlan*`, `qeth*`, and `iucv*` cannot be used). A fixed interface name is valid only for an activated interface. To assign a fixed interface name at system startup, specify `STARTMODE='onboot'`.

```
Example:
BOOTPROTO='static'
BROADCAST='192.168.1.255'
IPADDR='192.168.1.1'
MTU=' '
NETMASK='255.255.255.0'
NETWORK='192.168.1.0'
REMOTE_IPADDR=' '
STARTMODE='onboot'
UNIQUE='B35A.ilX5mG094wB'
PERSISTENT_NAME='nic0' ..... Interface name
_nm_name='bus-pci-0000:02:00.0'
```

This file is automatically read when the interface is activated. Therefore, the interface name must be specified before the interface is activated.

SUSE10

To set a fixed interface name in SUSE10, define the hardware address (MAC address) and its corresponding interface name in the 30-net-persistent-names.rules file in the /etc/udev/rules.d/ directory. To do so, write the following line (actually, write the statement on a single line) in the 30-net-persistent-names.rules file.

```
SUBSYSTEM=="net", ACTION=="add", SYSFS{address}=="MAC-address",  
IMPORT="/lib/udev/rename_netiface %k interface-name"
```

In SUSE10, a name automatically assigned by the kernel cannot be used as a fixed interface name (the names eth*, tr*, wlan*, qeth*, and iucv* cannot be used).

Example:

```
SUBSYSTEM=="net", ACTION=="add", SYSFS{address}=="00:0E:0C:70:C3:40", \  
IMPORT="/lib/udev/rename_netiface %k nic0"
```

\: Indicates no linefeed is inserted.

This file is automatically read when the interface is activated. Therefore, the interface name must be specified before the interface is activated.

3.4.5 Installation verification procedure

Installation results may be output as messages to the `/var/log/messages` file depending on the type of card and driver installed. To check installation results from such messages, see the related card manuals.

The following procedure is applicable to every type of card:

- 1 Enter the `/sbin/ifconfig` command to collect status information.

```
# /sbin/ifconfig -a
```

If the following message is output, installation is successful:

```
ethX      Link encap:Ethernet  HWaddr 00:20:ED:48:7C:C2
          inet addr:10.124.0.1  Bcast:10.124.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7529543 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6271349 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4076635362 (3887.7 Mb)  TX bytes:1154829596 (1101.3 Mb)
          Interrupt:3 Base address:0x3400 Memory:e8100000-e8100038
```

Notes:

- Especially, check the part displayed in boldface type. "UP" at the beginning indicates the status. In this way, a card whose driver has been added and a card that has swapped can be identified, and a link established with the switch can be confirmed. If the number of received packets or number of sent packets has been added, as shown in the above example, transmission has already begun.
- If an interface that should have been added is not found, swapping may have failed. Check whether the card is correctly inserted and whether the driver that supports the card has been prepared.
- If a name other than the intended one is displayed after a card is added, the edited setting file as described here may not match actual hardware settings. Check the work again.

3.5 Hot Plugging a SCSI Card (FC Card)

Hot plugging (addition, removal, or swapping) a SCSI card used to control an external disk requires special considerations in addition to the common hot plugging procedures.

This section describes hot plugging FC cards (referred to as an HBA, in this document), which are a type of SCSI card (it does not describe adding units to or removing units from external disk devices). The section describes procedures applicable to a SCSI card used in combination with PRIMECLUSTER GDS and/or ETERNUS multipath driver and procedures applicable to a SCSI card used without either of them. However, only an overview is provided on information specific to PRIMECLUSTER GDS. For details, see the PRIMECLUSTER GDS manuals.

Information already provided in the previous sections on the common procedures is not repeated here. For that information, see the sections on the common procedures.

Storage devices are assigned unique names in the system by the udev mechanism so that they are not affected by whether another device exists. Thus, they do not require any special procedure for setting fixed names for network cards.

Remarks: The FC card used for SAN boot does not support hot plugging.

An HBA runs in one of the three operation modes listed below. This section describes procedures for adding, removing, and swapping HBAs in each operation mode. Moreover, if multiple cards fail while PRIMECLUSTER GDS is running, the affected range depends on the fault locations. This section covers only typical cases of such events.

- PRIMECLUSTER GDS is not used:
ETERNUS multipath driver is not used. This is the simplest configuration, in which ETERNUS operates with a single path.
- PRIMECLUSTER GDS is not used:
ETERNUS multipath driver is used. This is a commonly used configuration, in which ETERNUS operates with a multipath.
- PRIMECLUSTER GDS is used:
ETERNUS multipath driver is used. This is a highly reliable configuration, in which each ETERNUS unit operates with a multipath and multiple ETERNUS units are used for inter-cabinet mirroring.

The section covers the following topics in the order given:

- [Hot plugging an HBA running without PRIMECLUSTER GDS and ETERNUS multipath driver \(→ 3.5.1\)](#)
- [Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS \(→ 3.5.2\)](#)
- [Hot plugging an HBA running with both PRIMECLUSTER GDS and ETERNUS multipath driver \(→ 3.5.3\)](#)

Some parts of the descriptions in the following sections refer to ETERNUS multipath driver and PRIMECLUSTER GDS commands. For details, see the *ETERNUS Multipath Driver V2.0 User's Guide for Linux*, and the *PRIMECLUSTER Global Disk Services Configuration and Administration Guide 4.1 (Linux)*.

3.5.1 Hot plugging an HBA running without PRIMECLUSTER GDS and ETERNUS multipath driver

3.5.1.1 Addition procedure

This section describes the procedure for adding an HBA (FC card) and ETERNUS.

Remarks: In the procedure, the steps with an asterisk (*) at the end of the operation description are the same as those for ordinary PCI cards.

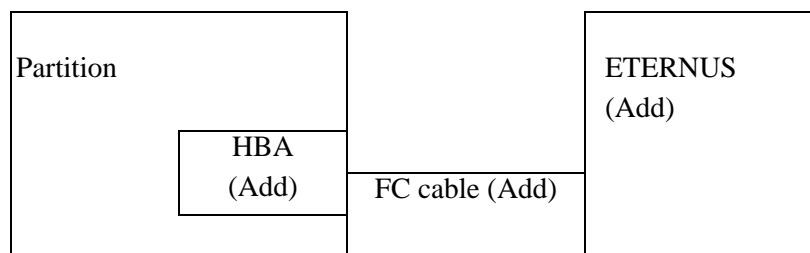


Figure 3.4 Addition of HBA (FC card) and ETERNUS

- 1 Make sure that power to the PCI slot is off (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 2 Add a PCI card.
- 3 Connect the FC cable.
- 4 Turn on power to the target PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)

- 5 Perform the necessary post-processing.
 - 1) Perform the setting according to the manuals for the storage device and FC switch.
 - 2) Check the installation results.See [Section 3.5.1.4, "Checking installation results."](#)

3.5.1.2 Removal procedure

This section describes the procedure for removing an HBA (FC card) and ETERNUS to exclude them from operation.

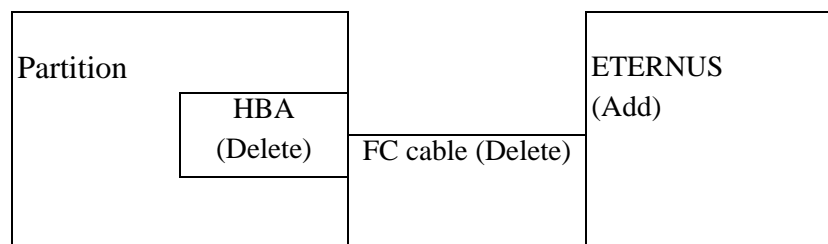


Figure 3.5 Removal of HBA (FC card) and ETERNUS

- 1 Perform the necessary preprocessing.

Stop access to the target HBA, such as by stopping an application.
- 2 Turn off power to the target PCI slot (*).

For details, see [Section 3.2.3, "Power operation procedure."](#)
- 3 Remove the PCI card.

3.5.1.3 Swapping procedure

This section describes the procedure for replacing only the faulty HBA while leaving ETERNUS as is.

Remarks: In the procedure, the steps with an asterisk (*) at the end of the operation description are the same as those for ordinary PCI cards.

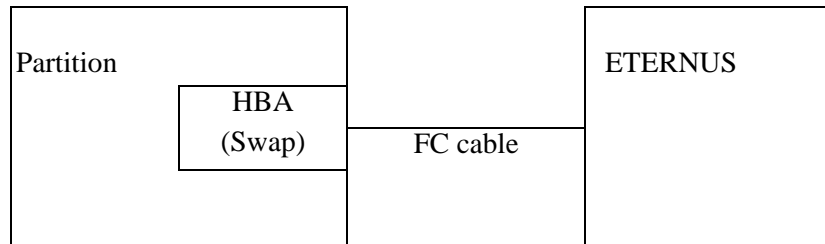


Figure 3.6 Swapping of HBA (FA card) and ETERNUS

- 1 Perform the necessary preprocessing.
Stop access to the faulty HBA such as by stopping an application.
- 2 Turn off power to the target PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 3 Swap the PCI card.
- 4 Connect the FC cable.
- 5 Turn on power to the PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 6 Perform the necessary post-processing.
 - 1) Perform the setting according to the manuals for the storage device and FC switch.
 - 2) Check the installation results.
See [Section 3.5.1.4, "Checking installation results."](#)
 - 3) If necessary, restart use of the HBA, such as by restarting the application.

3.5.1.4 Checking installation results

Check the results of FC card and driver installation, and take necessary action as follows.

1 Check the log.

If the following HBA installation message and device detection message are output to the /var/log/messages file, installation is successful:

```
SCSI10 : Emulex LightPulse LP9802 2 Gigabit PCI Fibre Channel  \
        Adapter on PCI bus 0f device 08 irq 59  ... (a)
        lpFC 0000:0f:01.0: 1:1303 Link Up Event x1 received  \
        Data: x1 x1 x4 x0  ... (b)
        Vendor: FUJITSU    Model: E3000                      \
        Rev: 0000          ... (c-1)
        Type:   Direct-Access                                \
        ANSI SCSI revision: 03  ... (c-2)
```

\: Indicates that no line feeds should be inserted.

- If only the message shown at (a) is output but the next line is not output or no such message is output:

HBA swapping failed.

Turn off power to the slot, and check the following again:

- Is the HBA normally inserted in the PCI slot?
- Is the latch set correctly?

Solve the problem, and turn on power again. Then, check the log.

- If the FC linkup message shown at (b) is not output even though the message shown at (a) is output:

The FC cable may be disconnected, or the FC path may have not correctly been set up.

Turn off power to the slot, and check the following:

- Check FC driver settings.

Moreover, check whether FC-AL and Fabric settings are correct.

- Check the FC cable connection.
- Check the FC setting for storage.

Moreover, specify FC-AL and Fabric correctly.

Solve the problem, and turn on power again. Then, check the log.

- If the message shown at (c-1) or (c-2) is not output even though the messages shown at (a) and (b) are output, no storage was found.

Make the checks listed below. Because these checks do not involve card-related problems, power to the slot need not be turned off for the checks.

- Check the settings for FC switch zoning.
- Check the settings for storage zoning.

- Check the settings for storage LUN mapping.

Moreover, check whether the storage can be viewed correctly from LUN0.

Solve the problem, and take action as follows for verification and system recognition:

- 1) Check the message at (a) for the host number of the installed HBA.
xx of SCSIxx (xx is a number) in the message at (a) is the host number.
In the above example, the host number is 10.
- 2) Enter the following command to scan the device:

```
# echo "- " "- " "- " >/sys/class/scsi_host/hostxx/scan  
(# is the command prompt.)
```

The host number determined in 1) is assigned to xx of hostxx.

In the above example, the following command is to be executed:

```
# echo "- " "- " "- " >/sys/class/scsi_host/host10/scan
```

- 3) Make sure that messages such as those at (c-1) and (c-2) were output to /var/log/messages.
If these messages are not output, check the settings again.

3.5.2 Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS

3.5.2.1 Addition procedure

This section describes the procedure for adding an HBA to add a path when ETERNUS multipath driver is already installed.

Remarks: In the procedure, the steps with an asterisk (*) at the end of the operation description are the same as those for ordinary PCI cards.

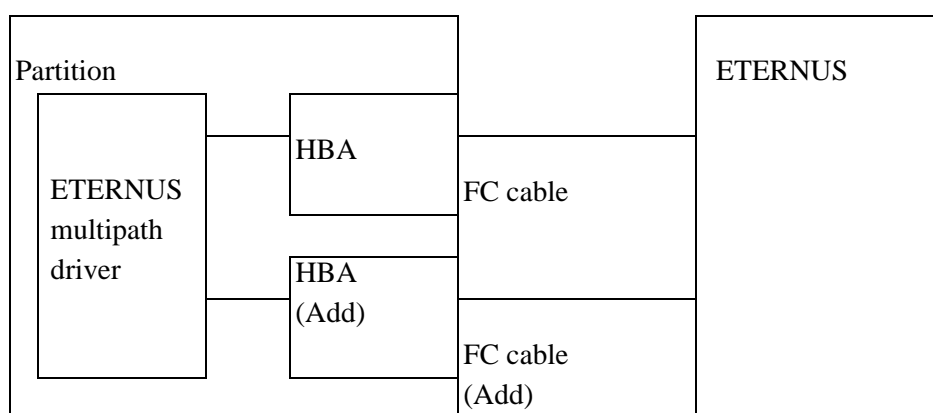


Figure 3.7 Path addition by HBA addition

- 1 Make sure that power to the target PCI slot is off (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 2 Add a PCI card.
- 3 Connect the FC cable.
- 4 Turn on power to the PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 5 Perform the necessary post-processing.
 - 1) Perform the setting according to the manuals for the storage device and FC switch.
 - 2) Make sure that the HBA is installed at the OS level (*).
See [Section 3.5.1.4, "Checking installation results."](#)
 - 3) In RHEL-AS4 (IPF), to make the ETERNUS multipath driver recognize the HBA, issue another command to the ETERNUS multipath driver to reconfigure the multipath.
In RHEL5 (IPF), this operation is not required.

```
# /usr/fjsvgmpd/bin/iompadm rescan
```

- 4) After executing the above command, enter the `iompadm info` command, and confirm that the added HBA has been normally installed.
If it has not been installed as intended, see [Section 3.5.1.4, "Checking installation results,"](#) and check installation conditions again.

3.5.2.2 Removal procedure

This section describes the procedure for removing one of the HBAs constituting a multipath (provided that removal of this HBA does not stop ETERNUS access).

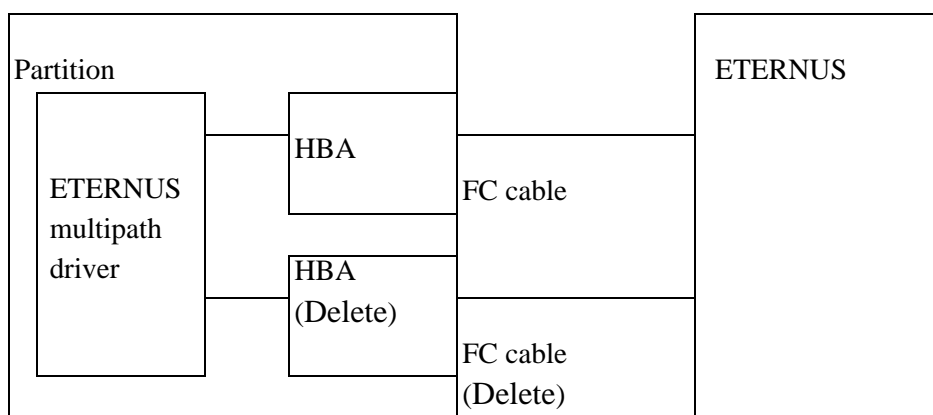


Figure 3.8 HBA removal (multi-path configuration)

- 1 In RHEL-AS4 (IPF), perform the necessary preprocessing. In RHEL5 (IPF), this operation is not required.
 - 1) Find the PCI bus address from the slot number of the HBA to be removed, or execute the command below and find the PCI bus address of the failed HBA. When the HBA is a FC card (dual type) and both ports have an ETERNUS disk array (excluding ETERNUS SX300) connected, find each PCI address.

```
# /usr/fjsgvgrpdp/bin/iompadm info
IOMP:vhba0
  Element:
    DISK:XXXXXX-XXXXXX-XXXX-XXXX (sdb)
    PATH:
      sdb (PCI bus address 1) active "online" X, Y, Z
      sdb (PCI bus address 2) fail " diagnosis error" X, Y, Z
```

Execute the command below to stop the ETERNUS disk array from being accessed via the HBA. When the HBA is a FC card (dual type) and both ports have an ETERNUS disk array (excluding ETERNUS SX300) connected, execute the following command for the two PCI addresses.

```
# /usr/fjsgvgrpdp/bin/iompadm change adapter (PCI bus address)
```

- 2) Execute the command below to remove the HBA from the control targets of ETERNUS multi-path driver control. When the HBA is a FC card (dual type) and both ports have an ETERNUS disk array (excluding ETERNUS SX300) connected, execute the following command for the two PCI addresses.

```
# /usr/fjsgmpd/bin/iompadm del (PCI bus address)
```

If the following message is displayed, execute the iompadm del command again.

```
could not delete (PCI bus address)
```

- 2 Turn off power to the target PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 3 Remove the PCI card.

3.5.2.3 Swapping procedure

This section describes the procedure for replacing one of the HBAs constituting a multipath.

Remarks: In the procedure, the steps with an asterisk (*) at the end of the operation description are the same as those for ordinary PCI cards.

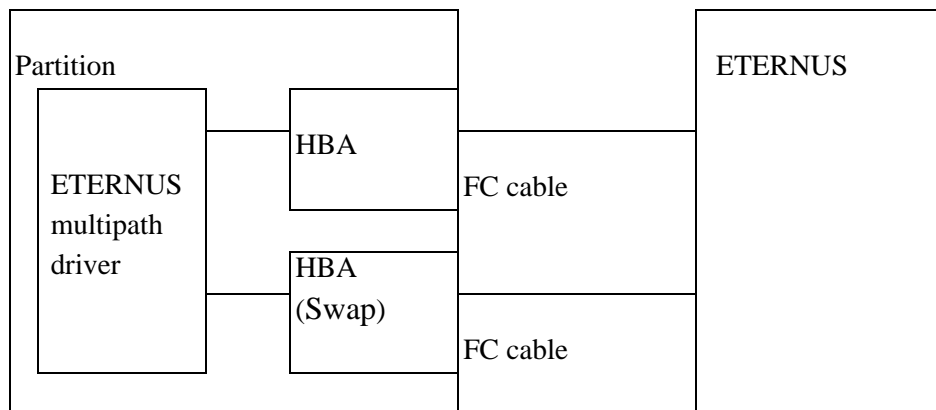


Figure 3.9 HBA swapping (multi-path configuration)

- 1 In RHEL-AS4 (IPF), perform the necessary preprocessing. In RHEL5 (IPF), this operation is not required.
Referring to [3.5.2.2, "Removal procedure,"](#) perform the same operations as those for removal.
- 2 Turn off power to the target PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 3 Swap the PCI card.
- 4 Connect the FC cable.
- 5 Turn on power to the PCI slot (*).
For details, see [Section 3.2.3, "Power operation procedure."](#)
- 6 Perform the necessary post-processing.
Referring to [3.5.2.1, "Addition procedure,"](#) perform the same operations as those for addition.

Remarks:

For details on the `iompadm` command, see the manual for the multipath driver.

3.5.3 Hot plugging an HBA running with both PRIMECLUSTER GDS and ETERNUS multipath driver

3.5.3.1 Addition procedure

In the environment where an ETERNUS multipath is used, the system must be rebooted to add or remove an ETERNUS. Therefore, PCI Hot Plug only makes it possible to add a path to ETERNUS (FC card addition) by providing an HBA in the environment that has already been duplicated by PRIMECLUSTER GDS. The procedure for this case is the same as that in [Section 3.5.2, "Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS."](#)

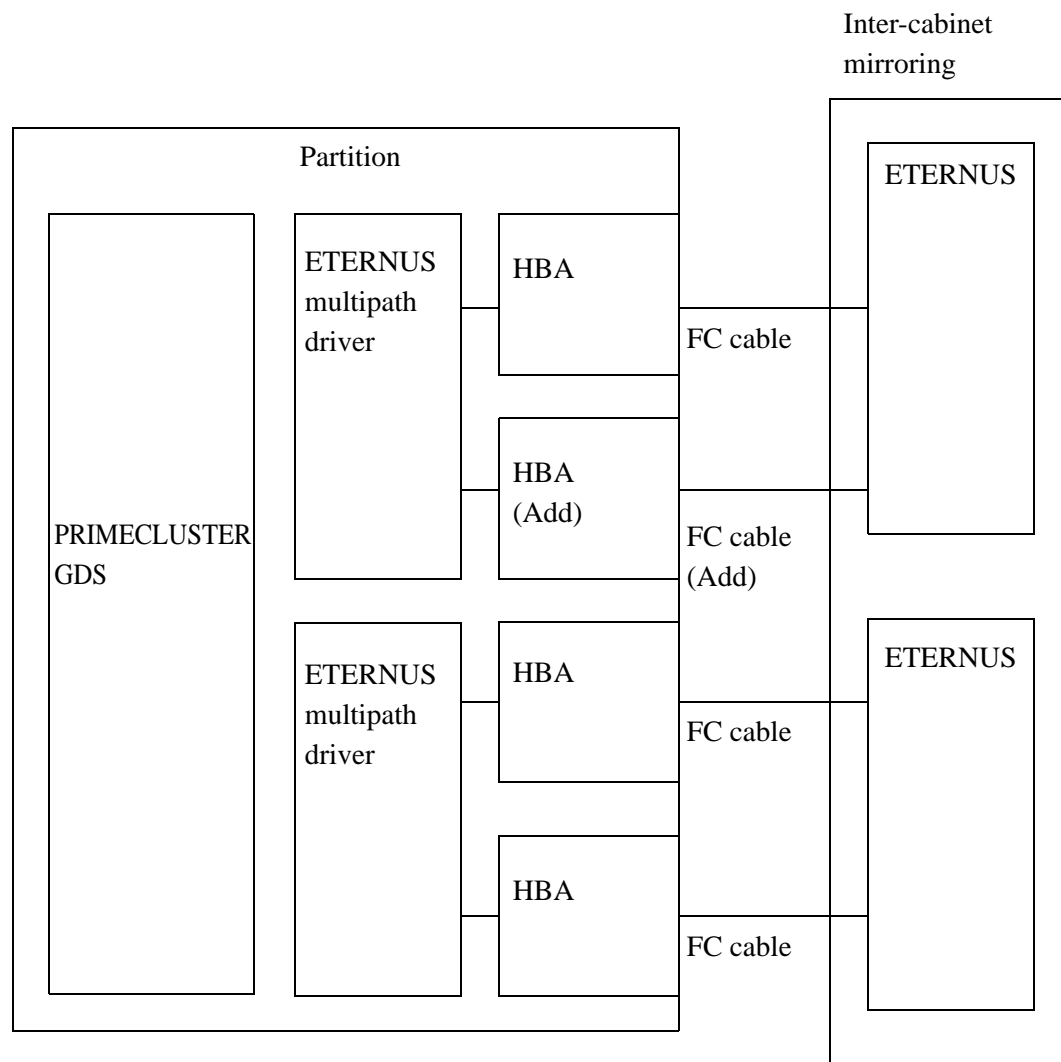


Figure 3.10 Adding a path to ETERNUS by adding an HBA

3.5.3.2 Removal procedure

The conditions are the same as those for addition. Remove an FC card by following the procedure in [Section 3.5.2, "Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS."](#)

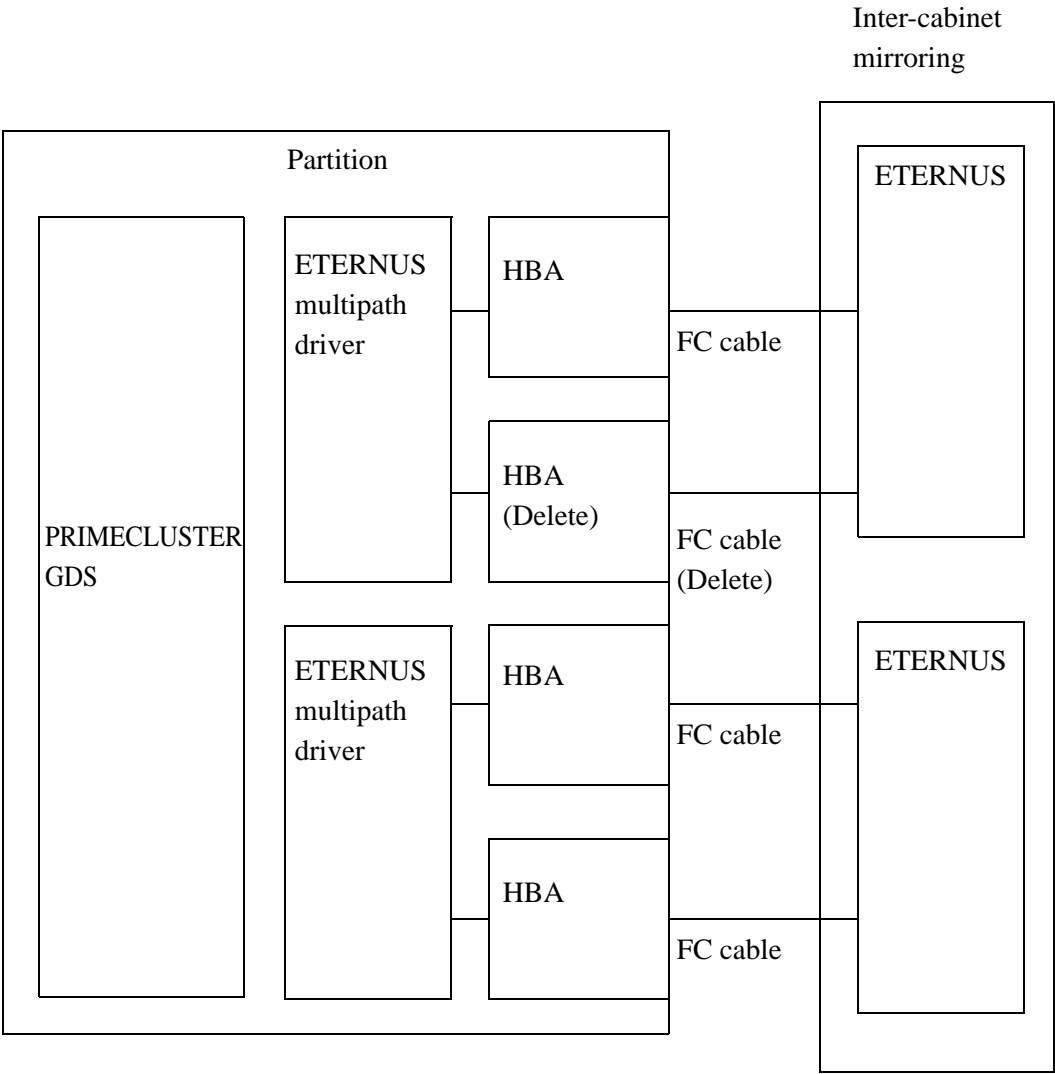


Figure 3.11 Removing an HBA constituting a multipath

3.5.3.3 Swapping procedure

This procedure swaps an HBA that normally constitutes a multipath. The procedure is therefore the same as that in [Section 3.5.2, "Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS."](#) An operation for PRIMECLUSTER GDS is not required.

When the cabinet on one side cannot be accessed because of a problem such as a double path error, take action as described below. For details, see the GDS manuals.

- 1 Before swapping a card, the disk units connected to the card must be excluded from the mirroring configuration. Enter the following command for every disk unit connected to the card to be replaced.

```
sdxswap -O -c <class-name> -d <SDX disk-name>
```

To check for the faulty physical disk (SDX-disk-name in the above code fragment), execute the following command provided by the ETERNUS multi-driver. This command displays the path statuses and names of connected physical disks. The targets of the command include any physical disk whose every path to the disk has an error.

```
# iompadm info
```

Output example:

```

IOMP: vhba0
Element:
    DISK: E6000- 000001-0000-0000 (sdb)
    PATH:
        sdb 0000:0a:00.0 active "online" 10, 31, c6
        sdb 0000:21:01.0 active "online" 0, 21, 86

    DISK: E6000- 000001-0000-0001 (sdc)
    PATH:
        sdc 0000:0a:00.0 active "online" 10, 31, c6
        sdc 0000:21:01.0 active "online" 0, 21, 86

IOMP: vhba1
Element:
    DISK: E6000- 000002-0000-0000 (sdd)
    PATH:
        sdb 0000:23:01.0 fail "internal error" 10, 31, c6
        sdb 0000:27:01.0 fail "internal error" 0, 21, 86

    DISK: E6000- 000002-0000-0001 (sde)
    PATH:
        sdc 0000:23:01.0 fail "internal error" 10, 31, c6
        sdc 0000:27:01.0 fail "internal error" 0, 21, 86

```

- 2 After swapping the card, incorporate the disk units connected to the swapped card into the mirroring configuration again. For the card swapping procedure, see [3.5.2, "Hot plugging an HBA running with ETERNUS multipath driver and without PRIMECLUSTER GDS."](#)

Swap one card at a time by performing that work sequentially for only that card. Do not physically swap multiple cards at the same time with commands executed concurrently. After the cards have been swapped, run the following command for all disks that are connected to the swapped cards.

```
# sdxswap -I -c <class-name> -d <SDX disk-name>
```

- 3 When the disk units are incorporated into the mirroring configuration again, equivalence restoration processing for mirroring is executed.
If an error is detected in the swapped card or in a connected path or disk unit, the equivalence restoration processing terminates abnormally. Execute the following command to check whether the equivalence restoration processing completed normally.

```
sdxinfo -S -c <class-name>
```

If the status of each of the displayed slices is active, the processing completed normally.

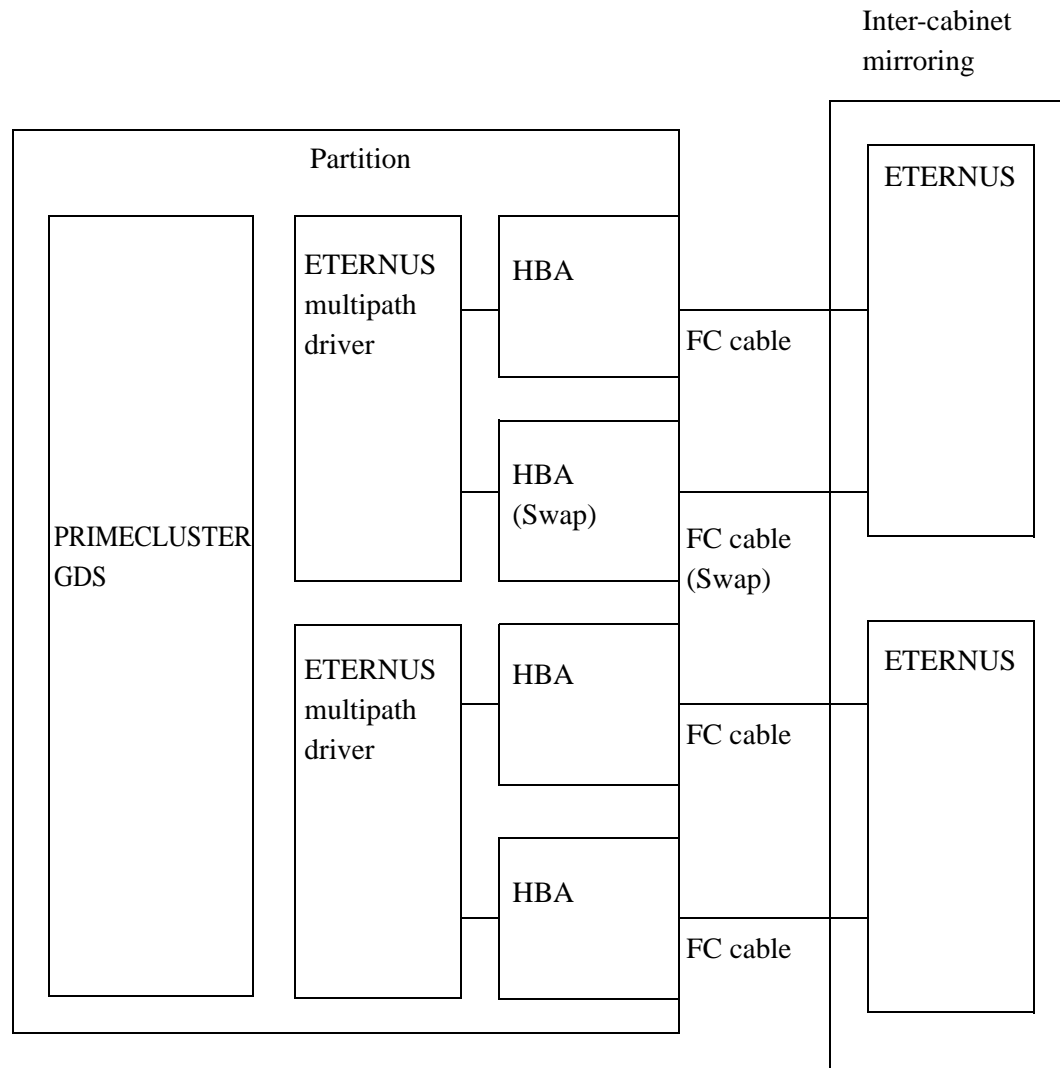


Figure 3.12 Replacing an HBA constituting a multipath

3.6 Resource Names (Reference)

This section provides reference information on names assigned by the udev mechanism.

Unique names are generated for PCI-SCSI in the PRIMEQUEST-series machine as shown below.

```
/dev/disk/by-path/{PCI-address(SCSI-card)}-{SCSI-port}-{SCSI-id}:Parti-
tion
```

PCI-address(SCSI-card)	: PCI address of a SCSI controller
SCSI-port	: SCSI port number
SCSI-id	: SCSI-id
Partition	: Disk partition

CHAPTER 4 Manual PSA Installation

4.1 Manual PSA installation (Linux: Red Hat) (PRIMEQUEST 580A/540A/580/540/480/440)

This section describes Manual PSA installation (Linux) to Linux OS (Red Hat).

Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

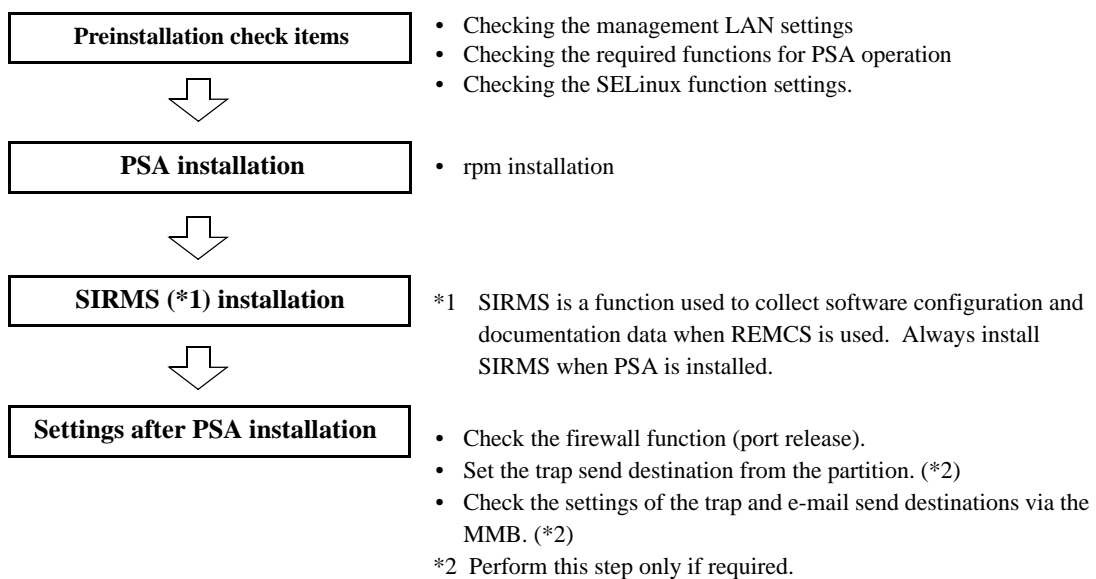
- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog partition monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of CPU, DIMM, and chip set recoverable errors
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- Partition information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.
- Hard disks cannot be maintained during operation. The partition must be stopped during maintenance.
- Linkage with PRIMECLUSTER is disabled.

Note: If the PEXU has been mounted, use PSA-1.10 or later.

4.1.1 Installation Workflow

The figure below shows the workflow for PSA installation.

Note: After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.



Remarks: If you choose to use the PRIMEQUEST Installation Support Tool/ Bundled-Software Package Installer for package installation, you do not need to install PSA and SIRMS. However, after the package installation using the PRIMEQUEST Installation Support Tool/Bundled-Software Package Installer, you need to confirm and set the items included in "Checking required before installation" and "Setup required after installation" explained above.

4.1.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.1.2.1)
- [Checking the required functions for PSA operation](#) (→ 4.1.2.2)
- [Checking the SELinux function settings](#) (→ 4.1.2.3)

4.1.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: To use the PRIMEQUEST installation support tool or bundled-software package installer for package installation, the appropriate settings must be made after batch package installation.

(1) Checking the settings for the NIC of the management LAN

Execute the following command to check the interface name assigned to the NIC of the management LAN.

- 1 Enter the `ifconfig` command to list the network interfaces recognized by the system and confirm the relevant interface name.

Command syntax:

```
/sbin/ifconfig -a
```

Example: eth0, eth1, and lo displayed on the left side are interface names.

```
# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.1.12  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3865 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

- 2 Use the `ethtool` command to find two network interface controllers (NIC) for the management LAN. Enter the command for each interface displayed in step 1 as shown below.

The NICs for the management LAN have bus-info (SEG:BUS:DEV.FUNC number) 0000:01:08.0 and 0000:01:00.0.

Command syntax:

```
/sbin/ethtool -i <interface-name>
```

Example: As the result of command execution for eth0 and eth1, these two interfaces match the NICs for the management LAN.


```
# /sbin/ethtool -i eth0
    driver: e100
    version: 3.0.27-k2-NAPI
    firmware-version: N/A
    bus-info: 0000:01:00.0 (Matches a NIC for the management LAN)

# /sbin/ethtool -i eth1
    driver: e100
    version: 3.0.27-k2-NAPI
    firmware-version: N/A
    bus-info: 0000:01:08.0 (Matches a NIC for the management LAN)
```

(2) Duplicating the two NICs for the management LAN

To duplicate the management LAN, activate the two NICs for the management LAN in the partition and use them. The duplication software (that controls LAN duplication) directs the send packets to the appropriate transmission line considering the status of the candidate transmission lines, thus achieving redundancy. When you specify duplication, a virtual interface is created to make the two NICs logically work as one NIC. PSA and other TCP/IP application programs use the IP address specified for this virtual interface as the local system IP address to ensure that they can communicate with the remote system without having to consider the redundant physical configuration.

There are two choices of duplication software: Bonding or PRIMECLUSTER GLS. Either one monitors the transmission line that extends to the external switch and, if it detects an error, switches the transmission line.

As shown in [Figure 4.1](#), PRIMEQUEST achieves duplication of the transmission line from the partition to the external switch by including the external switch connected to the MMB user port in the target of monitoring by the duplication software.

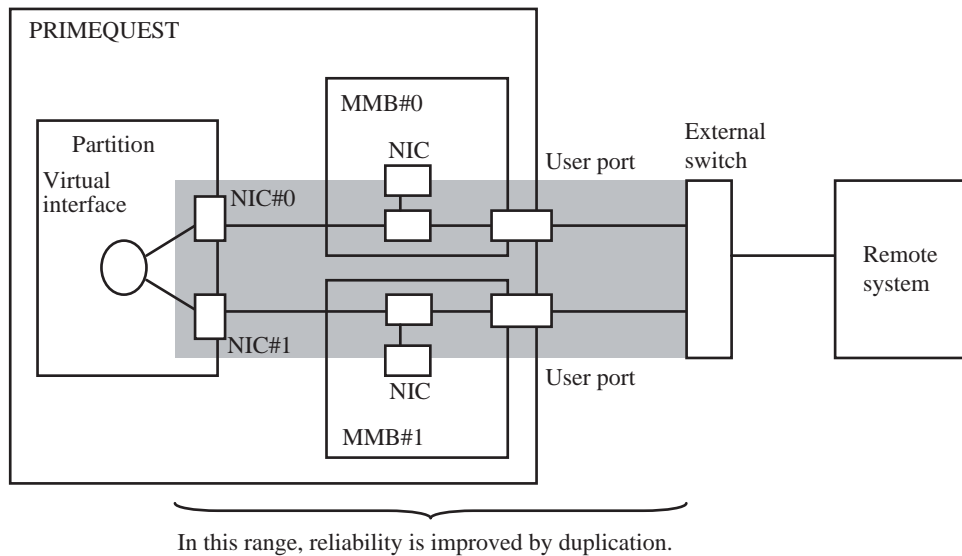


Figure 4.1 Concept of management LAN duplication in PRIMEQUEST

In addition, you can design further reliable transmission lines by duplicating the external switch and the transmission lines from the remote system to the external switch as shown in [Figure 4.2](#). The settings for duplication of the transmission line from the remote system to the external switch must be configured on the remote system.

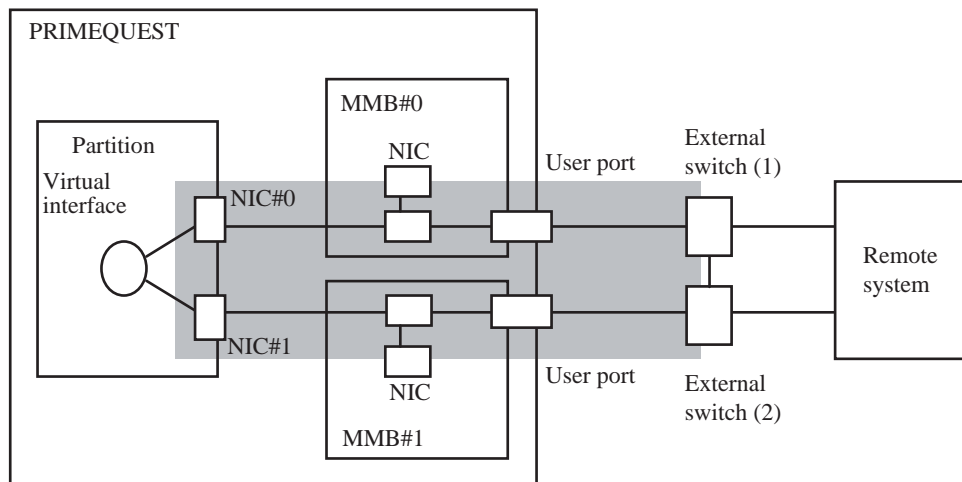


Figure 4.2 Concept of management LAN duplication in PRIMEQUEST
(a configuration characterized by improved reliability)

- Using Bonding

Note: Change the VLAN setting of the MMB management LAN hub to "VLAN Mode." (For details, see 2.2.4.5, "Setting a VLAN in a management LAN hub" in the *PRIMEQUEST 500A/500/400 Series Installation Manual*.)

- 1 Add the following to the `/etc/modprobe.conf` file.
Assign a name (bondN, where N is 0, 1, 2, ... in ascending order) to the Bonding interface.

```
# vi /etc/modprobe.conf

alias <management LAN NIC interface name 1> e100
alias <management LAN NIC interface name 2> e100
Add the following:
alias <Bonding interface name> bonding
options <Bonding interface name> max_bonds=N+1          /*1
options <Bonding interface name> mode=1
options <Bonding interface name> arp_interval=1000
options <Bonding interface name> arp_ip_target=<external switch IP address> /*2
```

- *1 If more than one Bonding interface is required, specify the number of Bonding interfaces required by including "max_bonds" in the bond0 options. The default value of this parameter is max_bonds=1.
- *2 For a configuration as shown in [Figure 4.1](#), specify one IP address. For a configuration as shown in [Figure 4.2](#), specify two IP addresses, as indicated below.

```
options <Bonding interface name> arp_ip_target=< external switch(1) IP address> ,
< external switch(2) IP address>
```

Example1: Creating a Bonding interface

The following example of the `/etc/modprobe.conf` file assumes that the management LAN interface names are eth0 and eth1. In the configuration shown in [Figure 4.2](#), the IP address of external switch (1) is 10.20.100.10 and the IP address of external switch (2) is 10.20.100.11.

```
alias eth0 e100
alias eth1 e100
alias bond0 bonding
options bond0 mode=1
options bond0 arp_interval=1000
options bond0 arp_ip_target=10.20.100.10, 10.20.100.11
```

Example 2: Adding a Bonding interface

The following example of the `/etc/modprobe.conf` file assumes that the management LAN interface names are `eth0` and `eth1`. In the configuration shown in [Figure 4.2](#), the IP address of external switch (1) is `10.20.100.10` and the IP address of external switch (2) is `10.20.100.11`.

```
alias bond0 bonding
options bond0 mode=0
options bond0 miimon=100
Add the following lines after the above lines.
options bond0 max_bonds=2
alias bond1 bonding
options bond1 mode=1
options bond1 arp_interval=1000
options bond1 arp_ip_target=10.20.100.10, 10.20.100.11
```

- 2 Edit the `ifcfg` file corresponding to the relevant interface under `/etc/sysconfig/network-scripts`. If the file does not exist, create it.

Note: If you use the PRIMEQUEST Installation Support Tool/Bundled-Software Package Installer for the package installation, do the following if a network for the management LAN is already set. Use the IP address of the `ifcfg` file, which has already been set, also for Bonding, and change the `ifcfg` file as in the duplication settings in this section.

- Management LAN NIC interface 0: `ifcfg-<interface name 1>`
Example: `ifcfg-eth0`
- Management LAN NIC interface 1: `ifcfg-<interface name 2>`
Example: `ifcfg-eth1`
- Bonding interface: `ifcfg-<Bonding interface name>` Example: `ifcfg-bond0`

A hardware address is required for setting the `ifcfg` file for the management LAN NIC interface.

If the address is not confirmed, use the `ifconfig` command to confirm it.

Command syntax:

```
/sbin/ifconfig -a
```

Example: The hardware address for the eth0 interface is 00:D0:B7:53:89:C3.

```
# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)
```

Edit or create the ifcfg file for each interface.

- Editing the ifcfg file for the management LAN NIC interface

```
# vi /etc/sysconfig/network-scripts/ifcfg-<NIC interface name>
```

Change or add the subsequent lines as shown below (you can arrange the lines in any order).

```
DEVICE=<NIC interface name>
BOOTPROTO=none
HWADDR=<hardware address>
ONBOOT=yes
MASTER=<Bonding interface name>
SLAVE=yes
```

- Editing the ifcfg file for the Bonding interface

```
# vi /etc/sysconfig/network-scripts/ifcfg-<Bonding interface name>
```

Change or add the subsequent lines as shown below (you can arrange the lines in any order).

```
DEVICE=<Bonding interface name>
BOOTPROTO=static
ONBOOT=yes
BROADCAST=<management LAN BROADCAST address>
IPADDR=<management LAN IP address>
NETMASK=<management LAN subnet mask>
```

Example: The following shows an example of the ifcfg file on the assumption that the management LAN interfaces are eth0 and eth1, and that the Bonding interface is bond0.

- ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=none
HWADDR=00:04:23:AB:94:5E
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

- ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:04:23:AB:94:5F
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

- ifcfg-bond0

```
DEVICE=bond0
BOOTPROTO=static
ONBOOT=yes
BROADCAST=192.168.0.255
IPADDR=192.168.0.1
NETMASK=255.255.255.0
```

Then, restart the network service to activate the Bonding interface.

Command syntax:

```
/sbin/service network restart
```

- Using PRIMECLUSTER GLS

For information on how to make the settings to duplicate the management LAN using PRIMECLUSTER GLS, see the PRIMECLUSTER GLS manuals.

Only the "NIC switching method" can be used for the duplication of the management LAN.

At this time, specify the external switches connected to the MMB user ports shown in [Figure 4.1](#) and [Figure 4.2](#) as the monitored hubs.

Note: If you use the PRIMEQUEST Installation Support Tool/Bundled-Software Package Installer for the package installation, do the following if a network for the management LAN is already set. Use the IP address of the ifcfg file, which has already been set, also for PRIMECLUSTER GLS, and perform the duplication settings according to the PRIMECLUSTER GLS manuals. After configuring the duplication settings by the GLS, restart the network service and then restart the PSA.

Command syntax:

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

4.1.2.2 Checking the required functions for PSA operation

The packages listed below are required for the PSA to run. Use the rpm command to check that each package is installed.

- net-snmp
- net-snmp-utils
- openssl
- gdb
- FJSVfepcl-related packages
- parted

Note: The command used for this check of FJSVfepcl-related packages depends on the OS version.

For details, see the *PRIMEQUEST 500/400 Series HBA Blockage Function User's Guide* (C122-E046EN).

In RHEL-AS4 (IPF)

Command: FJSVfepcl

Driver: FJSVfepcl-driver-<OS-version>

In RHEL5 (IPF)

Command: FJSVfepcl-<OS-version>-kmod-common

Driver: kmod-FJSVfepcl-driver-<OS-version>

Actually, <OS-version> is replaced by a character string indicating the OS version (e.g., RHEL4, RHEL4E2, RHEL5, RHEL5-xen).

Command syntax:

```
/bin/rpm -q <package name>
```

Use the uname command to check the kernel version.

Command syntax:

```
/bin/uname -r
```

Example: Checking whether the net-snmp package is installed, and the output result when it is installed:

```
#!/bin/rpm -q net-snmp
net-snmp-5.1.2-11
```

If the package is not installed, install the OS from the installation CD by using the RPM package installation method.

4.1.2.3 Checking the SELinux function settings

On the OS (redhat Linux) running in the partition on which you are installing the PSA, check whether SELinux functions are enabled. If they are, disable them.

The PRIMEQUEST system runs with the SELinux functions disabled.

Do as follows to verify whether the SELinux function is disabled. If not, disable it by editing the config file (/etc/selinux/config).

- Checking the setting

```
#cd /etc/selinux/  
#more config  
  
.....  
SELINUX=disabled  
.....
```

- Changing the setting

```
# vi /etc/selinux/config  
Change the following definition:  
.....  
SELINUX=disabled
```

4.1.3 PSA installation

Execute the following command to install the PSA package:

Command syntax:

```
/bin/rpm -ivh FJSVpsa-X.X.X-X.ia64.rpm
```

X.X.X-X is a PSA version.

4.1.4 Items automatically set during PSA installation

During PSA installation, the following modifications required for PSA operation are automatically put into effect:

- Addition of settings to syslog.conf
- Addition of settings to snmpd.conf
- snmptrapd.conf file setup
- Disabling of salinfo or salinfo_decode automatic startup setting (*1)
- Disabling of smartd automatic startup setting
- Addition of description to the services file (*2)

*1 These automatic startup settings are disabled because of conflicts with some PSA functions.

*2 Added port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. They may need to be changed.

4.1.5 Installing SIRMS

Use the following command to install two SIRMS packages.

Command syntax:

```
/bin/rpm -ivh sirms-X.X.X-X.ia64.rpm  
/bin/rpm -ivh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

X.X.X-X is a version.

4.1.6 Rebooting the partition

Reboot the partition after installing PSA and SIRMS.

```
/sbin/reboot
```

4.1.7 Settings after PSA installation

This section describes the settings to be made after PSA installation.

- [Checking the firewall function \(releasing ports\)](#) (→ [4.1.7.1](#))
- [Setting the destination of trap sending from the partition](#) (→ [4.1.7.2](#))
- [Setting the destinations of trap and e-mail sending via the MMB](#) (→ [4.1.7.3](#))
- [Other settings](#) (→ [4.1.7.4](#))

4.1.7.1 Checking the firewall function (releasing ports)

If the partition port has not been released during the firewall setting, release the ports required for PSA operation. Specifically, release the following ports for the management LAN interfaces that have been set:

- snmp port : udp / snmp or 161
- snmptrap port : udp / snmptrap or 162 (*1) (to the physical IP address of the MMB (both systems))
- web-mmb communication port : tcp / fj-webgate or 24450 (*2) (to the virtual IP address of the MMB)
- rmcp+ port : udp/7000 to 7100 (*1) (to the physical IP address of the MMB (both systems))
- localhost snmp port : udp/1025-65535
- psa-mmb communication port : tcp/MMB side 5000 (Note 3) (to the virtual IP address of the MMB)
icmp/icmp-type0, icmp-type8 (to the virtual IP address of the MMB)

*1 Release the port only when a PCL linkage is used.

Use the iptables command for checking the firewall setting.

*2 web-mmb communication port

*3 This is communication for the MMB 5000 port.

Because the partition operates as the client under this communication, the port number used at the partition side is undefined. (Any number from tcp/1025 to 65535 is selected for one port.)

Moreover, as indicated in the example below, no setting is required for port number 5000 when connection startup from the partition is enabled, or when communication is enabled for connection with the partition that has been established.

(Example)iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Command syntax:

`/sbin/iptables -L`

Use the iptables command or another command to release the port. For the usage, see command man.

Command syntax:

`/usr/bin/man iptables`

4.1.7.2 Setting the destination of trap sending from the partition

Notes:

- Make this setting only if required.
- The setting is required if partitions are managed with operation management software.

When sending SNMP traps from the partition, you must set the trap send destination on the partition. Add the trap send destination to the `snmpd.conf` file.

- Editing `snmpd.conf`

```
# vi /etc/snmp/snmpd.conf

Add the following lines for the SNMP version to be used. The lines can be provided in any order.
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
trapssess SNMPCMD_ARGS HOST[:PORT] # SNMPv3 trap setting
```

The settings are detailed below:

- Setting SNMPv1/SNMPv2 traps

```
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
```

Define the host that receives the traps (to which traps are sent).

- With this setting made, a cold start trap is sent when `snmpd` is started. If SNMP trap sending from the partition is defined, a trap is also sent when authentication fails.
- Multiple destinations can be defined by specifying multiple pairs of the `trapsink` and `trap2sink` lines.
- If `COMMUNITY` is not specified, the character string previously specified by the `trapcommunity` directive is used.

The `trapcommunity` command sets the default community string used to send traps. When using `trapcommunity` to set the community string, specify the string before the pair of `trapsink`-`trap2sink` lines.

```
trapcommunity STRING #COMMUNITY name setting
```

- If `PORT` is not specified, the default SNMP trap port (162) is used.

Example: When you want to send traps with the community name "public" to port 162 of the manager with IP address 192.168.1.10.

trapsink	192.168.1.10	public	162	##SNMPv1 trap setting
trap2sink	192.168.1.10	public	162	##SNMPv2 trap setting

● SNMPv3 trap setting

trapssess	SNMPCMD_ARGS	HOST[:PORT]	#SNMPv3 trap setting
-----------	--------------	-------------	----------------------

Define the host that receives the traps (to which traps are sent). If PORT is not specified, the default SNMP trap port (162) is used.

The major options that can be specified for SNMPCMD_ARGS are as follows:

- v version : Specifies the SNMP version. Specify 3 for SNMPv3.
- e engineID : Specifies the value of oldEngineID in the /var/net-snmp/snmpd.conf file in the trap sender.
- u secName : Specifies the SNMPv3 account. It must be the same as the setting in the manager.
- l secLevel : Specifies one of the following according to the security level of SNMPv3 messages:

Table 4.1 secLevel settings

Setting	Authentication	Encryption
noAuthNoPriv	No	No
authNoPriv	Yes	No
authPriv	Yes	Yes

- a authProtocol : Specifies MD5 or SHA as the protocol used to authenticate SNMPv3 messages. If SHA is to be used, a package must be created using openssl that is installed. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if authentication is not included.
- A authPassword : Specifies an authentication password (eight or more characters). The password must be the same as the setting in the manager. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if the authentication is not included.

- x privProtocol : Specifies the protocol used to encrypt SNMPv3 messages. Currently, only DES is supported as a privacy protocol. If encryption is included in the security level specified by the -l option, this option is valid; otherwise, it may be omitted.
- X privPassword : Specifies an encryption password (eight or more characters). The password must be the same as the setting in the manager. If encryption is included in the security level specified by the -l option, this option is valid; otherwise, it may be omitted.

Example: When you want to send SNMPv3 traps with the "PRIMEQUEST" account, with authentication and encryption enabled, to port 162 of the manager with IP address 192.168.1.10.

```
trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv -a
MD5 -A 00000000
-x DES -X 11111111 192.168.1.10:162      ##SNMPv3 trap setting
```

After setting the trap transfer destination, restart snmpd by executing the following command:

```
#/etc/rc.d/init.d/snmpd restart
```

After snmpd has been reactivated, activate PSA.

```
#/sbin/service y30FJSVpsa stop
#/sbin/service y30FJSVpsa start
```

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard net-snmp trap that would be used to restart snmpd. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that net-snmp standard traps can be received.

Restart snmpd by executing the following command on the trap transfer source machine:

```
# /etc/rc.d/init.d/snmpd restart
```

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard net-snmp trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 12:00:53 shaka snmptrapd[2600]: 2005-08-17 12:00:53
pq-server.fujitsu.com [192.168.1.10] (via 192.168.1.10) TRAP, SNMP v1,
community public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0)
Uptime: 0:00:00.17
```

4.1.7.3 Setting the destinations of trap and e-mail sending via the MMB

Notes:

- Make this setting only if required.
- The setting is required if partitions are managed with operation management software (such as Systemwalker).

The destinations of trap and e-mail sending via the MMB can be set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.1.7.4 Other settings

Remarks: Make this setting only if required.

- Setting required when a replicated disk is used
You can build a new partition by using a disk copied from a partition in the same cabinet, such as disk copy. In this case, you need to manually change the EngineID of SNMPv3 used for the PSA internal communication.

You can change the EngineID with root authority as follows:

- 1 Use the ps command to check whether PSA is active.

Command syntax:

<pre>ps ax grep psa</pre>

Example: PSA is active if the following processes under /opt/FJSVpsa/bin/ are displayed.

```
# ps ax | grep psa
4562 ?      S          0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/global/pmpsa.conf
4563 ?      S          0:18 /opt/FJSVpsa/bin/loggetd -p /
4564 ?      S          0:06 /opt/FJSVpsa/bin/sisp -p /
4565 ?      S          0:00 /opt/FJSVpsa/bin/mmbm -p /
4566 ?      S          0:01 /opt/FJSVpsa/bin/mmbs -p /
4567 ?      S          0:02 /opt/FJSVpsa/bin/fs -p /
4568 ?      S          0:00 /opt/FJSVpsa/bin/ciipmi -p /
4569 ?      S          7:40 /opt/FJSVpsa/bin/cilog -p /
4570 ?      S          8:47 /opt/FJSVpsa/bin/cios -p /
.
.
4578 ?      S          0:00 /opt/FJSVpsa/bin/cisalchild 1 /
4819 ?      Sl         0:00 /opt/FJSVpsa/bin/webgate -p /
21670 pts/5  S+         0:00 grep  psa
```

2 If PSA is active, use the service command to stop PSA.

Command syntax:

```
/sbin/service y30FJSVpsa stop
```

3 Enter the ps command to check whether snmpd is active.

Command syntax:

```
ps ax | grep snmpd
```

Example: snmpd is active if /usr/sbin/snmpd is displayed.

```
# ps ax | grep snmpd
32611 ?      S          0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/snmpd -a
```

4 If snmpd is active, enter the service command to stop snmpd.

Command syntax:

```
/sbin/service snmpd stop
```

5 Change the value of oldEngineID defined in the /var/net-snmp/snmpd.conf file.

Remarks: You can change to any value in up to 34 hexadecimal digits, provided that it is unique throughout the partitions in the same cabinet.

Example: To change the value of oldEngineID to 0x19760523

```
#vi /var/net-snmp/snmpd.conf  
oldEngineID 0x19760523
```

6 Enter the service command to start snmpd.

Command syntax:

```
/sbin/service snmpd start
```

7 Change the current directory to /opt/FJSVpsa/sh/ to regenerate the snmpv3 password used for the PSA internal communication.

Command syntax:

```
cd /opt/FJSVpsa/sh/
```

8 Execute snmpsetup.sh in the above directory.

Executing this command automatically generates the snmpv3 password used for the PSA internal communication.

Command syntax:

```
./snmpsetup.sh install
```

9 Start PSA.

Command syntax:

```
/sbin/service y30FJSVpsa start
```

4.1.8 PSA update installation

Using the following commands in the order shown, stop the PSA service, and perform update installation for the PSA package.

Command syntax:

Update from PSA-1.2.X-X or late

```
/sbin/service y30FJSVpsa stop  
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm  
/sbin/service y30FJSVpsa start
```


Update from PSA-1.1.X-X

```
/sbin/service y30FJSVpsa stop
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm
/sbin/service y10FJSVpsa start
/sbin/service y30FJSVpsa start
```

* X.X.X-X indicates the PSA version.

4.1.9 SIRMS update installation

Using the following commands, perform update installation for the two SIRMS packages.

Command syntax:

```
/bin/rpm -Uvh sirms-X.X.X-X.ia64.rpm
/bin/rpm -Uvh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

* X.X.X-X indicates the version.

4.1.10 PSA uninstallation

Using the following commands in the order shown, stop the PSA service, and uninstall the PSA package.

Command syntax:

```
/sbin/service y30FJSVpsa stop
/bin/rpm -e FJSVpsa
```

4.1.11 SIRMS uninstallation

Using the following commands, uninstall the two SIRMS packages.

Command syntax:

```
/bin/rpm -e sirms
/bin/rpm -e FJSVsoftmsg
```

4.2 Manual PSA installation (Linux: Red Hat) (PRIMEQUEST 520A/520/420)

This section describes Manual PSA installation (Linux) to Linux OS (Red Hat).

Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

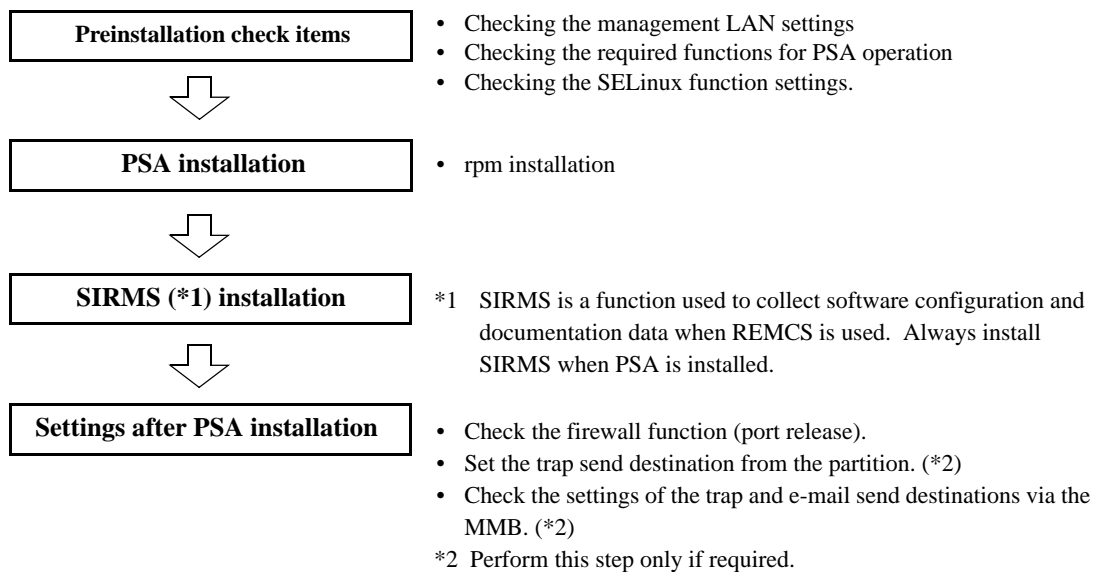
- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog system monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of CPU, DIMM, and chip set recoverable errors
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- OS information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.
- Maintenance cannot be performed on hard disks during operation. The partition or BB system must be shut down during such maintenance.
- Linkage with PRIMECLUSTER is disabled.

Note: If the PEXU has been mounted, use PSA-1.10 or later.

4.2.1 Installation Workflow

The figure below shows the workflow for PSA installation.

Note: After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.



Remarks: If you choose to use the PRIMEQUEST Installation Support Tool/Bundled-Software Package Installer for package installation, you do not need to install PSA and SIRMS. However, after the package installation using the PRIMEQUEST Installation Support Tool/Bundled-Software Package Installer, you need to confirm and set the items included in "Checking required before installation" and "Setup required after installation" explained above.

4.2.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.2.2.1)
- [Checking the required functions for PSA operation](#) (→ 4.2.2.2)
- [Checking the SELinux function settings](#) (→ 4.2.2.3)

4.2.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: To use the PRIMEQUEST installation support tool or bundled-software package installer for package installation, the appropriate settings must be made after batch package installation.

(1) Checking the settings for the NIC of the management LAN

Execute the following command to check the interface name assigned to the NIC of the management LAN.

- 1 Enter the `ifconfig` command to list the network interfaces recognized by the system and confirm the relevant interface name.

Command syntax:

```
/sbin/ifconfig -a
```

Example: eth0, eth1, and lo displayed on the left side are interface names.

```
# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.1.12  Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3865 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

- 2 Use the ethtool command to find network interface controller (NIC) for the management LAN. Enter the command for each interface displayed in step 1 as shown below.

The NICs for the management LAN have bus-info (SEG:BUS:DEV.FUNC number) 0000:01:08.0.

Command syntax:

```
/sbin/ethtool -i <interface-name>
```

Example: As the result of command execution for eth0, the interface matches the NIC for the management LAN.

```
# /sbin/ethtool -i eth0
  driver: e100
  version: 3.0.27-k2-NAPI
  firmware-version: N/A
  bus-info: 0000:01:08.0 (Matches a NIC for the management LAN)
```

(2) Setting the NIC for the management LAN

- 1 Edit the ifcfg file corresponding to the relevant interface under /etc/sysconfig/network-scripts. If the file does not exist, create it.
 - Management LAN NIC interface: ifcfg-<interface name> Example: ifcfg-eth0

A hardware address is required for setting the ifcfg file for the management LAN NIC interface.

If the address is not confirmed, use the ifconfig command to confirm it.

Command syntax:

```
/sbin/ifconfig -a
```

Example: The hardware address for the eth0 interface is 00:D0:B7:53:89:C3.

```
# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)
```

Edit or create the ifcfg file for each interface.

- Editing the ifcfg file for the management LAN NIC interface

```
# vi /etc/sysconfig/network-scripts/ifcfg-<NIC interface name>
```

Change or add the subsequent lines as shown below (you can arrange the lines in any order).

```
DEVICE=<NIC interface name>
```

```
BOOTPROTO=static
```

```
HWADDR=<hardware address>
```

```
ONBOOT=yes
```

```
BROADCAST=<management LAN BROADCAST address>
```

```
IPADDR=<management LAN IP address>
```

```
NETMASK=<management LAN subnet mask>
```

Example: The following shows an example of the ifcfg file on the assumption that the management LAN interface is eth0.

- ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:D0:B7:53:89:C3
ONBOOT=yes
BROADCAST=192.168.0.255
IPADDR=192.168.0.1
NETMASK=255.255.255.0
```

Then, restart the network service to activate the network interface.

Command syntax:

```
/sbin/service network restart
```

4.2.2.2 Checking the required functions for PSA operation

The packages listed below are required for the PSA to run. Use the `rpm` command to check that each package is installed.

- net-snmp
- net-snmp-utils
- openssl
- gdb
- FJSVfepcl-related packages
- parted

Note: The command used for this check of FJSVfepcl-related packages depends on the OS version.

For details, see the *PRIMEQUEST 500/400 Series HBA Blockage Function User's Guide* (C122-E046EN).

In RHEL-AS4 (IPF)

Command: FJSVfepcl

Driver: FJSVfepcl-driver-<OS-version>

In RHEL5 (IPF)

Command: FJSVfepcl-<OS-version>-kmod-common

Driver: kmod-FJSVfepcl-driver-<OS-version>

Actually, <OS-version> is replaced by a character string indicating the OS version (e.g., RHEL4, RHEL4E2, RHEL5, RHEL5-xen).

Command syntax:

```
/bin/rpm -q <package name>
```

Use the uname command to check the kernel version.

Command syntax:

```
/bin/uname -r
```

Example: Checking whether the net-snmp package is installed, and the output result when it is installed:

```
#/bin/rpm -q net-snmp  
net-snmp-5.1.2-11
```

If the package is not installed, install the OS from the installation CD by using the RPM package installation method.

4.2.2.3 Checking the SELinux function settings

On the OS (redhat Linux) on which you are installing the PSA, check whether SELinux functions are enabled. If they are, disable them.

The PRIMEQUEST system runs with the SELinux functions disabled.

Do as follows to verify whether the SELinux function is disabled. If not, disable it by editing the config file (/etc/selinux/config).

- Checking the setting

```
#cd /etc/selinux/  
#more config  
  
.....  
SELINUX=disabled  
.....
```

- Changing the setting

```
# vi /etc/selinux/config  
Change the following definition:  
.....  
SELINUX=disabled
```

4.2.3 PSA installation

Execute the following command to install the PSA package:

Command syntax:

```
/bin/rpm -ivh FJSVpsa-X.X.X-X.i686.rpm
```

X.X.X-X is a PSA version.

4.2.4 Items automatically set during PSA installation

During PSA installation, the following modifications required for PSA operation are automatically put into effect:

- Addition of settings to syslog.conf
- Addition of settings to snmpd.conf
- snmptrapd.conf file setup
- Disabling of salinfo or salinfo_decode automatic startup setting (*1)
- Disabling of smartd automatic startup setting
- Addition of description to the services file (*2)

*1 These automatic startup settings are disabled because of conflicts with some PSA functions.

*2 Added port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. They may need to be changed.

4.2.5 Installing SIRMS

Use the following command to install two SIRMS packages.

Command syntax:

```
/bin/rpm -ivh sirms-X.X.X-X.ia64.rpm  
/bin/rpm -ivh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

X.X.X-X is a version.

4.2.6 Rebooting the OS

Reboot the OS after installing PSA and SIRMS.

```
/sbin/reboot
```

4.2.7 Settings after PSA installation

This section describes the settings to be made after PSA installation.

- [Checking the firewall function \(releasing ports\)](#) (→ [4.2.7.1](#))
- [Setting the destination of trap sending from the partition](#) (→ [4.2.7.2](#))
- [Setting the destinations of trap and e-mail sending via the MMB](#) (→ [4.2.7.3](#))
- [Other settings](#) (→ [4.2.7.4](#))

4.2.7.1 Checking the firewall function (releasing ports)

If the port has not been released during the firewall setting, release the ports required for PSA operation. Specifically, release the following ports for the management LAN interfaces that have been set:

- snmp port : udp / snmp or 161
- snmptrap port : udp / snmptrap or 162 (*1)
(to the IP address of the MMB)
- web-mmb communication port : tcp / fj-webgate or 24450 (*2)
(to the IP address of the MMB)
- rmcp+ port : udp/7000 to 7100 (*1)
(to the IP address of the MMB)
- localhost snmp port : udp/1025-65535
- psa-mmb communication port : tcp/MMB side 5000 (Note 3) (to the virtual IP address of the MMB)
icmp/icmp-type0, icmp-type8 (to the virtual IP address of the MMB)

*1 Release the port only when a PCL linkage is used.

Use the iptables command for checking the firewall setting.

*2 web-mmb communication port

*3 This is communication for the MMB 5000 port.

Because PSA operates as a client under this communication, the port number used by PSA is undefined. (Any number ranging from tcp/1025 to 65535 is selected for one port.)

Moreover, as indicated in the example below, no setting is required for port number 5000 while connection startup is enabled or while communication is enabled for an established connection with the port.

(Example)iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Command syntax:

```
/sbin/iptables -L
```

Use the iptables command or another command to release the port. For the usage, see command man.

Command syntax:

```
/usr/bin/man iptables
```

4.2.7.2 Setting the destination of trap sending from the partition

Notes:

- Make this setting only if required.
- This setting is required for linkage with operation management software.

When sending SNMP traps, you must set the trap send destination. Add the trap send destination to the `snmpd.conf` file.

- Editing `snmpd.conf`

```
# vi /etc/snmp/snmpd.conf
```

Add the following lines for the SNMP version to be used. The lines can be provided in any order.

```
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
trapsess SNMPCMD_ARGS HOST[:PORT] # SNMPv3 trap setting
```

The settings are detailed below:

- Setting SNMPv1/SNMPv2 traps

```
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
```

Define the host that receives the traps (to which traps are sent).

- With this setting made, a cold start trap is sent when `snmpd` is started. If SNMP trap sending is defined, a trap is also sent when authentication fails.
- Multiple destinations can be defined by specifying multiple pairs of the `trapsink` and `trap2sink` lines.
- If `COMMUNITY` is not specified, the character string previously specified by the `trapcommunity` directive is used.

The `trapcommunity` command sets the default community string used to send traps. When using `trapcommunity` to set the community string, specify the string before the pair of `trapsink`-`trap2sink` lines.

```
trapcommunity STRING #COMMUNITY name setting
```

- If `PORT` is not specified, the default SNMP trap port (162) is used.

Example: When you want to send traps with the community name "public" to port 162 of the manager with IP address 192.168.1.10.

trapsink	192.168.1.10	public	162	##SNMPv1 trap setting
trap2sink	192.168.1.10	public	162	##SNMPv2 trap setting

● SNMPv3 trap setting

trapssess	SNMPCMD_ARGS	HOST[:PORT]	#SNMPv3 trap setting
-----------	--------------	-------------	----------------------

Define the host that receives the traps (to which traps are sent). If PORT is not specified, the default SNMP trap port (162) is used.

The major options that can be specified for SNMPCMD_ARGS are as follows:

- v version : Specifies the SNMP version. Specify 3 for SNMPv3.
- e engineID : Specifies the value of oldEngineID in the /var/net-snmp/snmpd.conf file in the trap sender.
- u secName : Specifies the SNMPv3 account. It must be the same as the setting in the manager.
- l secLevel : Specifies one of the following according to the security level of SNMPv3 messages:

Table 4.2 secLevel settings

Setting	Authentication	Encryption
noAuthNoPriv	No	No
authNoPriv	Yes	No
authPriv	Yes	Yes

- a authProtocol : Specifies MD5 or SHA as the protocol used to authenticate SNMPv3 messages. If SHA is to be used, a package must be created using openssl that is installed. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if authentication is not included.
- A authPassword : Specifies an authentication password (eight or more characters). The password must be the same as the setting in the manager. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if the authentication is not included.

- x privProtocol** : Specifies the protocol used to encrypt SNMPv3 messages. Currently, only DES is supported as a privacy protocol. If encryption is included in the security level specified by the **-l** option, this option is valid; otherwise, it may be omitted.
- X privPassword** : Specifies an encryption password (eight or more characters). The password must be the same as the setting in the manager. If encryption is included in the security level specified by the **-l** option, this option is valid; otherwise, it may be omitted.

Example: When you want to send SNMPv3 traps with the "PRIMEQUEST" account, with authentication and encryption enabled, to port 162 of the manager with IP address 192.168.1.10.

```
trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv -a
MD5 -A 00000000
-x DES -X 11111111 192.168.1.10:162      ##SNMPv3 trap setting
```

After setting the trap transfer destination, restart snmpd by executing the following command:

```
#/etc/rc.d/init.d/snmpd restart
```

After snmpd has been reactivated, activate PSA.

```
#/sbin/service y30FJSVpsa stop
#/sbin/service y30FJSVpsa start
```

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard net-snmp trap that would be used to restart snmpd. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that net-snmp standard traps can be received.

Restart snmpd by executing the following command on the trap transfer source machine:

```
# /etc/rc.d/init.d/snmpd restart
```

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard net-snmp trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 12:00:53 shaka snmptrapd[2600]: 2005-08-17 12:00:53
pq-server.fujitsu.com [192.168.1.10] (via 192.168.1.10) TRAP, SNMP v1,
community public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0)
Uptime: 0:00:00.17
```

4.2.7.3 Setting the destinations of trap and e-mail sending via the MMB

Notes:

- Make this setting only if required.
- The setting is required if partitions are managed with operation management software (such as Systemwalker).

The destinations of trap and e-mail sending via the MMB can be set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.2.7.4 Other settings

Remarks: Make this setting only if required.

- Setting required when a replicated disk is used
You can build a new partition by using a disk copied from a partition in the same cabinet, such as disk copy. In this case, you need to manually change the EngineID of SNMPv3 used for the PSA internal communication.

You can change the EngineID with root authority as follows:

- 1 Use the ps command to check whether PSA is active.

Command syntax:

<pre>ps ax grep psa</pre>

Example: PSA is active if the following processes under /opt/FJSVpsa/bin/ are displayed.

```
# ps ax | grep psa
4562 ?      S          0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/
global/pmpsa.conf
4563 ?      S          0:18 /opt/FJSVpsa/bin/loggetd -p /
4564 ?      S          0:06 /opt/FJSVpsa/bin/sisp -p /
4565 ?      S          0:00 /opt/FJSVpsa/bin/mmbm -p /
4566 ?      S          0:01 /opt/FJSVpsa/bin/mmbs -p /
4567 ?      S          0:02 /opt/FJSVpsa/bin/fs -p /
4568 ?      S          0:00 /opt/FJSVpsa/bin/ciipmi -p /
4569 ?      S          7:40 /opt/FJSVpsa/bin/cilog -p /
4570 ?      S          8:47 /opt/FJSVpsa/bin/cios -p /
.
.
4578 ?      S          0:00 /opt/FJSVpsa/bin/cisalchild 1 /
4819 ?      Sl         0:00 /opt/FJSVpsa/bin/webgate -p /
21670 pts/5  S+         0:00 grep psa
```

2 If PSA is active, use the service command to stop PSA.

Command syntax:

```
/sbin/service y30FJSVpsa stop
```

3 Enter the ps command to check whether snmpd is active.

Command syntax:

```
ps ax | grep snmpd
```

Example: snmpd is active if /usr/sbin/snmpd is displayed.

```
# ps ax | grep snmpd
32611 ?      S          0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/
snmpd -a
```

4 If snmpd is active, enter the service command to stop snmpd.

Command syntax:

```
/sbin/service snmpd stop
```

5 Change the value of oldEngineID defined in the /var/net-snmp/snmpd.conf file.

Remarks: You can change to any value in up to 34 hexadecimal digits, provided that it is unique throughout the partitions in the same cabinet.

Example: To change the value of oldEngineID to 0x19760523

```
#vi /var/net-snmp/snmpd.conf  
oldEngineID 0x19760523
```

6 Enter the service command to start snmpd.

Command syntax:

```
/sbin/service snmpd start
```

7 Change the current directory to /opt/FJSVpsa/sh/ to regenerate the snmpv3 password used for the PSA internal communication.

Command syntax:

```
cd /opt/FJSVpsa/sh/
```

8 Execute snmpsetup.sh in the above directory.

Executing this command automatically generates the snmpv3 password used for the PSA internal communication.

Command syntax:

```
./snmpsetup.sh install
```

9 Start PSA.

Command syntax:

```
/sbin/service y30FJSVpsa start
```

4.2.8 PSA update installation

Using the following commands in the order shown, stop the PSA service, and perform update installation for the PSA package.

Command syntax:

```
/sbin/service y30FJSVpsa stop  
/bin/rpm -Uvh FJSVpsa-X.X.X-X.i64.rpm  
/sbin/service y30FJSVpsa start
```

* X.X.X-X indicates the PSA version.

4.2.9 SIRMS update installation

Using the following commands, perform update installation for the two SIRMS packages.

Command syntax:

```
/bin/rpm -Uvh sirms-X.X.X-X.ia64.rpm  
/bin/rpm -Uvh FJSVsoftmsg-X.X.X-X.ia64.rpm
```

* X.X.X-X indicates the version.

4.2.10 PSA uninstallation

Using the following commands in the order shown, stop the PSA service, and uninstall the PSA package.

Command syntax:

```
/sbin/service y30FJSVpsa stop  
/bin/rpm -e FJSVpsa
```

4.2.11 SIRMS uninstallation

Using the following commands, uninstall the two SIRMS packages.

Command syntax:

```
/bin/rpm -e sirms  
/bin/rpm -e FJSVsoftmsg
```

4.3 Manual PSA installation (Linux: SUSE) (PRIMEQUEST 500A/500/400 Series common)

This section describes Manual PSA installation (Linux) to Linux OS (SUSE). The procedure described in the section is performed after the operating system is installed.

Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

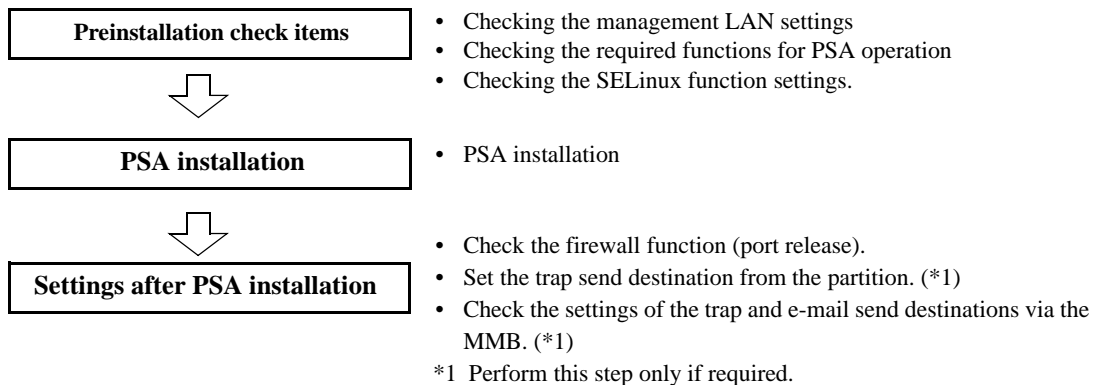
- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog system monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of CPU, DIMM, and chip set recoverable errors
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- OS information cannot be collected with operation management software.
- Maintenance cannot be performed on hard disks during operation. The partition or BB system must be shut down during such maintenance.
- Linkage with PRIMECLUSTER is disabled.

Note: If the PEXU has been mounted, use PSA-1.10 or later.

4.3.1 Installation Workflow

The figure below shows the workflow for PSA installation.

Note: After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.



4.3.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ [4.3.2.1](#))
- [Checking the required functions for PSA operation](#) (→ [4.3.2.3](#))
- [SELinux function](#) (→ [4.3.2.4](#))

4.3.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

(1) Checking the settings for the NIC of the management LAN

Execute the following command to check the interface name assigned to the NIC of the management LAN.

- 1 Enter the `ifconfig` command to list the network interfaces recognized by the system and confirm the relevant interface name.
Command syntax:

```
/sbin/ifconfig -a
```

Example: `eth0`, `eth1`, and `lo` displayed on the left side are interface names.

```
# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1      Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
          inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
          Base address:0x5cc0 Memory:fbfe0000-fc000000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3865 errors:0 dropped:0 overruns:0 frame:0
```

- 2 Use the `ethtool` command to find the network interface controller (NIC) for the management LAN. (One NIC for management LAN for PRIMEQUEST 580A/540A/580/540/480/440 and two NICs for management LAN for PRIMEQUEST 520A/520/420)

Enter the command for each interface displayed in step 1 as shown below.

The NICs for the management LAN have bus info (SEG:BUS:DEV:FUNC number) as follows:

PRIMEQUEST 580A/540A/580/540/480/440: 0000:01:08.0 and 0000:01:00.0

PRIMEQUEST 520A/520/420: 0000:01:08.0

Command syntax:

```
/usr/sbin/ethtool -i <interface-name>
```

Example: As the result of command execution for `eth0` and `eth1`, these two interfaces match the NICs for the management LAN.

Note: The following example assumes that a PRIMEQUEST 580A/540A/580/540/480/440 is used.

```
# /usr/sbin/ethtool -i eth0
    driver: e100
    version: 3.0.27-k2-NAPI
    firmware-version: N/A
    bus-info: 0000:01:00.0 (Matches a NIC for the management LAN)

# /usr/sbin/ethtool -i eth1
    driver: e100
    version: 3.0.27-k2-NAPI
    firmware-version: N/A
    bus-info: 0000:01:08.0 (Matches a NIC for the management LAN)
```

- 3 Execute the following command for the found NIC for the management LAN, and record the hardware address:

Command syntax

```
/sbin/ifconfig <interface-name>
```

Example: Command execution for eth0 and eth1

```
#!/sbin/ifconfig eth0
Link encap:Ethernet HWaddr 00:D0:B7:53:89:C3
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1107704 errors:0 dropped:0 overruns:0 frame:0
TX packets:2653820 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:390009908 (371.9 MiB) TX bytes:809006934 (771.5 MiB)

#!/sbin/ifconfig eth1
Link encap:Ethernet HWaddr 00:0E:0C:21:83:97
inet addr:192.168.1.12 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1538726 errors:0 dropped:0 overruns:0 frame:0
TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:341051195 (325.2 MiB) TX bytes:22862 (22.3 KiB)
Base address:0x5cc0 Memory:fbfe0000-fc000000
```

In this example, the hardware addresses of eth0 and eth1 are as follows:

- Hardware address of eth0: 00:D0:B7:53:89:C3
- Hardware address of eth1: 00:0E:0C:21:83:97

Then, configure each NIC for the management LAN. See one of the following sections:

- For the PRIMEQUEST 580A/540A/580/540/480/440:
 - (2) Duplicating the two NICs for the management LAN (PRIMEQUEST 580A/540A/580/540/480/440)
- For the PRIMEQUEST 520A/520/420:
 - (3) Configuring the NIC for the management LAN (PRIMEQUEST 520/420)

(2) Duplicating the two NICs for the management LAN (PRIMEQUEST 580A/540A/580/540/480/440)

- SUSE 9

To duplicate the management LAN, activate the two NICs for the management LAN in the partition and use them. The duplication software (that controls LAN duplication) directs the send packets to the appropriate transmission line considering the status of the candidate transmission lines, thus achieving redundancy. When you specify duplication, a virtual interface is created to make the two NICs logically work as one NIC. PSA and other TCP/IP application programs use the IP address specified for this virtual interface as the local system IP address to ensure that they can communicate with the remote system without having to consider the redundant physical configuration.

The duplication software monitors the transmission line that extends to the external switch and, if it detects an error, switches the transmission line.

As shown in [Figure 4.3](#), PRIMEQUEST achieves duplication of the transmission line from the partition to the external switch by including the external switch connected to the MMB user port in the target of monitoring by the duplication software.

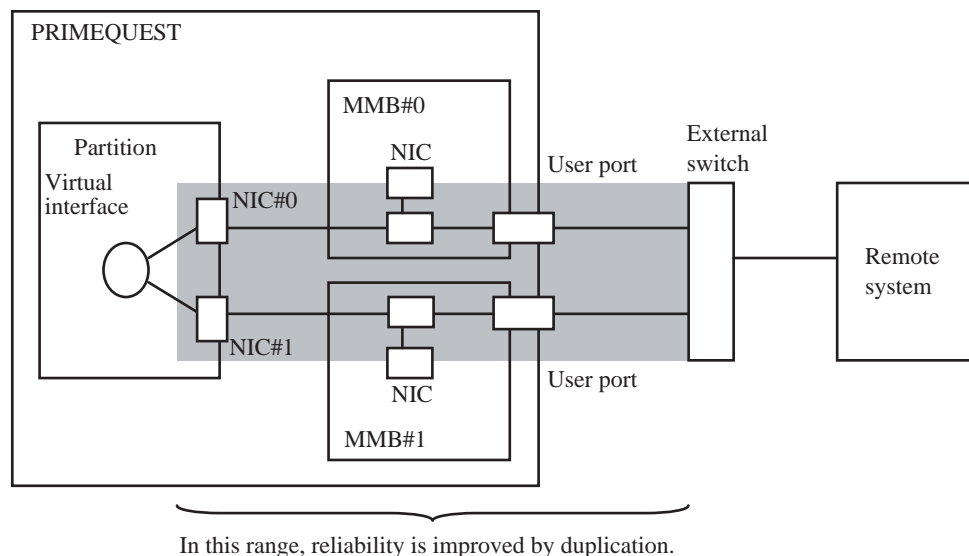


Figure 4.3 Concept of management LAN duplication in PRIMEQUEST

In addition, you can design further reliable transmission lines by duplicating the external switch and the transmission lines from the remote system to the external switch as shown in [Figure 4.4](#). The settings for duplication of the transmission line from the remote system to the external switch must be configured on the remote system.

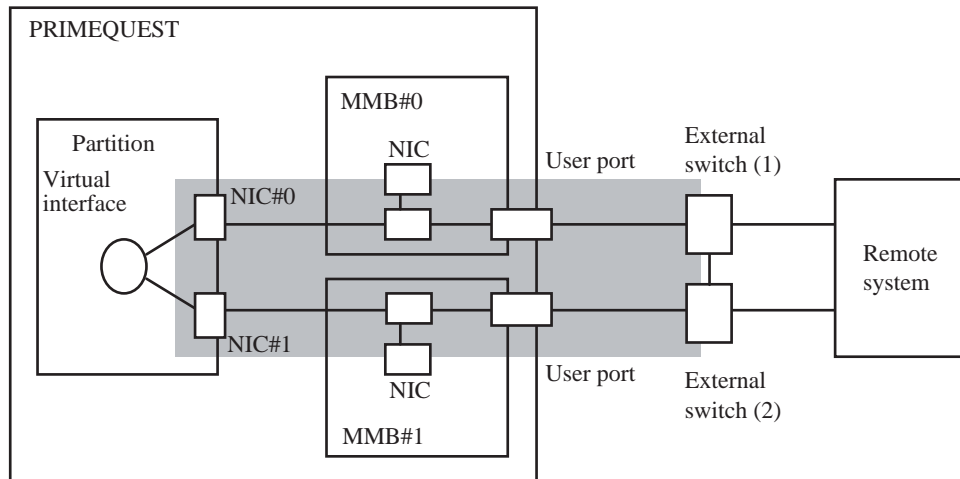


Figure 4.4 Concept of management LAN duplication in PRIMEQUEST
(a configuration characterized by improved reliability)

- Using Bonding

Note: Change the VLAN setting of the MMB management LAN hub to "VLAN Mode." (For details, see 2.3.4.5, "Setting a VLAN in a management LAN hub" in the *PRIMEQUEST 500A/500/400 Installation Manual*).

- 1 Edit the ifcfg file for the relevant interface in /etc/sysconfig/network/. If the file does not exist, create it. To edit the file, first stop the network.
 - Bonding interface: ifcfg-<bonding-interface-name> Example: ifcfg-bond0

Remarks: If the relevant interfaces for the management LAN are in /etc/sysconfig/network/, disable them by deleting them.

 - File name of the ifcfg file of the interface for the management LAN: ifcfg-eth-id-<hardware-address>
- Editing the ifcfg file of the NIC interface for the management LAN

```
# rcnetwork stop
# rm /etc/sysconfig/network/ifcfg-eth-id-<hardware-address>
..
# vi /etc/sysconfig/network/ifcfg- <bonding-interface-name>
```

Change or add lines as shown below.

Example: The editing of the ifcfg file shown in the following example assumes that the Bonding interface is ifcfg-bond0.

```
ifcfg-bond0:
    BOOTPROTO='static'
    MTU=''
    REMOTE_IPADDR=''
    IPADDR='192.168.16.138'      # Same subnet as the MMB
    NETMASK='255.255.255.0'
    BROADCAST='192.168.16.255'
    STARTMODE='onboot'
    BONDING_MASTER=yes
    BONDING_SLAVE_0='bus-pci-0000:01:08.0'
    # bus-info number for management LAN NIC#0
    BONDING_SLAVE_1='bus-pci-0000:01:00.0'
    # bus-info number for management LAN NIC#1
    BONDING_MODULE_OPTS='arp_interval=1000 arp_ip_target=192.168.16.111,
    192.168.16.112 mode=1'
    # external switch IP address
```

Then, enter "start" for the network service to activate the Bonding interface.

Command syntax:

```
rcnetwork start
```

To make the management LAN NIC settings effective, PSA need to be restarted.
Command syntax:

```
/etc/init.d/y30FJSVpsa stop
/etc/init.d/y30FJSVpsa start
```

- Using PRIMECLUSTER GLS

For the settings to duplicate the management LAN using PRIMECLUSTER GLS, see the PRIMECLUSTER GLS manual. To use PRIMECLUSTER GLS, specify the external switches connected to the MMB user ports shown in [Figure 4.3](#) and [Figure 4.4](#) as the monitored hubs.

Note: If a network has already been configured for the management LAN, use the IP address specified in the ifcfg file as the IP address for PRIMECLUSTER GLS and configure the duplication settings by following the instructions in the PRIMECLUSTER GLS manuals.

After configuring the duplication settings by the GLS, restart the network service and then restart the PSA.

Command syntax:

```
/etc/init.d/y30FJSVpsa stop
/etc/init.d/y30FJSVpsa start
```

- SUSE 10

- 1 Add the line shown below to the end of /etc/modprobe.conf.local.
Name the Bonding interface (bondN, where N is a number assigned in ascending order, such as 0, 1, 2...).

```
# vi /etc/modprobe.conf.local
```

Add the following line to the end of the file :

```
alias <Bonding interface-name> bonding
options <Bonding interface-name> mode=1 arp_interval=1000
arp_ip_target=<external-switch-IP-address> // (*1)
```

- *1 For the configuration shown in [Figure 4.5](#), specify one IP address. For the configuration shown in [Figure 4.6](#), specify two IP addresses.

```
options <Bonding interface-name> arp_ip_target=<external-switch-IP-
address(1)> , <external-switch-IP-address(2)>
```

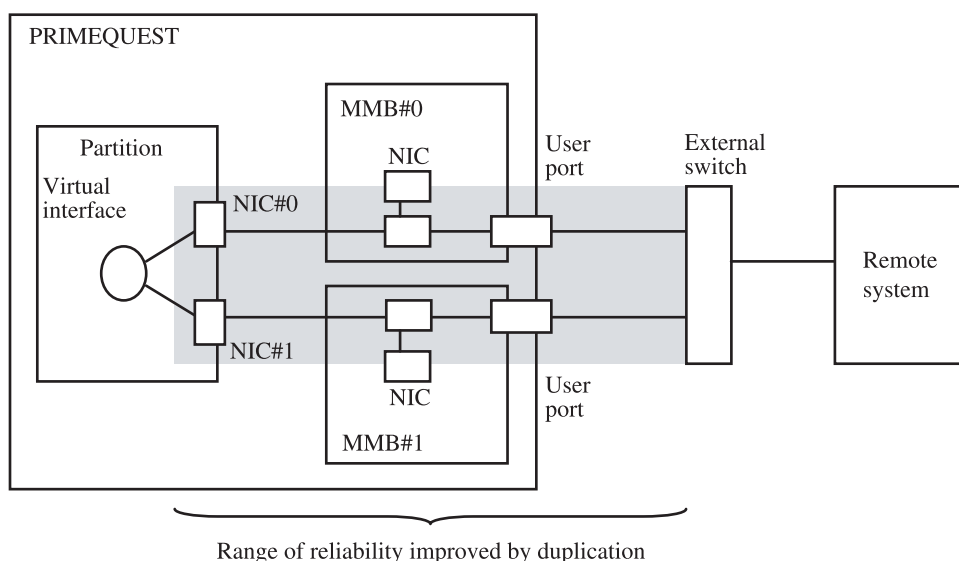


Figure 4.5 Concept of management LAN duplication in PRIMEQUEST

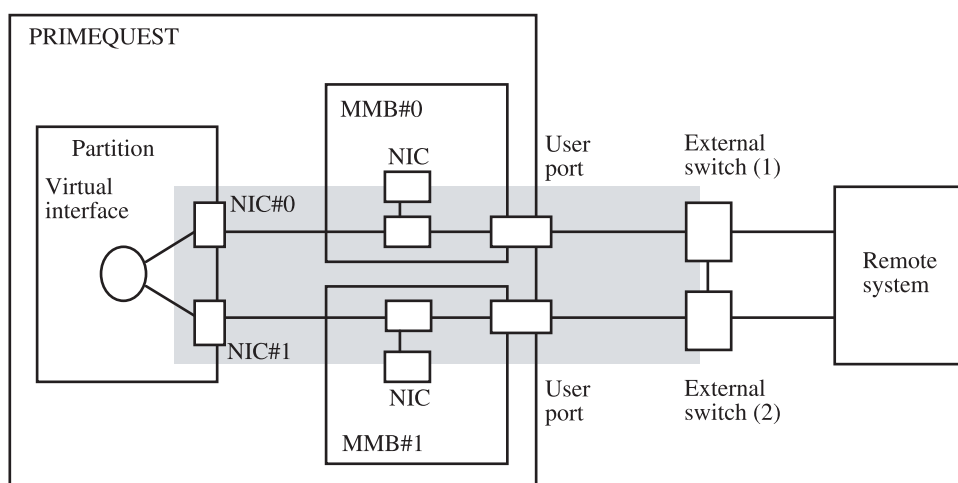


Figure 4.6 Concept of management LAN duplication in PRIMEQUEST (configuration characterized by improved reliability)

- 2 Edit the ifcfg file for the relevant interface in `/etc/sysconfig/network/`. If the file does not exist, create it. To edit the file, first stop the network.
 - Bonding interface-name: `ifcfg-<Bonding interface-name>` Example: `ifcfg-bond0`

Remarks: If the relevant interface for the management LAN is in `/etc/sysconfig/network/`, disable it by deleting it.

- File name of the ifcfg file of the interface for the management LAN: `ifcfg-eth-id-<hardware-address>`

- Editing the ifcfg file of the NIC interface for the management LAN

```
# rcnetwork stop
# rm /etc/sysconfig/network/ifcfg-eth-id-<hardware-address>
..
# vi /etc/sysconfig/network/ifcfg-<Bonding interface-name>
```

Change or add lines as shown below.

Example: The editing of the ifcfg file shown in the following examples assumes that the Bonding interface is ifcfg-bond0.

```
ifcfg-bond0:
BOOTPROTO='static'
MTU=' '
REMOTE_IPADDR=' '
IPADDR='192.168.16.138' # Same subnet as the MMB
NETMASK='255.255.255.0'
BROADCAST='192.168.16.255'
STARTMODE='onboot'
BONDING_MASTER=yes
BONDING_SLAVE_0='bus-pci-0000:01:08.0'
# bus-info number of the NIC for management LAN#0
BONDING_SLAVE_1='bus-pci-0000:01:00.0'
# bus-info number of the NIC for management LAN#1
```

The Bonding interface is activated with the restart of the network service.

Command syntax

```
/sbin/service network restart
```

To make the NIC settings for the management LAN effective, PSA needs to be restarted.

Command syntax

```
/etc/init.d/y30FJSVpsa stop
/etc/init.d/y30FJSVpsa start
```

(3) Configuring the NIC for the management LAN (PRIMEQUEST 520A/520/420)

The connected management LAN NIC must be activated for communication with the MMBs via the management LAN. Configure the NIC by following the procedure below. Use YaST to configure it.

- 1 Execute the following command, and record the card name of the NIC for the management LAN:

Command syntax

```
/sbin/lspci -s 0000:01:08.0
```

Example: In this example, the card name is "Intel Corporation 82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller".

```
# /sbin/lspci -s 0000:01:08.0
01:08.0 Ethernet controller: Intel Corporation 82562ET/EZ/
GT/GZ - PRO/100 VE (LOM) Ethernet Controller (rev 04)
```

- 2 Execute the following command to activate YaST.

Command syntax:

```
# yast
```

- 3 Select [Network Devices] - [Network Card] from the menu, and proceed to the network card selection window.
- 4 From the network cards displayed in the [Network Card Configuration] window, select the card (NIC for the management LAN) that has the name recorded in step 1.

Note: The name that is recorded in step 1 may not be displayed completely according to YaST specifications. As shown in [Figure 4.7](#), "Fujitsu" may be added in front of the card name, and only the last part of the card name may be displayed. In such cases, select the name whose displayed character strings excluding "Fujitsu" matches the last part of the name recorded in step 1.

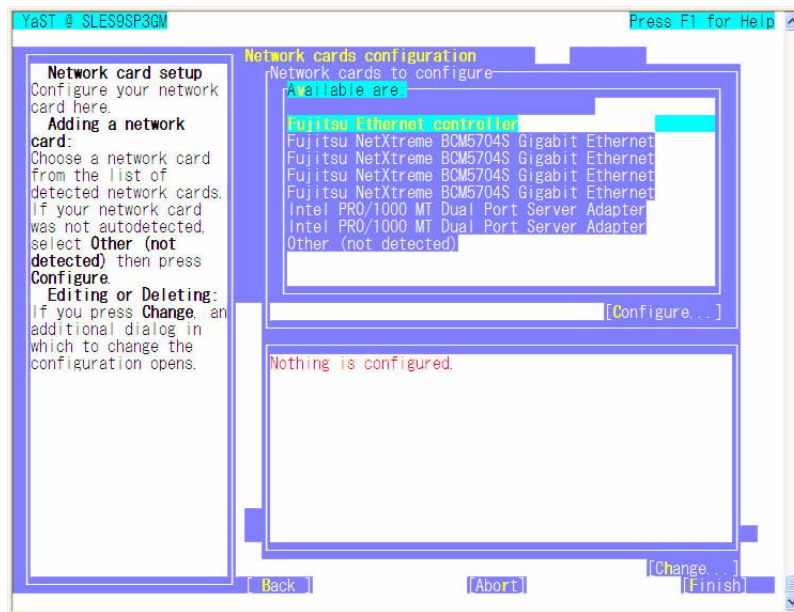


Figure 4.7 YaST window

- * This example is an SUSE9 window. The displayed contents may vary depending on the version of the OS.
 - * In the example, the second choice (Fujitsu Ethernet controller) matches the last part of the name recorded in step 1.
- 5 Go to the [Network Address Setup] window to set up the network card. Confirm that the value of [Configuration Name] includes the hardware address that was checked in (1), "Checking the settings for the NIC of the management LAN." Check [Static address setup], and specify the IP address and the subnet mask.
 Note: The specified IP address and the IP address of the MMB must have the same subnet mask.
 - 6 Quit YaST.

4.3.2.2 Procedures for monitoring syslog

When using SUSE™ Linux Enterprise Server 10, you must make the addition settings below.

Note: If you fail to make the settings below before installing PSA, the following message may be output when you install PSA and PSA may not be able to monitor driver messages.

syslogd: /var/opt/FJSVpsa/path/syslogd.fifo: Operation not permitted

Remarks: Use the [↑] and [↓] keys to move the cursor up and down on the YaST screen.

- 1 Enter the following command to confirm the active syslog daemon.

```
# grep SYSLOG_DAEMON /etc/sysconfig/syslog
```

If SYSLOG_DAEMON = If "syslog-ng" is displayed for SYSLOG_DAEMON,
/sbin/syslog-ng is running as the syslog daemon.

If SYSLOG_DAEMON = If "syslog" is displayed for SYSLOG_DAEMON,
/sbin/syslogd is running as the syslog daemon.

Record the name of the running syslog daemon.

- 2 Change the AppArmor settings by following the procedure below:

- 1) Start YaST.

```
# yast
```



Figure 4.8 YaST start screen

- 2) From the left-side menu in [Figure 4.9](#), select "Novell AppArmor" and press the [Tab] key.
Next, from the right-side menu, select "Edit Profile" and press the [Enter] key.



Figure 4.9 Novell AppArmor- select screen

- 3 Use the [Tab] key to move to "Profile Name," and check for the active syslog daemon under "Profile Name." The active syslog daemon is the one that was confirmed in step 1.
If you do not find the active syslog daemon under "Profile Name," the subsequent settings need not be made. In this case, select "Abort" from the bottom menu, and press the [Enter] key to exit from this window. Then, select "Quit" from the bottom menu, and press the [Enter] key to quit YaST.
If you find the active syslog daemon under "Profile Name," select the name of the syslog daemon. Then, press the [Tab] key to select "Next" from the bottom menu, and press the [Enter] key.

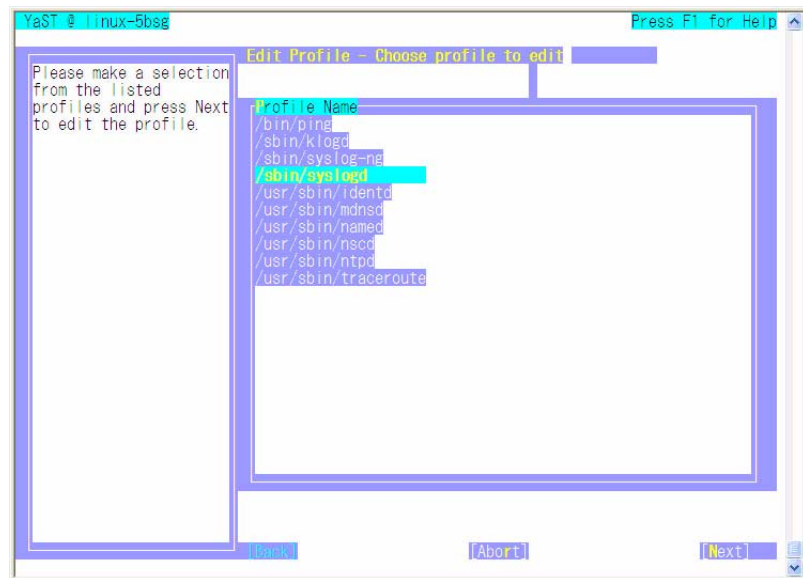


Figure 4.10 AppArmor Profile select screen

- 4 Press the [Tab] key to select "Add Entry" from the bottom menu, and press the [Enter] key.

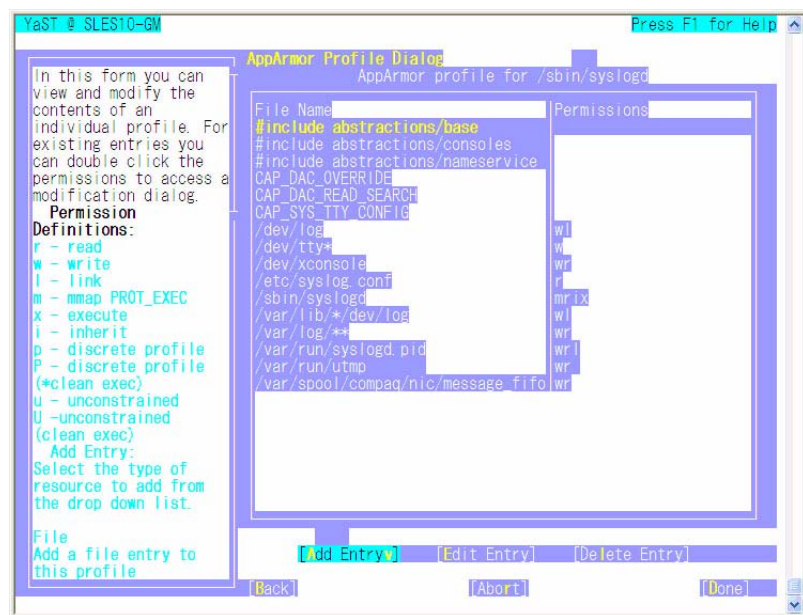


Figure 4.11 AppArmor Profile window

Select "File" from the displayed list, and press the [Enter] key.

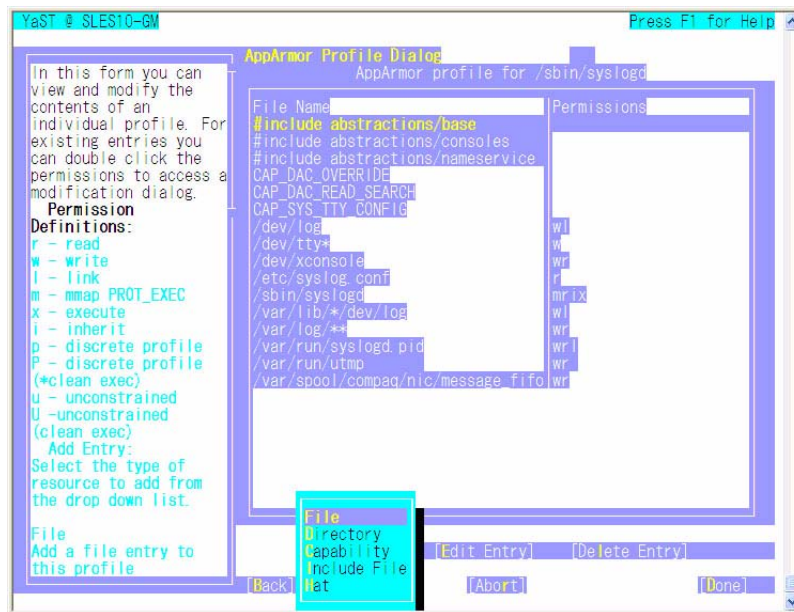


Figure 4.12 Entry addition and selection screen

- 5 Enter `"/var/opt/FJSVpsa/path/syslog_fifo"` at the "Enter or modify Filename" field and press the [Tab] key.

Next, in the "Permissions" field, use the [Space] key to mark the "Read" and "Write" checkboxes.

Press the [Tab] key to select OK and press the [Enter] key.

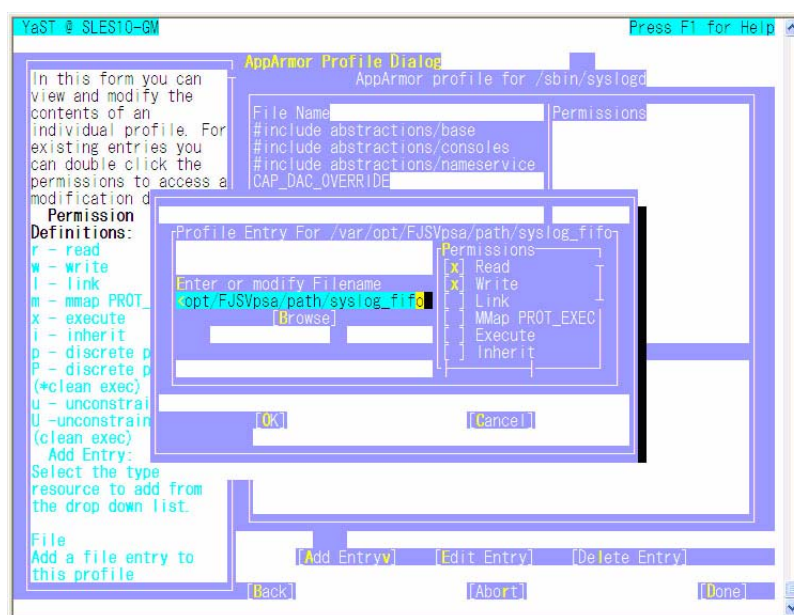


Figure 4.13 Adding the Profiles Entry screen

6 Confirm that the changes made in step 5 have been applied.

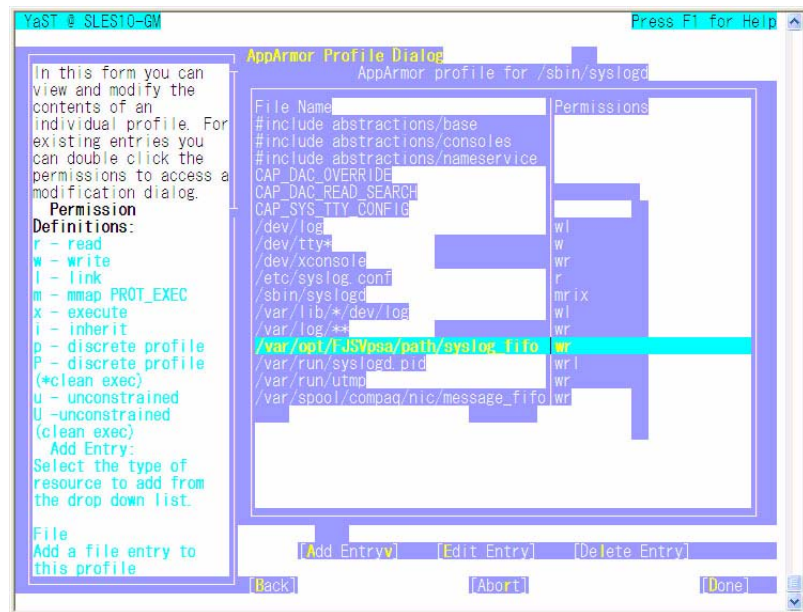


Figure 4.14 Entry list screen

- 7 Press the [Tab] key to select "Done" from the bottom menu. The [Save changes to the Profile] screen is then displayed. From the [Save changes to the Profile] screen, select [Yes] and press the [Enter] key.

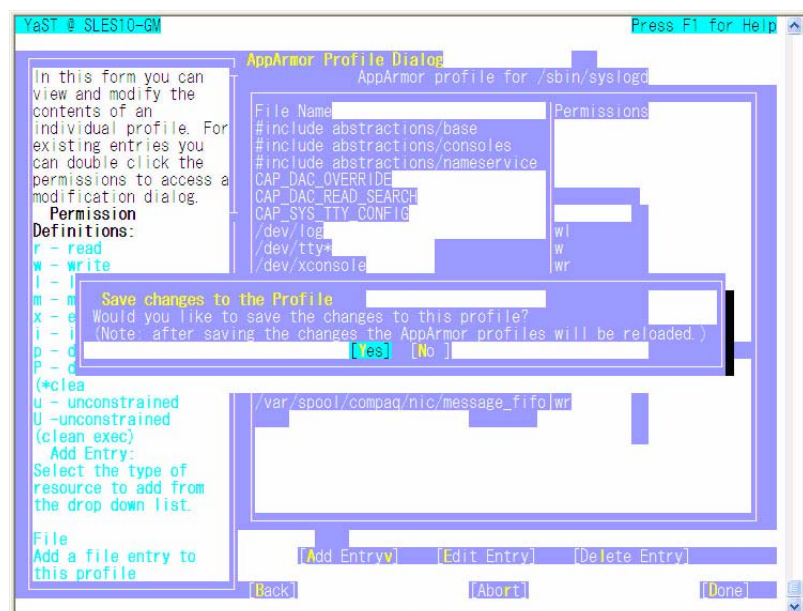


Figure 4.15 Saving the profiles screen

- 8 Press the [Tab] key to select "Quit" from the bottom menu and press the [Enter] key to quit YaST.
- 9 Restart AppArmor.

```
# /etc/init.d/boot.apparmor restart
Reloading AppArmor profiles                                done
```

- 10 Restart the syslog services.

```
# /etc/init.d/syslog restart
Shutting down syslog services                                done
Starting syslog services                                    done
```

4.3.2.3 Checking the required functions for PSA operation

The packages listed below are required for the PSA to run. Use the `rpm` command to check that each package is installed.

When using SUSE 9 Service Pack 2, check for the `km_ipmi` package.

- `net-snmp`
- `openssl`
- `gdb`
- `parted`
- `km_ipmi` (used only for SUSE 9 Service Pack 2)

Command syntax:

```
/bin/rpm -q <package name>
```

Example: Checking whether the `net-snmp` package is installed, and the output result when it is installed:

```
#!/bin/rpm -q net-snmp
net-snmp-5.1-80.16
```

If the package is not installed, install the OS from the installation CD by using the RPM package installation method. For details on how to install the IPMI driver (`km_ipmi`), see the *PRIMEQUEST Installation Support Tool User's Guide (SUSE)* (C122-E047EN).

4.3.2.4 SELinux function

By default, the SELinux function is disabled on the PRIMEQUEST-series machine after OS installation. Do not use the SELinux function.

4.3.3 PSA installation

Execute the following command to install the PSA package:

Command syntax:

```
/bin/rpm -ivh FJSVpsa-X.X.X-X.ia64.rpm
```

X.X.X-X is a PSA version.

4.3.4 Items automatically set during PSA installation

During PSA installation, the following modifications required for PSA operation are automatically put into effect:

- Addition of settings to syslog.conf
- Addition of settings to snmpd.conf
- snmptrapd.conf file setup.
- Disabling of salinfo_decode automatic startup setting (*1)
- Disabling of smartd automatic startup setting
- Addition of description to the services file (*2)

*1 These automatic startup settings are disabled because of conflicts with some PSA functions.

*2 Added port: Port numbers are not checked for duplication when contents are added to the fj-webgate (24450) services file. They may need to be changed.

4.3.5 Rebooting the partition

Reboot the partition after installing PSA.

```
/sbin/reboot
```

4.3.6 Settings after PSA installation

This section describes the settings to be made after PSA installation.

- [Checking the firewall function \(releasing ports\)](#) (→ 4.3.6.1)
- [Setting the destination of trap sending from the partition](#) (→ 4.3.6.2)
- [Setting the destinations of trap and e-mail sending via the MMB](#) (→ 4.3.6.3)
- [Other settings](#) (→ 4.3.6.4)

4.3.6.1 Checking the firewall function (releasing ports)

If the port has not been released during the firewall setting, release the ports required for PSA operation. Specifically, release the following ports for the management LAN interfaces that have been set:

- snmp port : udp / snmp or 161
- snmptrap port : udp / snmptrap or 162 (*1) (to the physical IP address of the MMB (both systems))
- web-mmb communication port : tcp / fj-webgate or 24450 (*2) (to the virtual IP address of the MMB)
- rmcp+ port : udp/7000 to 7100 (*1) (to the physical IP address of the MMB (both systems))
- localhost snmp port : udp/1025-65535
- psa-mmb communication port : tcp/MMB side 5000 (Note 3) (to the virtual IP address of the MMB)
icmp/icmp-type0, icmp-type8 (to the virtual IP address of the MMB)

*1 Release the port only when a PCL linkage is used.

Use the iptables command for checking the firewall setting.

*2 web-mmb communication port

*3 This is communication for the MMB 5000 port.

Because PSA operates as a client under this communication, the port number used by PSA is undefined. (Any number ranging from tcp/1025 to 65535 is selected for one port.)

Moreover, as indicated in the example below, no setting is required for port number 5000 while connection startup is enabled or while communication is enabled for an established connection with the port.

(Example) iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT
iptables -A INPUT -m state --state ESTABLISH -j ACCEPT

Command syntax:

```
/sbin/iptables -L
```

Use the iptables command or another command to release the port. For the usage, see command man.

Command syntax:

```
/usr/bin/man iptables
```

4.3.6.2 Setting the destination of trap sending from the partition

Notes:

- Make this setting only if required.
- This setting is required for linkage with operation management software.

When sending SNMP traps, you must set the trap send destination. Add the trap send destination to the snmpd.conf file.

- Editing snmpd.conf

```
# vi /etc/snmp/snmpd.conf

Add the following lines for the SNMP version to be used. The lines can be provided in any order.
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
trapsess SNMPCMD_ARGS HOST[:PORT] # SNMPv3 trap setting
```

The settings are detailed below:

- Setting SNMPv1/SNMPv2 traps

```
trapsink HOST [COMMUNITY [PORT]] # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]] # SNMPv2 trap setting
```

Define the host that receives the traps (to which traps are sent).

- With this setting made, a cold start trap is sent when snmpd is started. If SNMP trap sending is defined, a trap is also sent when authentication fails.
- Multiple destinations can be defined by specifying multiple pairs of the trapsink and trap2sink lines.

- If COMMUNITY is not specified, the character string previously specified by the trapcommunity directive is used.

The trapcommunity command sets the default community string used to send traps. When using trapcommunity to set the community string, specify the string before the pair of trapsink-trap2sink lines.

trapcommunity STRING	#COMMUNITY name setting
----------------------	-------------------------

- If PORT is not specified, the default SNMP trap port (162) is used.

Example: When you want to send traps with the community name "public" to port 162 of the manager with IP address 192.168.1.10.

trapsink 192.168.1.10 public 162	##SNMPv1 trap setting
trap2sink 192.168.1.10 public 162	##SNMPv2 trap setting

● SNMPv3 trap setting

trapsess SNMPCMD_ARGS HOST[:PORT]	#SNMPv3 trap setting
-----------------------------------	----------------------

Define the host that receives the traps (to which traps are sent). If PORT is not specified, the default SNMP trap port (162) is used.

The major options that can be specified for SNMPCMD_ARGS are as follows:

- v version : Specifies the SNMP version. Specify 3 for SNMPv3.
- e engineID : Specifies the value of oldEngineID in the /var/lib/net-snmp/snmpd.conf file in the trap sender.
- u secName : Specifies the SNMPv3 account. It must be the same as the setting in the manager.
- l secLevel : Specifies one of the following according to the security level of SNMPv3 messages:

Table 4.3 secLevel settings

Setting	Authentication	Encryption
noAuthNoPriv	No	No
authNoPriv	Yes	No
authPriv	Yes	Yes

- a authProtocol : Specifies MD5 or SHA as the protocol used to authenticate SNMPv3 messages. If SHA is to be used, a package must be created using openssl that is installed. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if authentication is not included.
- A authPassword : Specifies an authentication password (eight or more characters). The password must be the same as the setting in the manager. This option is valid when authentication is included in the security level specified by the -l option. It can be omitted if the authentication is not included.
- x privProtocol : Specifies the protocol used to encrypt SNMPv3 messages. Currently, only DES is supported as a privacy protocol. If encryption is included in the security level specified by the -l option, this option is valid; otherwise, it may be omitted.
- X privPassword : Specifies an encryption password (eight or more characters). The password must be the same as the setting in the manager. If encryption is included in the security level specified by the -l option, this option is valid; otherwise, it may be omitted.

Example: When you want to send SNMPv3 traps with the "PRIMEQUEST" account, with authentication and encryption enabled, to port 162 of the manager with IP address 192.168.1.10.

```
trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l authPriv -a
MD5 -A 00000000
-x DES -X 11111111 192.168.1.10:162      ##SNMPv3 trap setting
```

After setting the trap transfer destination, restart snmpd by executing the following command:

```
#/etc/rc.d/init.d/snmpd restart
```

After snmpd has been reactivated, activate PSA.

```
#!/sbin/service y30FJSVpsa stop
#!/sbin/service y30FJSVpsa start
```

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard net-snmp trap that would be used to restart snmpd. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that net-snmp standard traps can be received.

Restart snmpd by executing the following command on the trap transfer source machine:

```
# /etc/rc.d/init.d/snmpd restart
```

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard net-snmp trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 12:00:53 pq-server snmptrapd[2600]: 2005-08-17 12:00:53 pq-  
server.fujitsu.com [192.168.1.10](via 192.168.1.10) TRAP, SNMP v1, community  
public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start  
Trap (0) Uptime: 0:00:00.17
```

Note: If the operating system is SUSE™ Linux Enterprise Server 9 Service Pack2 and direct reporting of traps to the SNMP manager has been set, "0.0.0.0" is reported as the Agent Address value in the SNMP layer in reported trap data. Consequently, the SNMP manager cannot identify the IP address of the trap transfer source from the Agent Address value. However, the transfer source of a PSA expansion trap can be identified, since its trap data is accompanied by a host name. IP addresses are reported in the IP layer. To use a trap transfer source IP address for the purpose of identification, the "%b" option can be added to the initial parameters in snmptrapd, such as for reception of the IP address by the SNMP manager using snmptrapd. This method can output information including the trap transfer IP source address, so the transfer source can be identified. For details on the initial parameters in snmptrapd, see the man page for snmptrapd.

4.3.6.3 Setting the destinations of trap and e-mail sending via the MMB

Notes:

- Make this setting only if required.
- This setting is required for linkage with operation management software.

The destinations of trap and e-mail sending via the MMB can be set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.3.6.4 Other settings

Remarks: Make this setting only if required.

- Setting required when a replicated disk is used
You can build a new partition by using a disk copied from a partition in the same cabinet, such as disk copy. In this case, you need to manually change the EngineID of SNMPv3 used for the PSA internal communication.

You can change the EngineID with root authority as follows:

- 1 Use the `ps` command to check whether PSA is active.

Command syntax:

```
ps ax | grep psa
```

Example: PSA is active if the following processes under `/opt/FJSVpsa/bin/` are displayed.

```
# ps ax | grep psa
4562 ? S 0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/FJSVpsa/global/pmpsa.conf
4563 ? S 0:18 /opt/FJSVpsa/bin/loggetd -p /
4564 ? S 0:06 /opt/FJSVpsa/bin/sisp -p /
4565 ? S 0:00 /opt/FJSVpsa/bin/mmblm -p /
4566 ? S 0:01 /opt/FJSVpsa/bin/mmbs -p /
4567 ? S 0:02 /opt/FJSVpsa/bin/fs -p /
4568 ? S 0:00 /opt/FJSVpsa/bin/ciipmi -p /
4569 ? S 7:40 /opt/FJSVpsa/bin/cilog -p /
4570 ? S 8:47 /opt/FJSVpsa/bin/cios -p /
4578 ? S 0:00 /opt/FJSVpsa/bin/cisalchild 1 /
4819 ? Sl 0:00 /opt/FJSVpsa/bin/webgate -p /
21670 pts/5 S+ 0:00 grep psa
```

- 2 If PSA is active, use the following command to stop PSA.

Command syntax:

```
/etc/init.d/y30FJSVpsa stop
```

- 3 Enter the ps command to check whether snmpd is active.

Command syntax:

```
ps ax | grep snmpd
```

Example: snmpd is active if /usr/sbin/snmpd is displayed.

```
# ps ax | grep snmpd
32611 ? S 0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p /var/run/
snmpd -a
```

- 4 If snmpd is active, enter the following command to stop snmpd.

Command syntax:

```
/etc/init.d/snmpd stop
```

- 5 Change the value of oldEngineID defined in the /var/lib/net-snmp/snmpd.conf file.

Remarks: You can change to any value in up to 34 hexadecimal digits, provided that it is unique throughout the partitions in the same cabinet.

Example: To change the value of oldEngineID to 0x19760523

```
#vi /var/lib/net-snmp/snmpd.conf
oldEngineID 0x19760523
```

- 6 Enter the following command to start snmpd.

Command syntax:

```
/etc/init.d/snmpd start
```

- 7 Change the current directory to /opt/FJSVpsa/sh/ to regenerate the snmpv3 password used for the PSA internal communication.

Command syntax:

```
cd /opt/FJSVpsa/sh/
```

- 8 Execute snmpsetup.sh in the above directory.
Executing this command automatically generates the snmpv3 password used for the PSA internal communication.

Command syntax:

```
./snmpsetup.sh install
```

- 9 Start PSA.

Command syntax:

```
/etc/init.d/y30FJSVpsa start
```

4.3.7 PSA update installation

Using the following commands in the order shown, stop the PSA service, and perform update installation for the PSA package.

Command syntax:

Update from PSA-1.2.X-X or late

```
/etc/init.d/y30FJSVpsa stop  
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm  
/etc/init.d/y30FJSVpsa start
```

Update from PSA-1.1.X-X

```
/etc/init.d/y30FJSVpsa stop  
/bin/rpm -Uvh FJSVpsa-X.X.X-X.ia64.rpm  
/etc/init.d/y10FJSVpsa start  
/etc/init.d/y30FJSVpsa start
```

* X.X.X-X indicates the PSA version.

4.3.8 PSA uninstallation

Using the following commands in the order shown, stop the PSA service, and uninstall the PSA package.

Command syntax:

```
/etc/init.d/y30FJSVpsa stop  
/bin/rpm -e FJSVpsa
```

4.4 Manual PSA Installation (Windows Server 2003) (PRIMEQUEST 580A/540A/580/540/480/440)

This section describes the procedure for installing PSA under the Windows Server 2003 operating system. Before starting the installation procedure, log in to the system with the administrator privilege.

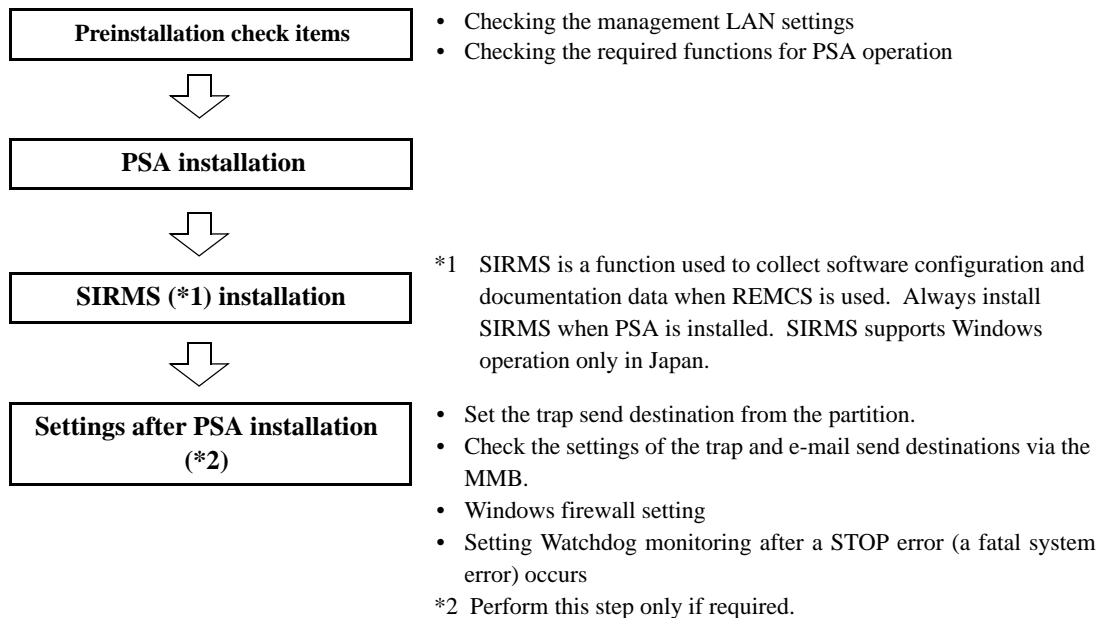
Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog partition monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of CPU, DIMM, and chip set recoverable errors
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- Partition information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.

Note: If the PEXU has been mounted, use PSA-1.10 or later.

4.4.1 Installation Workflow

The figure below shows the workflow for PSA installation.



Remarks: If you perform batch installation using the batch installer included in the High-Reliability Tools, this PSA and SIRMS installation work is unnecessary. However, after such a batch installation, the procedures described in the above "Preinstallation check items" and "Settings after PSA installation" sections must be followed.

Notes:

- In the first attempt to open the PSA window from the Web-UI after the system restart following PSA installation, the error message "E_33077 PSA is Not Active. (01:0000)" may be displayed. This may occur because PSA requires a certain amount of time to acquire sensor information for the system. Wait a few minutes, then try to open the window again.
- After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.
- Do not stop the Windows service, print spooler service. The operating system information collection function uses the Windows Management Instrumentation (WMI) to collect the configuration information. However, when the print spooler service is stopped, an error is reported to WMI and configuration information is not collected correctly.

4.4.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.4.2.1)
- [Verifying the services required for PSA operation](#) (→ 4.4.2.2)

4.4.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: If you perform batch installation using the batch installer included in the High-Reliability Tools, configure the management LAN after the batch installation is completed.

(1) Verifying the NIC for the management LAN

In Device Manager, display the properties of the network adapters (Intel PRO/100 VE Network Connection and Intel PRO/100 M Network Connection) assigned to the management LAN, and check the settings in [Location] on the [General] tab.

Connect the network adapters for the management LAN to MMB#0 and MMB#1 as follows:

- MMB#0: PCI Bus 1, Device 8, Function 0
- MMB#1: PCI Bus 1, Device 0, Function 0

Use the teaming function of Intel PROSet to configure the above network adapters for duplicated communication with the management LAN.

For Intel PROSet teaming, specify the IP addresses of the devices for the management LAN that are configured for duplicated communication.

(2) Configuring the two network adapters for the management LAN so that the adapters are duplicated

Use the teaming function of Intel PROSet to configure the network adapter for the management LAN to guarantee management LAN operation for duplicated communication.

Install Intel PROSet beforehand.

Note:

- Change the VLAN setting of the MMB management LAN hub to "VLAN Mode." (For details, see 2.2.4.5, "Setting a VLAN in a management LAN hub" in the *PRIMEQUEST 500A/500/400 Installation Manual*.)
- The Spanning Tree Protocol (STP) function of the switch connected to the user port (management LAN) of the MMB must be disabled.
- To make settings through a connection to a remote desktop, a console session connection must be established. Establish this type of connection according to the following procedure:

- 1) Select [Start], and click [Run]. The [Run] dialog box opens.
- 2) Enter "mstsc /v:<servername/ip address> /console" in the [Open] input box, and click the [OK] button.

For the connection to the server, specify an actual server name and IP address in <servername/ip address>. (A virtual IP address in the cluster cannot be specified.)

* For details on the options for mstsc, you can enter "mstsc /?".

- 1 Click [Control Panel] → [Administrative Tools] → [Computer Management] → [Device Manager].

- 2 Open [Network Adapter], and click [Inter(R) PRO/100 VE Network Connection] to select it.

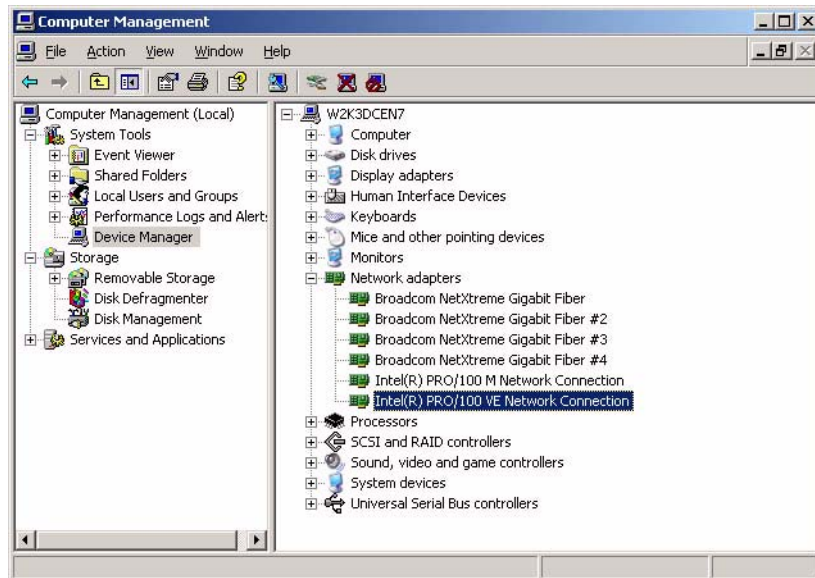


Figure 4.16 [Computer Management] window

- 3 The [Intel(R) PRO/100 VE Network Connection Properties] dialog box opens. Click the [Teaming] tab, select [Team with other adapters], and click the [New Team] button.

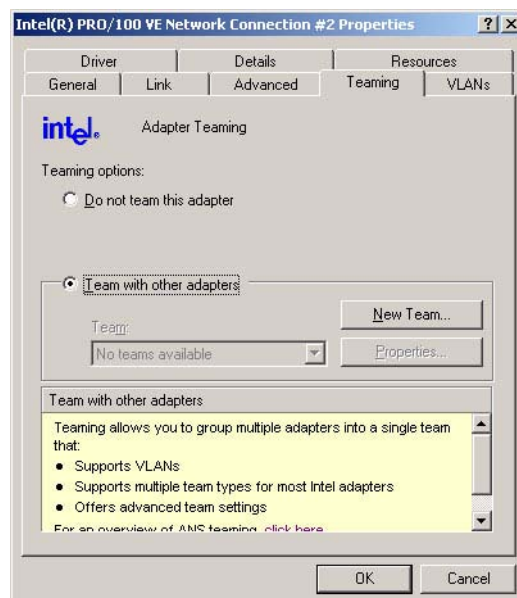


Figure 4.17 [Teaming] tab

- 4 The [New Team Wizard] window is displayed. Enter a team name (the default team name is Team #0), and click the [Next] button.



Figure 4.18 [New Team Wizard] window

- 5 A list of network adapters is displayed for teaming. Select [Intel(R) PRO/100 VE Network Connection] and [Intel(R) Pro/100 M Network Connection] check boxes, and click the [Next] button.

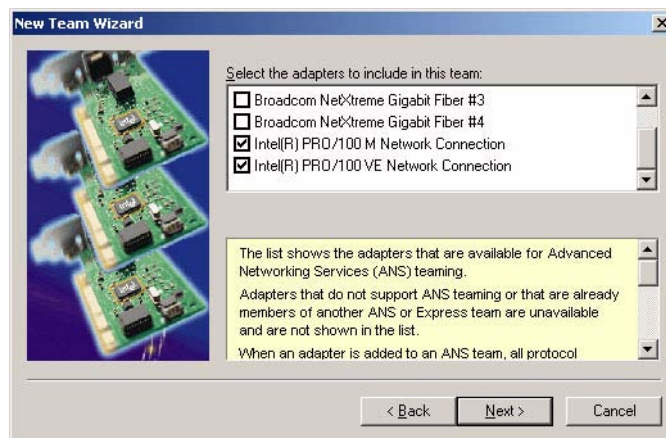


Figure 4.19 List of network adapters

- 6 Select [Adapter Fault Tolerance] from the mode list, and click the [Next] button.

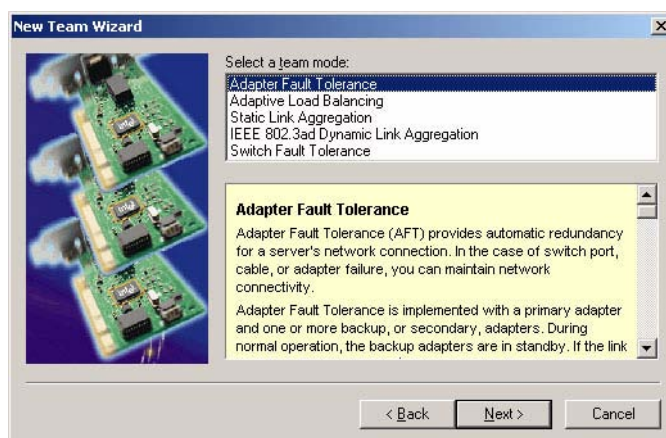


Figure 4.20 List of team mode

- 7 The following window is displayed. Teaming configuration processing starts when you click the [Finish] button.

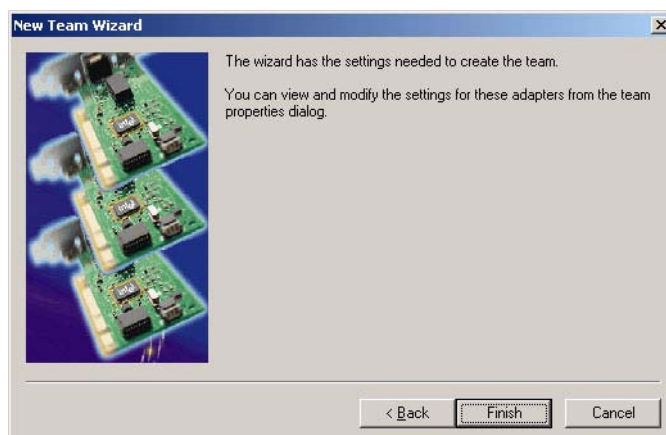


Figure 4.21 Selection Completed window

- 8 When the configuration processing for Teaming is finished, a Teaming device is created, and Team properties are displayed.
Click the [Settings] tab, and confirm that the displayed adapter information is correct. If the information is correct, click the [OK] button to exit. Otherwise, click the [Remove Team] button to delete the Teaming device, and start again from step 2 of this procedure.

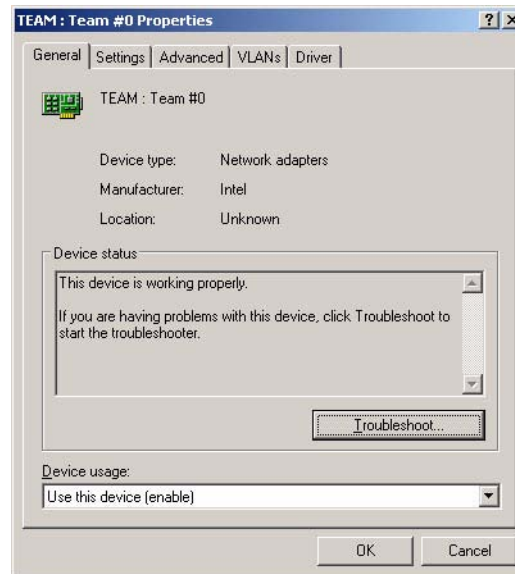


Figure 4.22 Team Number 0 Properties window

- 9 The [Intel(R) PRO/100 VE Network Connection Properties] dialog box opens again.
Click the [OK] button to finish processing, and close [Computer Management].
- 10 Click [Control Panel] and [Network Connections].
A list of networks is displayed.
- 11 Select the network whose device name is the specified Team name (e.g., Team #0), and select [Properties] from the right-click menu.
- 12 Select [Internet Protocol (TCP/IP)], click the [Properties] button, and specify the IP address, subnet mask, default gateway, and other parameters in the [Internet Protocol (TCP/IP) Properties] dialog box.

- 13 Click the [Configure] button to display the Team properties.

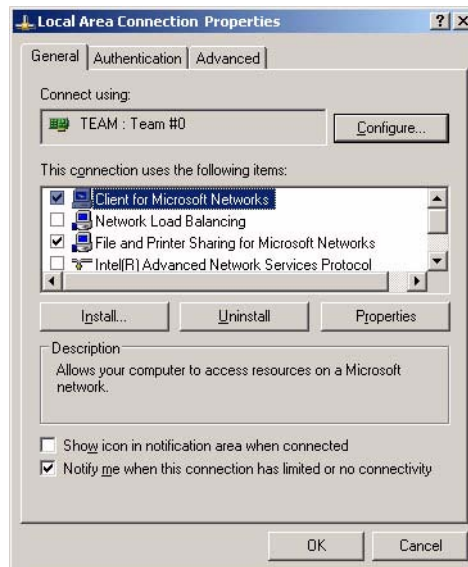


Figure 4.23 [Local Area Network Connection Properties] dialog box

- 14 Click the [Advanced] tab, select [Probe] in [Settings], select [Enable] in [Value], and click the [OK] button.

As a result, the adapter activates its link monitoring function, thereby setting management LAN duplication.

Reboot to make the Teaming settings effective.

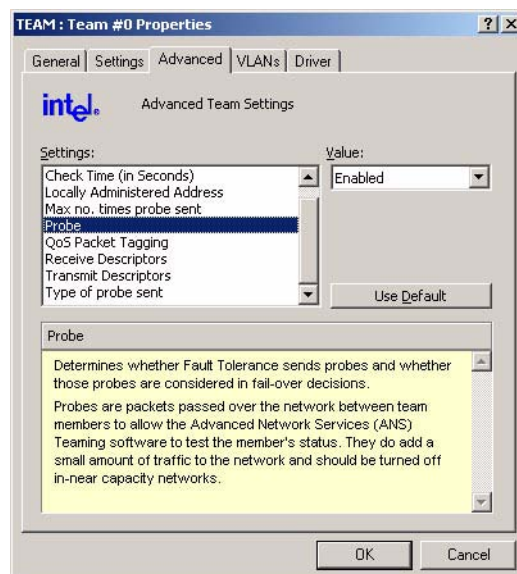


Figure 4.24 [Advanced] tab

4.4.2.2 Verifying the services required for PSA operation

The SNMP service is required for running PSA. Confirm that the SNMP service is installed by following the procedure below.

Remarks: This operation requires the Windows installation DVD.

- 1 Select [Control Panel] → [Add/Remove Programs] → [Add/Remove Windows Components].
The Windows Component Wizard is started.
- 2 Select [Management and Monitoring Tools], and click [Details].
The [Management and Monitoring Tools] window is displayed.
- 3 Confirm that the [On] check box of [Simple Network Management Protocol (SNMP)] is selected, and click [OK].

The Windows Components Wizard is displayed again.

Note: If the check box is not checked, the SNMP service is not installed. Make sure to select the appropriate check box to install the SNMP service.
In the [Windows Component Wizard] window, click the [Next] button, and install the service by following instructions from the wizard.

4.4.3 Installing PSA

Prepare the "PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003" (C122-E024) that are supplied with the main unit.

- 1 Execute Tools\General\PSA\fjpsaxxxx.exe. (xxxx: version number).
The following window is displayed while the installation procedure is being prepared.

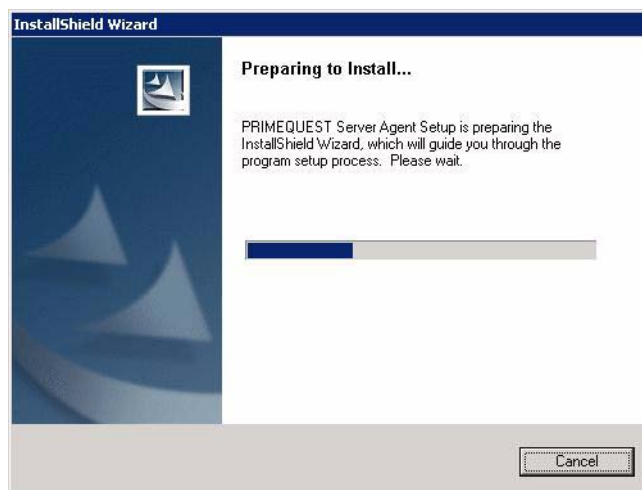


Figure 4.25 Installation preparation window

- 2 When the following window is displayed, indicating that the system is ready for installation, click [Next] to perform installation.

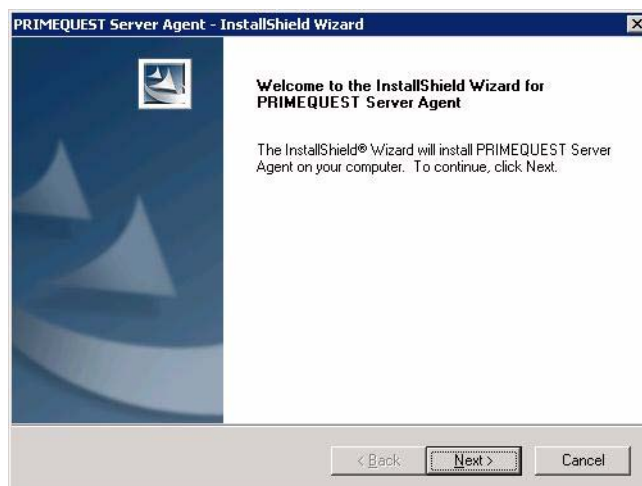


Figure 4.26 Setup window

- 3 Specify the installation destination, and click [Next].
PSA is installed in the Program Files\Fujitsu folder by default. To change the installation destination, click [Browse] and specify the desired folder.

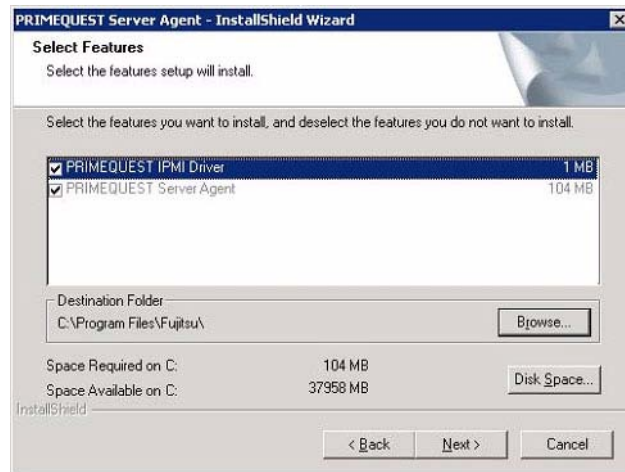


Figure 4.27 [Select Features] window

- 4 When installation is completed, the following completion window is displayed. Click [Finish].

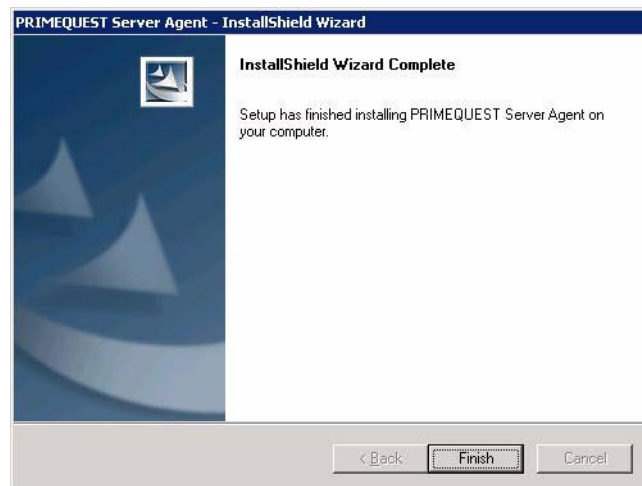


Figure 4.28 Installation completion window

- 5 If a reboot is necessary, a message is displayed to ask whether you want to restart the PC immediately. Check whether the PC can be restarted. If it can, select the restart option, and click the [Finish] button.

4.4.4 Items automatically set during PSA installation

During PSA installation, the specified values of various parameters for PSA operation are automatically set:

- 1 Service settings
 - PRIMEQUEST Server Agent
 - PRIMEQUEST PEM Command Service
 - PRIMEQUEST PSA Environment Control Service
- 2 Environment variable settings
 - PATH variable
Values for use by PSA are added to the existing PATH variable.
 - FJSVpsa_INSTALLPATH variable
This is a new variable that is added.
- 3 Port setting
The parameter is set to ensure that PSA uses the TCP:24450 port.
- 4 SNMP security setting
Make SNMP Service security settings because PSA must receive SNMP packets from the MMB.
The subsequent processes vary as follows depending on the parameter selected on the [Security] tab in the [Properties] dialog box of [SNMP Service] during PSA installation.
 - If [Accept SNMP packets from any host] was selected:
Make no SNMP security setting.
 - If [Accept SNMP packets from these hosts] was selected:
Make the SNMP security setting unless the IP address of the MMB and localhost parameter are specified.

Note: To change the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts] after PSA installation, or to change the IP address of the MMB, execute the SNMP security setting command (setsnmpsec). For details on this command, see the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

5 Window Management Instrumentation (WMI) setting

PSA collects information on PCI cards and SCSI devices by using WMI, which is installed as standard with Windows.

If the amount of memory and the number of internal handles that WMI uses to collect this information are insufficient because there are many LUNs, such as in RAIDs, change settings to the following values:

- Maximum amount of memory used: 536,870,912 bytes
- Maximum number of internal handles: 65,536

6 Task scheduler settings

To monitor for errors involving the power supply of the expansion file unit and FANs, make the following task scheduler settings:

Task name: File Unit Status Check

Activation interval: 5 minutes

The configuration information is collected when the PSA is started. Error monitoring is then performed based on the collected information until the next time the PSA is started. If an expansion file unit is not connected, configuration information is collected according to the schedule, but the process is completed immediately without error monitoring performed. Therefore, no additional workload is imposed on the system.

4.4.5 Settings after PSA installation

This section describes the settings to be made after PSA installation:

- [Setting the destination of trap sending from the partition](#) (→ 4.4.5.1)
- [Setting the destinations of trap and e-mail sending via the MMB](#) (→ 4.4.5.2)
- [Windows firewall setting](#) (→ 4.4.5.3)
- [Setting Watchdog monitoring after a STOP error \(a fatal system error\) occurs](#) (→ 4.4.5.4)

Notes:

- Do not enable Visual Notification in the Dr. Watson options.
Otherwise, if a PSA error occurs and a message box opens, PSA cannot be restarted until the message box is closed.
- In the properties for the system log of the event viewer or the application log, do not change the operation that is performed when the maximum log size is reached to "Do not overwrite events (clear log manually)." Otherwise, any error that occurs when the maximum log size is reached is not output to the log, so PSA cannot detect the error.

4.4.5.1 Setting the destination of trap sending from the partition

Note:

- SNMP v.3 is not supported in Windows.
- Perform the tasks for this setting only if the setting is required.
- If partitions are managed by operation management software, this setting is required.

- 1 Click [Control Panel] → [Administrative Tools].
- 2 Click [Computer Management].
- 3 In the left tree, click [Services and Applications] → [Services].
- 4 In the right pane, click [SNMP Service].
The [SNMP Service] dialog box appears.
- 5 Click the [Trap] tab.
- 6 Enter the desired community name in the [Community Name] field, and click [Add to List].
- 7 Click [Add] in the [Trap Send Destination] area.
- 8 Enter the host name or IP address of the server that will receive traps (for notification), and click [Add].

- 9 Click [OK].
- 10 Click the [Action] menu → [Restart] to restart the SNMP service.

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard SNMP Service trap that is normally used during the SNMP Service restart in step 10. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that standard SNMP Service traps can be received.

On the trap transfer source machine, restart SNMP Service by performing step 10.

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard SNMP Service trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03
pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP
v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap
(0) Uptime: 0:00:00.00
```

4.4.5.2 Setting the destinations of trap and e-mail sending via the MMB

Note:

- Perform the tasks for this setting only if the setting is required.
- If partitions are managed by operation management software, this setting is required.

Destinations for trap and e-mail sending via the MMB are the addresses set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.4.5.3 Windows firewall setting

To run your system with the Windows firewall enabled, specify [Exceptions] for the following ports to guarantee that data can be sent to and received from the MMB through the following ports:

- TCP port used by PSA: 24450 port
 - TCP port used for SNMP: 161 port
- 1 Click [Control Panel] → [Windows Firewall].
The [Windows Firewall] window opens.
 - 2 Click the [Exceptions] tab, and click the [Add Port] button.
The [Add Port] dialog box opens.
 - 3 Enter the port number used by PSA, and click the [OK] button.

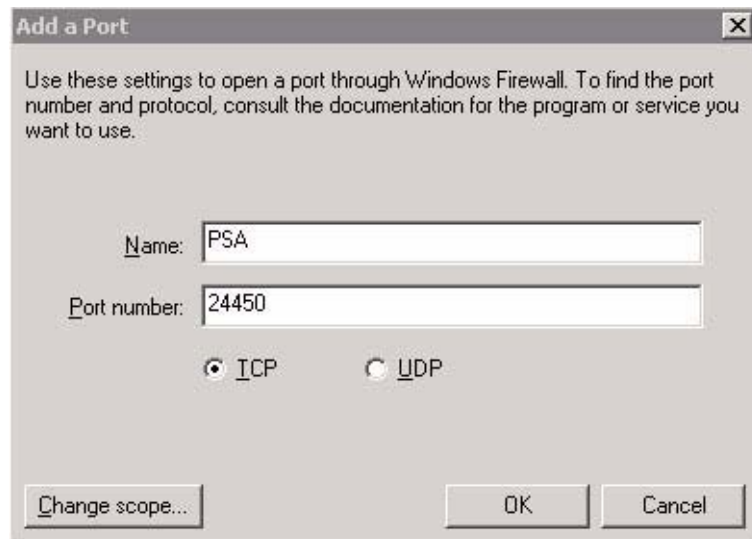


Figure 4.29 [Add a Port] dialog box

- 4 Click the [Add Port] button in the [Windows Firewall] window again.
The [Add Port] dialog box opens.

- 5 Enter the port number used by SNMP, and click the [OK] button.

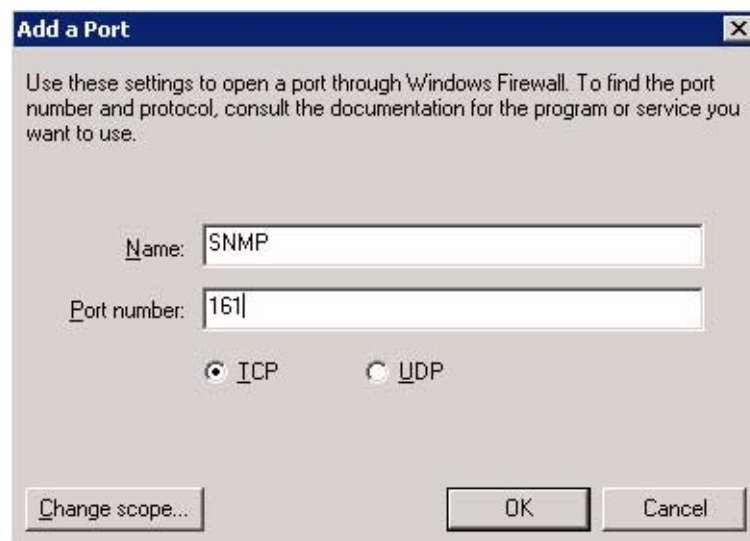


Figure 4.30 [Add a Port] dialog box

- 6 In the [Windows Firewall] window, click the [OK] button, and this ends the setting procedure.

4.4.5.4 Setting Watchdog monitoring after a STOP error (a fatal system error) occurs

If a STOP error (a fatal system error) occurs in the system, the results are as follows:

- "Panic" is displayed for "System Progress" of the relevant partition in [Partition]-[Power Control] of the MMB Web-UI.
- A memory dump is collected in the system.

In such cases, to prevent the system from freezing or otherwise becoming non-responsive, monitoring using the Watchdog timer can be set.

When the specified time has elapsed, the MMB executes a Hard Reset, and the OS is rebooted.

Setting procedure

- 1 Open the following file:
[PSA installation folder] \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Example: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf)
- 2 Specify a key value as shown below. The default is 0.
Section: [WATCHDOG]
Key: [TIMER]
Set value (unit: seconds) 0 (Watchdog timer not used)
1 to 6000 (Watchdog timer monitoring time)
Remarks: For the set value, measure the time required for memory dump in the applicable partition and determine the appropriate value. If the required time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog timer not used).
If the set value is shorter than the time required for memory dump processing, the Watchdog timer expires, resulting in execution of a Hard Reset, with the result that the memory dump cannot be collected correctly.

4.4.6 PSA update installation

This section describes the PSA update installation procedure.

Note: If the version of the fix program to be installed is the same as that of the installed PSA, a confirmation dialog box appears. Clicking the [OK] button in the dialog box uninstalls and then reinstalls the PSA.

Remarks: For the procedure for obtaining fix programs, ask your Fujitsu certified engineer or the support center.

(1) Minor update installation

- 1 Save the fix program (fjpsaxxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.



Figure 4.31 Installation preparation window

- 3 When the following window is displayed to indicate that the system is ready for installation, click the [Next] button to perform installation. Program updating is started.

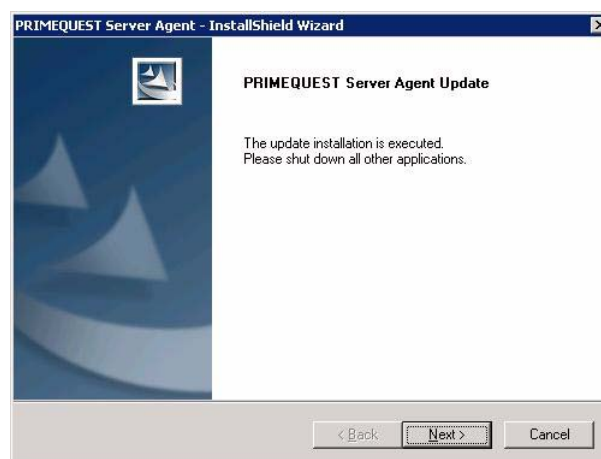


Figure 4.32 Update installation window

- 4 Click the [Finish] button to finish processing.

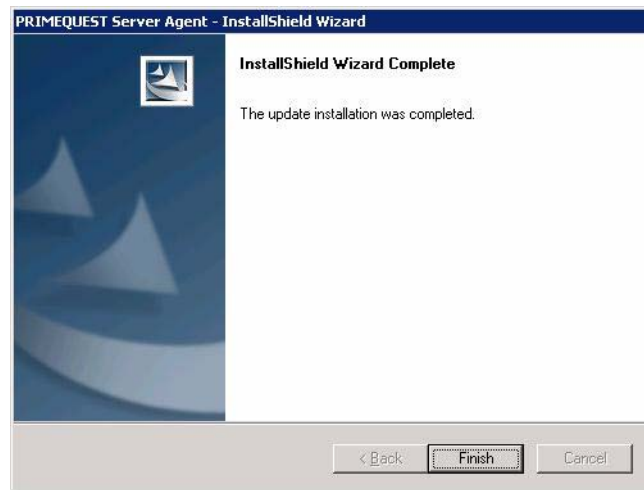


Figure 4.33 Update completion window

- 5 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

(2) Major update installation

- 1 Save the fix program (fjpsaxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.

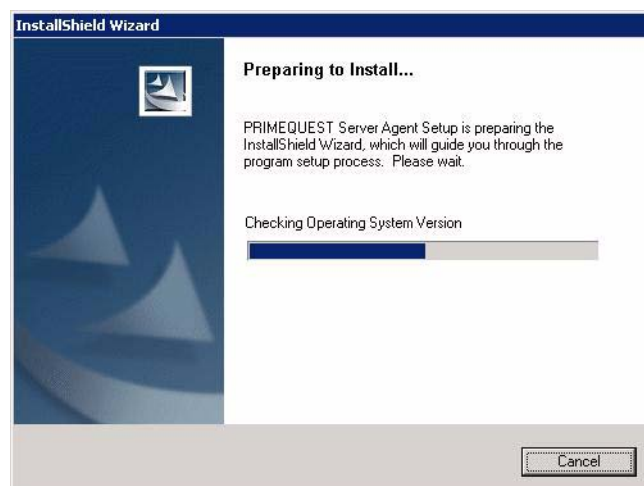


Figure 4.34 Installation preparation window

- 3 When a confirmation message is displayed, click the [OK] button. Uninstallation is started.

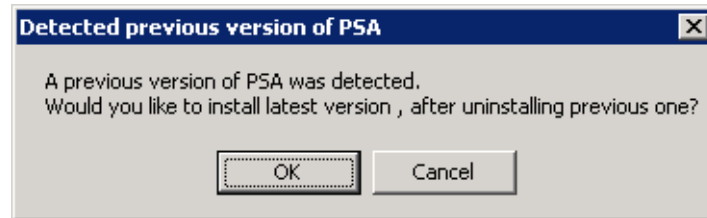


Figure 4.35 [Detected previous version of PSA] window

- 4 When uninstallation is completed, installation of the new version is started.
For the installation procedure, see steps 3 to 5 in Section [4.4.3, "Installing PSA."](#)

4.4.7 PSA uninstallation

This section describes the procedure for uninstalling PSA.

- 1 Click [Control Panel] → [Add/Remove Programs].
- 2 Select [PRIMEQUEST Server Agent] from [Currently Installed Programs], and click [Change/Delete].
- 3 A deletion confirmation message appears. Click [OK] to start uninstallation.

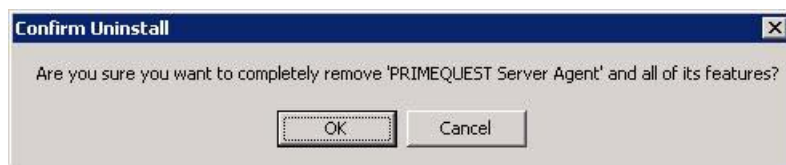


Figure 4.36 Confirmation message window

- 4 When uninstallation is completed, a maintenance completion window is displayed. Click [Finish].

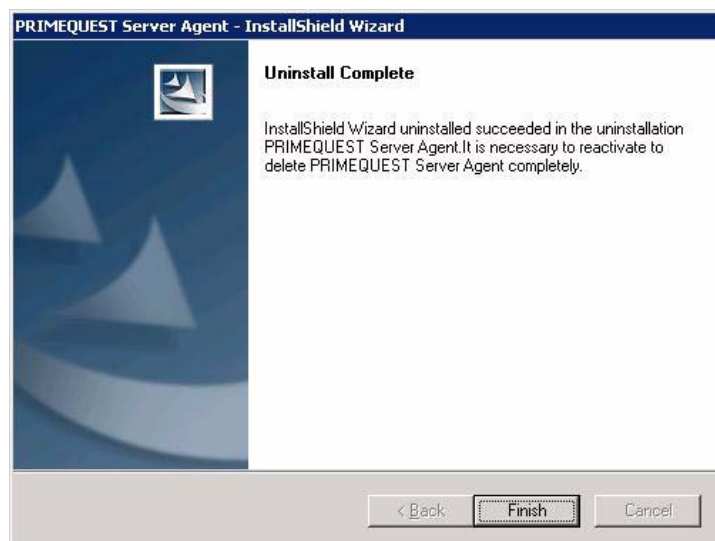


Figure 4.37 Maintenance completion window

- 5 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

4.5 Manual PSA Installation (Windows Server 2003) (PRIMEQUEST 520A/520/420)

This section describes the procedure for installing PSA under the Windows Server 2003 operating system. Before starting the installation procedure, log in to the system with the administrator privilege.

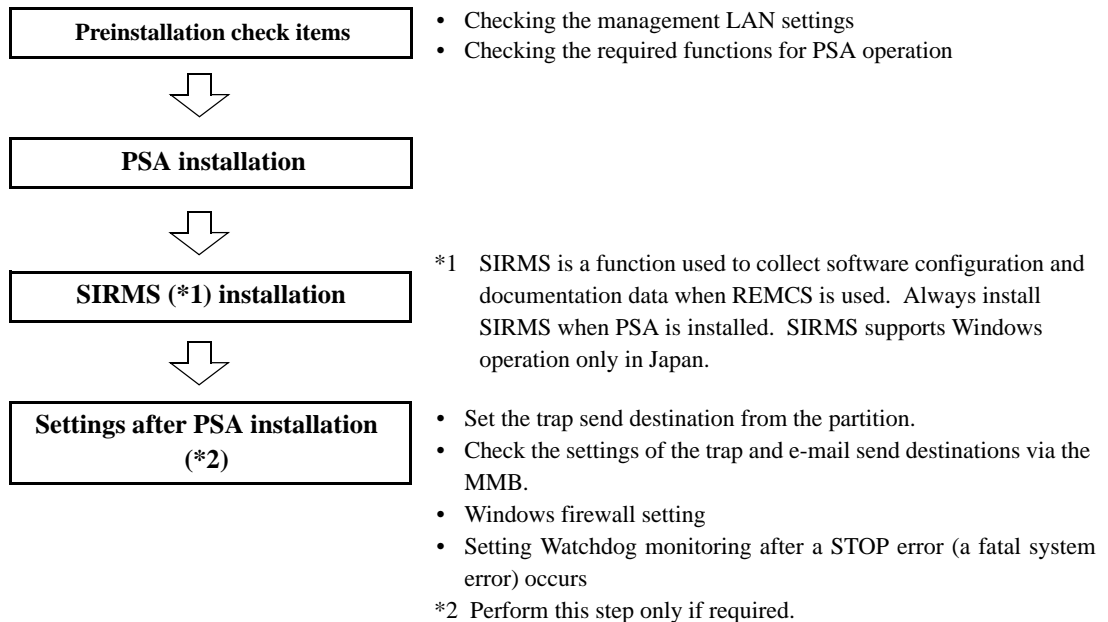
Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog system monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of CPU, DIMM, and chip set recoverable errors
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- OS information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.

Note: If the PEXU has been mounted, use PSA-1.10 or later.

4.5.1 Installation Workflow

The figure below shows the workflow for PSA installation.



Remarks: If you perform batch installation using the batch installer included in the High-Reliability Tools, this PSA and SIRMS installation work is unnecessary. However, after such a batch installation, the procedures described in the above "Preinstallation check items" and "Settings after PSA installation" sections must be followed.

Notes:

- In the first attempt to open the PSA window from the Web-UI after the system restart following PSA installation, the error message "E_33077 PSA is Not Active. (01:0000)" may be displayed. This may occur because PSA requires a certain amount of time to acquire sensor information for the system. Wait a few minutes, then try to open the window again.
- After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.
- Do not stop the Windows service, print spooler service. The operating system information collection function uses the Windows Management Instrumentation (WMI) to collect the configuration information. However, when the print spooler service is stopped, an error is reported to WMI and configuration information is not collected correctly.

4.5.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.5.2.1)
- [Verifying the services required for PSA operation](#) (→ 4.5.2.2)

4.5.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: If you perform batch installation using the batch installer included in the High-Reliability Tools, configure the management LAN after the batch installation is completed.

(1) Verifying the NIC for the management LAN

In Device Manager, display the properties of the network adapters (Intel PRO/100 VE Network Connection) assigned to the management LAN, and check the settings in [Location] on the [General] tab.

Connect the network adapter for the management LAN to MMB as follows:

- MMB: PCI Bus 1, Device 8, Function 0

(2) Setting the network adapter for the management LAN

- 1 Click [Control Panel] and [Network Connections].
A list of networks is displayed.
- 2 Select the network whose device name is the specified Team name and select [Properties] from the right-click menu.
- 3 Select [Internet Protocol (TCP/IP)], click the [Properties] button, and specify the IP address, subnet mask, default gateway, and other parameters in the [Properties] dialog box of [Internet Protocol (TCP/IP)].

4.5.2.2 Verifying the services required for PSA operation

The SNMP service is required for running PSA. Confirm that the SNMP service is installed by following the procedure below.

Remarks: This operation requires the Windows installation DVD.

- 1 Select [Control Panel] → [Add/Remove Programs] → [Add/Remove Windows Components].

The Windows Component Wizard is started.

- 2 Select [Management and Monitoring Tools], and click [Details].

The [Management and Monitoring Tools] window is displayed.

- 3 Confirm that the [On] check box of [Simple Network Management Protocol (SNMP)] is selected, and click [OK].

The Windows Components Wizard is displayed again.

Note: If the check box is not checked, the SNMP service is not installed. Make sure to select the appropriate check box to install the SNMP service.

In the [Windows Component Wizard] window, click the [Next] button, and install the service by following instructions from the wizard.

4.5.3 Installing PSA

Prepare the "PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2003" (C122-E024) that are supplied with the main unit.

- 1 Execute Tools\General\PSA\fjpsaxxxx.exe. (xxxx: version number).
The following window is displayed while the installation procedure is being prepared.

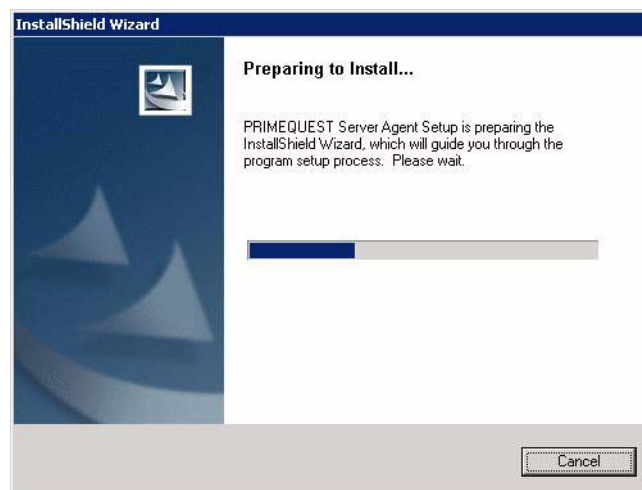


Figure 4.38 Installation preparation window

- 2 When the following window is displayed, indicating that the system is ready for installation, click [Next] to perform installation.



Figure 4.39 Installation window

- 3 Specify the installation destination, and click [Next].
PSA is installed in the Program Files\Fujitsu folder by default. To change the installation destination, click [Browse] and specify the desired folder.

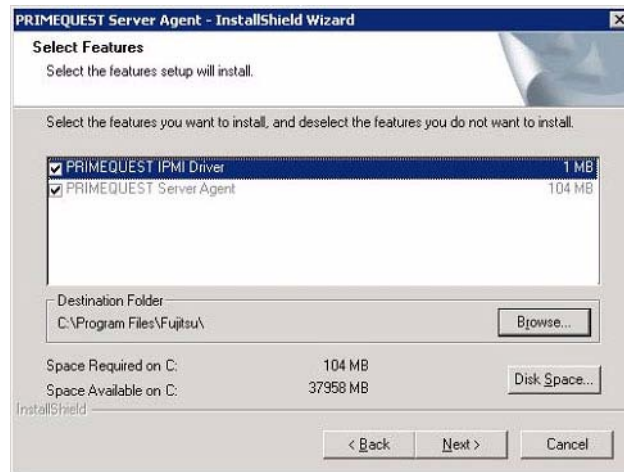


Figure 4.40 [Select Features] window

- 4 When installation is completed, the following completion window is displayed. Click [Finish].

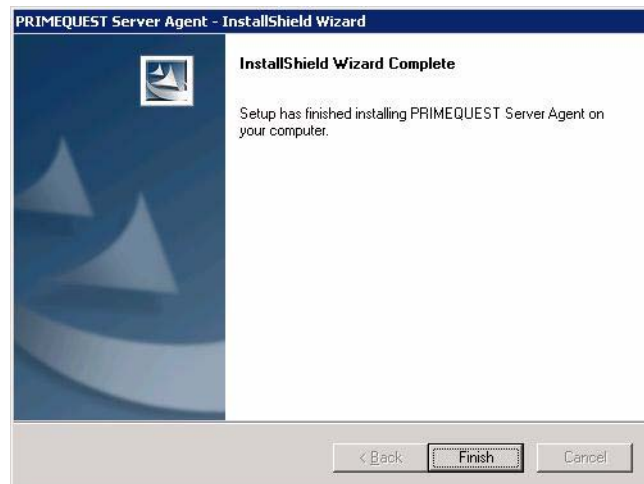


Figure 4.41 Setup completion window

- 5 If a reboot is necessary, a message is displayed to ask whether you want to restart the PC immediately. Check whether the PC can be restarted. If it can, select the restart option, and click the [Finish] button.

4.5.4 Items automatically set during PSA installation

During PSA installation, the specified values of various parameters for PSA operation are automatically set:

- 1 Service settings
 - PRIMEQUEST Server Agent
 - PRIMEQUEST PEM Command Service
 - PRIMEQUEST PSA Environment Control Service
- 2 Environment variable settings
 - PATH variable
Values for use by PSA are added to the existing PATH variable.
 - FJSVpsa_INSTALLPATH variable
This is a new variable that is added.
- 3 Port setting
The parameter is set to ensure that PSA uses the TCP:24450 port.
- 4 SNMP security setting
Make SNMP Service security settings because PSA must receive SNMP packets from the MMB.
The subsequent processes vary as follows depending on the parameter selected on the [Security] tab in the [Properties] dialog box of [SNMP Service] during PSA installation.
 - If [Accept SNMP packets from any host] was selected:
Make no SNMP security setting.
 - If [Accept SNMP packets from these hosts] was selected:
Make the SNMP security setting unless the IP address of the MMB and localhost parameter are specified.

Note: To change the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts] after PSA installation, or to change the IP address of the MMB, execute the SNMP security setting command (setsnmpsec). For details on this command, see the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

5 Window Management Instrumentation (WMI) setting

PSA collects information on PCI cards and SCSI devices by using WMI, which is installed as standard with Windows.

If the amount of memory and the number of internal handles that WMI uses to collect this information are insufficient because there are many LUNs, such as in RAIDs, change settings to the following values:

- Maximum amount of memory used: 536,870,912 bytes
- Maximum number of internal handles: 65,536

6 Task scheduler settings

To monitor for errors involving the power supply of the expansion file unit and FANs, make the following task scheduler settings:

Task name: File Unit Status Check

Activation interval: 5 minutes

The configuration information is collected when the PSA is started. Error monitoring is then performed based on the collected information until the next time the PSA is started. If an expansion file unit is not connected, configuration information is collected according to the schedule, but the process is completed immediately without error monitoring performed. Therefore, no additional workload is imposed on the system.

4.5.5 Settings after PSA installation

This section describes the settings to be made after PSA installation:

- [Setting the destination of trap sending from the partition \(→ 4.5.5.1\)](#)
- [Setting the destinations of trap and e-mail sending via the MMB \(→ 4.5.5.2\)](#)
- [Windows firewall setting \(→ 4.5.5.3\)](#)
- [Setting Watchdog monitoring after a STOP error \(a fatal system error\) occurs \(→ 4.5.5.4\)](#)

Notes:

- Do not enable Visual Notification in the Dr. Watson options.
Otherwise, if a PSA error occurs and a message box opens, PSA cannot be restarted until the message box is closed.
- In the properties for the system log of the event viewer or the application log, do not change the operation that is performed when the maximum log size is reached to "Do not overwrite events (clear log manually)." Otherwise, any error that occurs when the maximum log size is reached is not output to the log, so PSA cannot detect the error.

4.5.5.1 Setting the destination of trap sending from the partition

Note:

- SNMP v.3 is not supported in Windows.
- Perform the tasks for this setting only if the setting is required.
- This setting is required for linkage with operation management software.

- 1 Click [Control Panel] → [Administrative Tools].
- 2 Click [Computer Management].
- 3 In the left tree, click [Services and Applications] → [Services].
- 4 In the right pane, click [SNMP Service].
The [SNMP Service] dialog box appears.
- 5 Click the [Trap] tab.
- 6 Enter the desired community name in the [Community Name] field, and click [Add to List].
- 7 Click [Add] in the [Trap Send Destination] area.
- 8 Enter the host name or IP address of the server that will receive traps (for notification), and click [Add].

- 9 Click [OK].
- 10 Click the [Action] menu → [Restart] to restart the SNMP service.

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard SNMP Service trap that is normally used during the SNMP Service restart in step 10. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that standard SNMP Service traps can be received.

On the trap transfer source machine, restart SNMP Service by performing step 10.

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard SNMP Service trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03
pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP
v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap
(0) Uptime: 0:00:00.00
```

4.5.5.2 Setting the destinations of trap and e-mail sending via the MMB

Note:

- Perform the tasks for this setting only if the setting is required.
- This setting is required for linkage with operation management software.

Destinations for trap and e-mail sending via the MMB are the addresses set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.5.5.3 Windows firewall setting

To run your system with the Windows firewall enabled, specify [Exceptions] for the following ports to guarantee that data can be sent to and received from the MMB through the following ports:

- TCP port used by PSA: 24450 port
 - UDP port used for SNMP: 161 port
- 1 Click [Control Panel] → [Windows Firewall].
The [Windows Firewall] window opens.
 - 2 Click the [Exceptions] tab, and click the [Add Port] button.
The [Add Port] dialog box opens.
 - 3 Enter the port number used by PSA, and click the [OK] button.

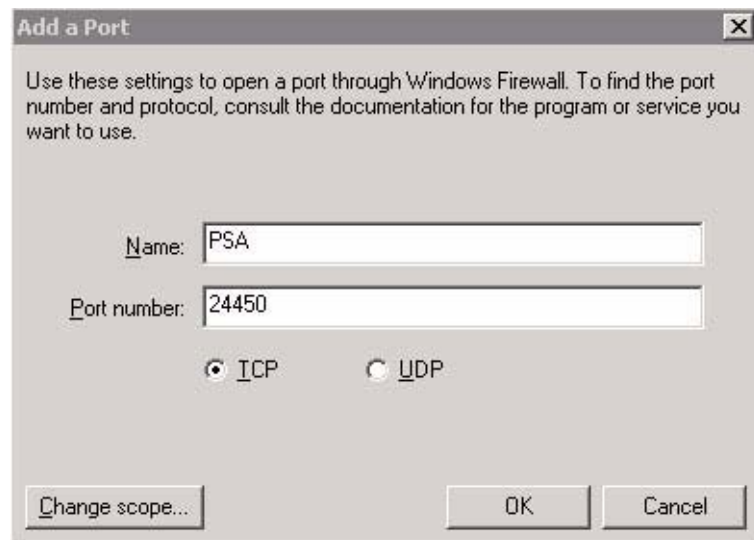


Figure 4.42 [Add a Port] dialog box

- 4 Click the [Add Port] button in the [Windows Firewall] window again.
The [Add Port] dialog box opens.

- 5 Enter the port number used by SNMP, and click the [OK] button.

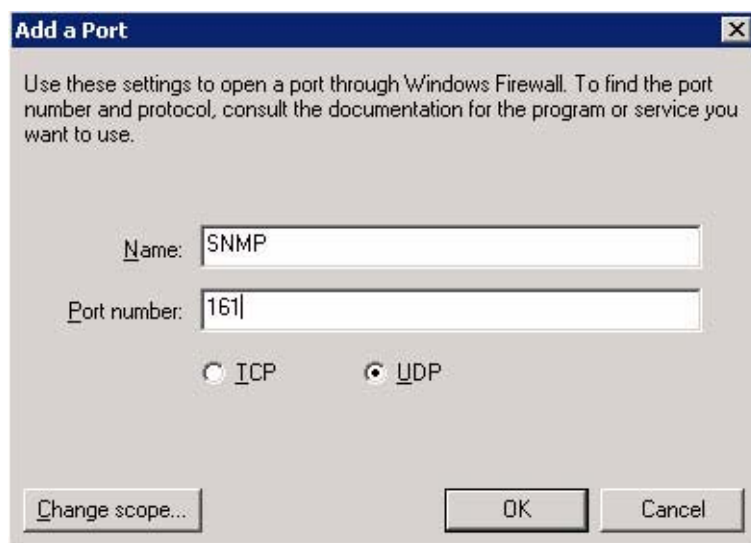


Figure 4.43 [Add a Port] dialog box

- 6 In the [Windows Firewall] window, click the [OK] button, and this ends the setting procedure.

4.5.5.4 Setting Watchdog monitoring after a STOP error (a fatal system error) occurs

If a STOP error (a fatal system error) occurs in the system, the results are as follows:

- "Panic" is displayed for "System Progress" of the relevant partition in [Partition]-[Power Control] of the MMB Web-UI.
- A memory dump is collected in the system.

In such cases, to prevent the system from freezing or otherwise becoming non-responsive, monitoring using the Watchdog timer can be set.

When the specified time has elapsed, the MMB executes a Hard Reset, and the OS is rebooted.

Setting procedure

- 1 Open the following file:
[PSA installation folder] \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Example: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf)
- 2 Specify a key value as shown below. The default is 0.
Section: [WATCHDOG]
Key: [TIMER]
Set value (unit: seconds) 0 (Watchdog timer not used)
1 to 6000 (Watchdog timer monitoring time)
Remarks: For the set value, measure the time required for memory dump in the applicable environment and determine the appropriate value. If the required time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog timer not used).
If the set value is shorter than the time required for memory dump processing, the Watchdog timer expires, resulting in execution of a Hard Reset, with the result that the memory dump cannot be collected correctly.

4.5.6 PSA update installation

This section describes the PSA update installation procedure.

Note: If the version of the fix program to be installed is the same as that of the installed PSA, a confirmation dialog box appears. Clicking the [OK] button in the dialog box uninstalls and then reinstalls the PSA.

Remarks: For the procedure for obtaining fix programs, ask your Fujitsu certified engineer or the support center.

(1) Minor update installation

- 1 Save the fix program (fjpsaxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.

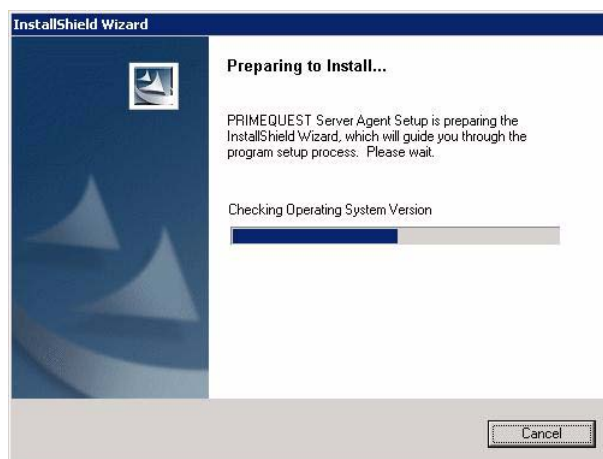


Figure 4.44 Installation preparation window

- 3 When the following window is displayed to indicate that the system is ready for installation, click the [Next] button to perform installation. Program updating is started.



Figure 4.45 PRIMEQUEST Server Agent Update window

- 4 Click the [Finish] button to finish processing.

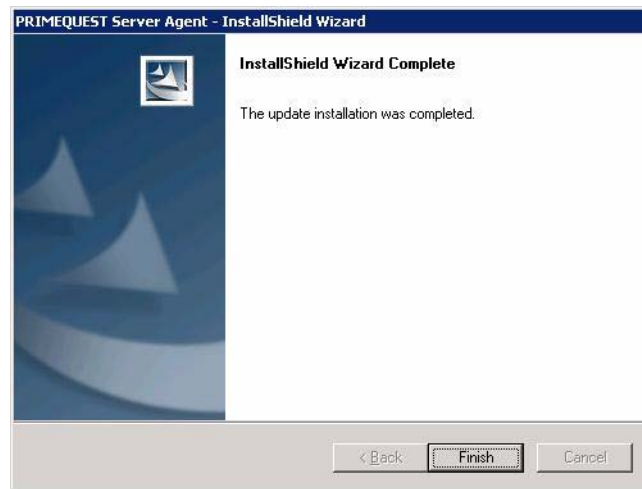


Figure 4.46 Update completion window

- 5 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

(2) Major update installation

- 1 Save the fix program (fjpsaxxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.



Figure 4.47 Installation preparation window

- 3 When a confirmation message is displayed, click the [OK] button. Uninstallation is started.

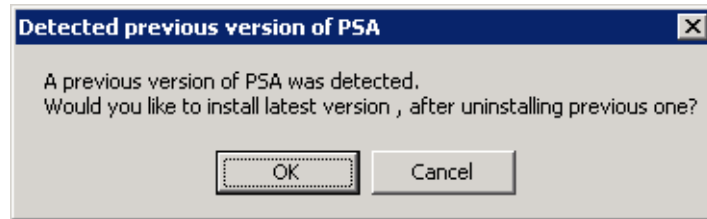


Figure 4.48 [Deleted previous version of PSA] window

- 4 When uninstallation is completed, installation of the new version is started. For the installation procedure, see steps 3 to 5 in Section [4.5.3, "Installing PSA."](#)

4.5.7 PSA uninstallation

This section describes the procedure for uninstalling PSA.

- 1 Click [Control Panel] → [Add/Remove Programs].
- 2 Select [PRIMEQUEST Server Agent] from [Currently Installed Programs], and click [Change/Delete].
- 3 A deletion confirmation message appears. Click [OK] to start uninstallation.

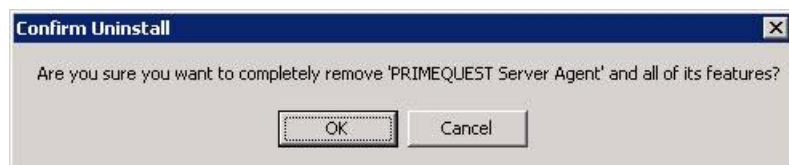


Figure 4.49 Confirmation window

- 4 When uninstallation is completed, a maintenance completion window is displayed. Click [Finish].

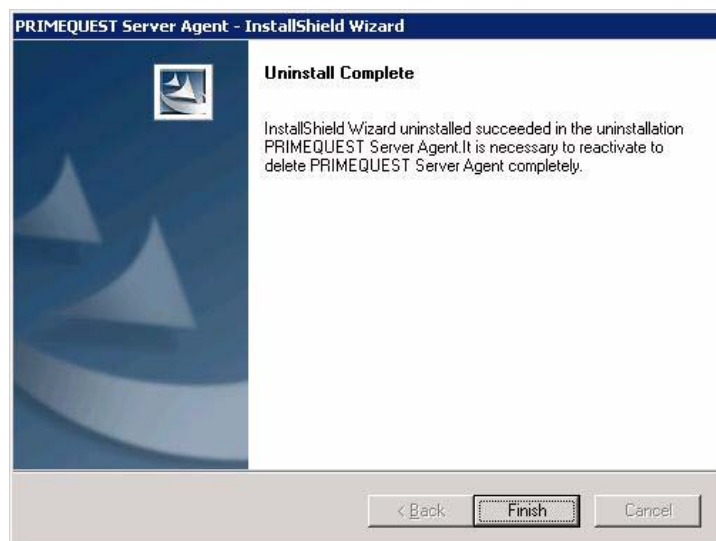


Figure 4.50 Maintenance completion window

- 5 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

4.6 Manual PSA Installation (Windows Server 2008) (PRIMEQUEST 580A/540A/580/540)

This section describes the procedure for installing PSA under the Windows Server 2008 operating system. Before starting the installation procedure, log in to the system with the administrator privilege.

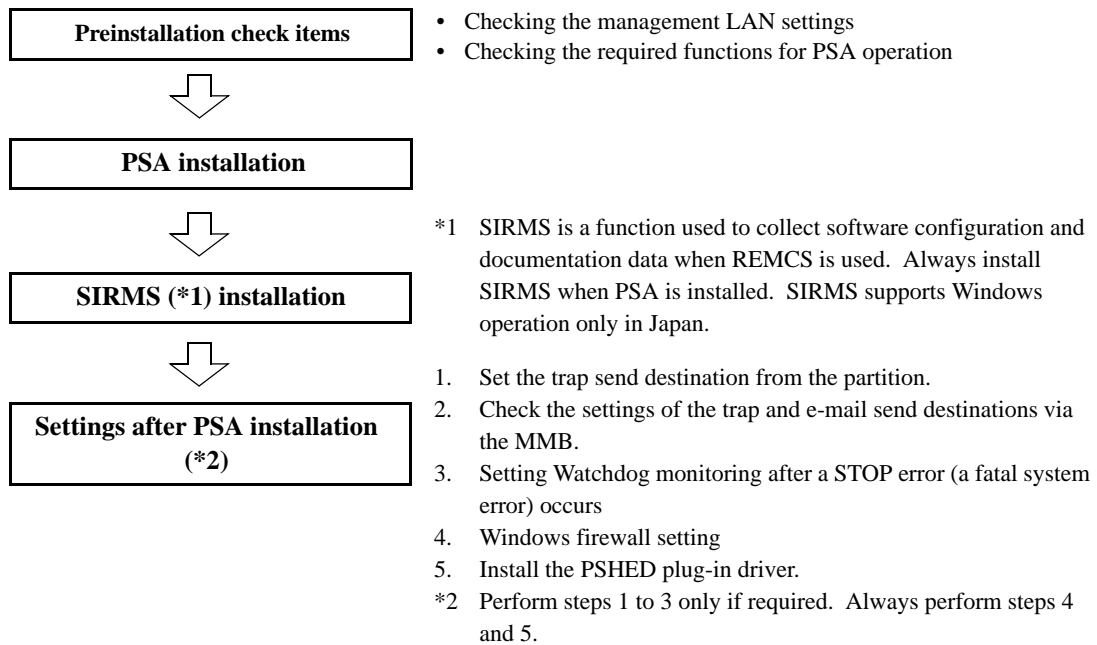
Notes: When using Windows Server 2008 OS, use PSA version 1.15 or later.

Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog partition monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- Partition information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.

4.6.1 Installation Workflow

The figure below shows the workflow for PSA installation.



Remarks: If you perform batch installation using the batch installer included in the High-Reliability Tools, this PSA and SIRMS installation work is unnecessary. However, after such a batch installation, the procedures described in the above "Preinstallation check items" and "Settings after PSA installation" sections must be followed.

Notes:

- In the first attempt to open the PSA window from the Web-UI after the system restart following PSA installation, the error message "E_33077 PSA is Not Active. (01:0000)" may be displayed. This may occur because PSA requires a certain amount of time to acquire sensor information for the system. Wait a few minutes, then try to open the window again.
- After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.
- Do not stop the Windows service, print spooler service. The operating system information collection function uses the Windows Management Instrumentation (WMI) to collect the configuration information. However, when the print spooler service is stopped, an error is reported to WMI and configuration information is not collected correctly.

4.6.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.6.2.1)
- [Verifying the services required for PSA operation](#) (→ 4.6.2.2)

4.6.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: If you perform batch installation using the batch installer included in the High-Reliability Tools, configure the management LAN after the batch installation is completed.

(1) Verifying the NIC for the management LAN

In Device Manager, display the properties of the network adapters (Intel PRO/100 VE Network Connection and Intel PRO/100 M Network Connection) assigned to the management LAN, and check the settings in [Location] on the [General] tab.

Connect the network adapters for the management LAN to MMB#0 and MMB#1 as follows:

- MMB#0: PCI Bus 1, Device 8, Function 0
- MMB#1: PCI Bus 1, Device 0, Function 0

Use the teaming function of Intel PROSet to configure the above network adapters for duplicated communication with the management LAN.

For Intel PROSet teaming, specify the IP addresses of the devices for the management LAN that are configured for duplicated communication.

(2) Configuring the two network adapters for the management LAN so that the adapters are duplicated

Use the teaming function of Intel PROSet to configure the network adapter for the management LAN to guarantee management LAN operation for duplicated communication.

Install Intel PROSet beforehand.

Note:

- Change the VLAN setting of the MMB management LAN hub to "VLAN Mode." (For details, see 2.2.4.5, "Setting a VLAN in a management LAN hub" in the *PRIMEQUEST 500A/500/400 Installation Manual*.)
 - The Spanning Tree Protocol (STP) function of the switch connected to the user port (management LAN) of the MMB must be disabled.
 - Implementing teaming initializes the network settings. In this case, perform operations from the console.
- 1 Click [Control Panel] → [Administrative Tools] → [Computer Management] → [Device Manager].
 - 2 Open [Network Adapter], and click [Inter(R) PRO/100 VE Network Connection] to select it.

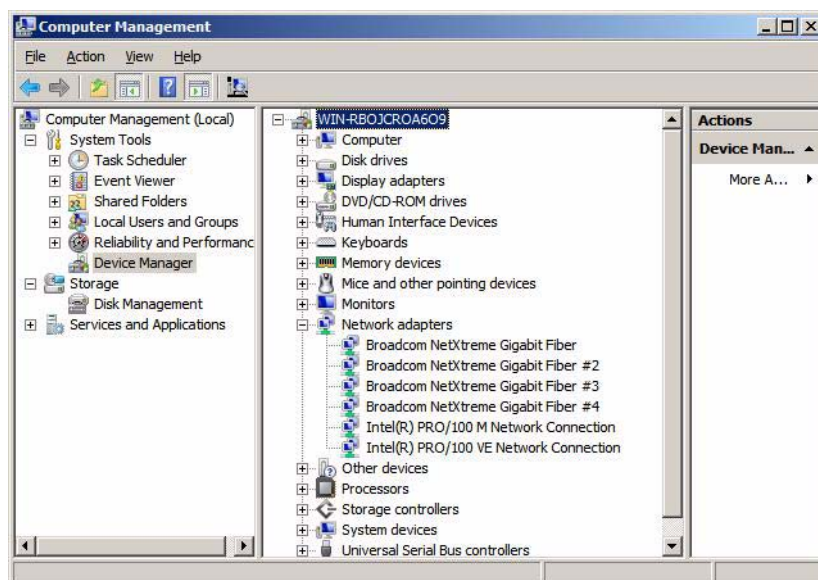


Figure 4.51 [Computer Management] window

- 3 The [Intel(R) PRO/100 VE Network Connection Properties] dialog box opens. Click the [Teaming] tab, select [Team with other adapters], and click the [New Team] button.

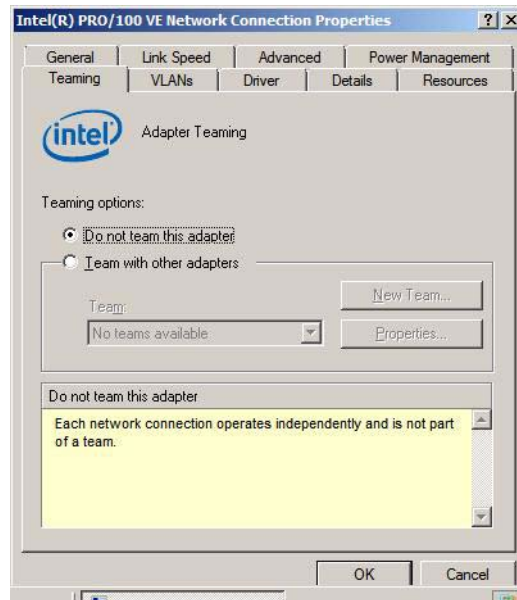


Figure 4.52 [Teaming] tab

- 4 The [New Team Wizard] window is displayed. Enter a team name (the default team name is Team #0), and click the [Next] button.

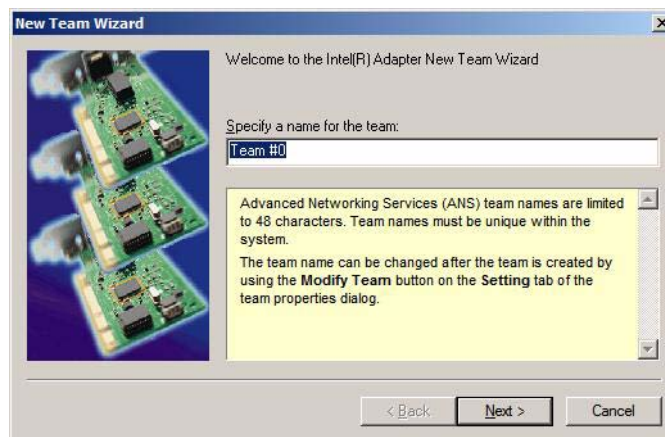


Figure 4.53 [New Team Wizard] window

- 5 A list of network adapters is displayed for teaming.
Select [Intel(R) PRO/100 VE Network Connection] and [Intel(R) Pro/100 M Network Connection] check boxes, and click the [Next] button.

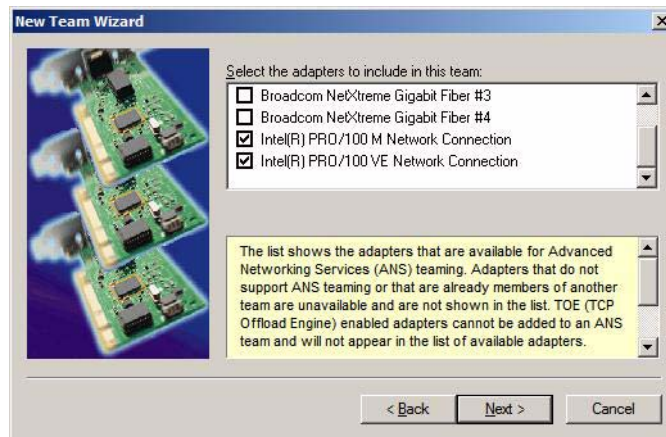


Figure 4.54 List of network adapters

- 6 Select [Adapter Fault Tolerance] from the mode list, and click the [Next] button.

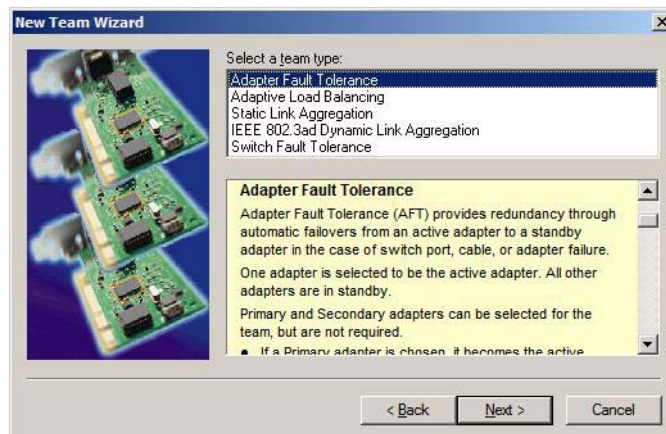


Figure 4.55 List of team mode

- 7 The following window is displayed. Teaming configuration processing starts when you click the [Finish] button.

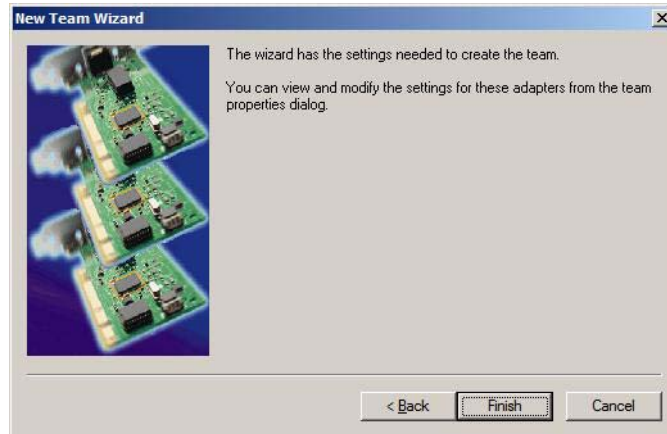


Figure 4.56 Selection Completed window

- 8 When the configuration processing for Teaming is finished, a Teaming device is created, and Team properties are displayed. Click the [Settings] tab, and confirm that the displayed adapter information is correct. If the information is correct, click the [OK] button to exit. Otherwise, click the [Remove Team] button to delete the Teaming device, and start again from step 2 of this procedure.

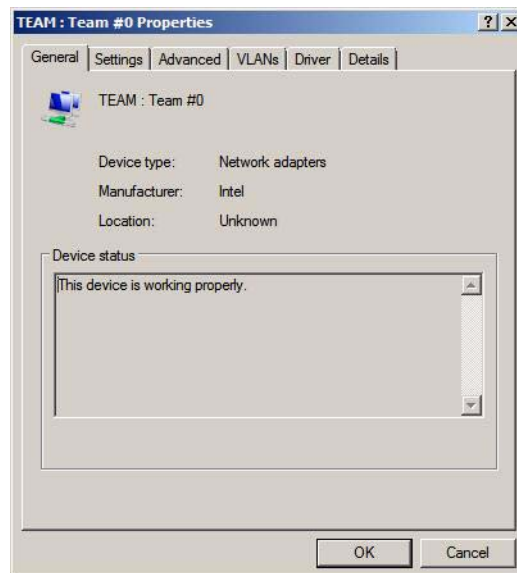


Figure 4.57 Team Number 0 Properties window

- 9 The [Intel(R) PRO/100 VE Network Connection Properties] dialog box opens again.
Click the [OK] button to finish processing, and close [Computer Management].
- 10 Click [Control Panel] → [Network and Sharing Center] → [Manage network connections].
A list of networks is displayed.
- 11 Select the network whose device name is the specified Team name (e.g., Team #0), and select [Properties] from the right-click menu.
- 12 Select [Internet Protocol Version 4 (TCP/IPv4)], click the [Properties] button, and specify the IP address, subnet mask, default gateway, and other parameters in the [Internet Protocol Version 4 (TCP/IPv4) Properties] dialog box. After completing the settings, click the [OK] button.

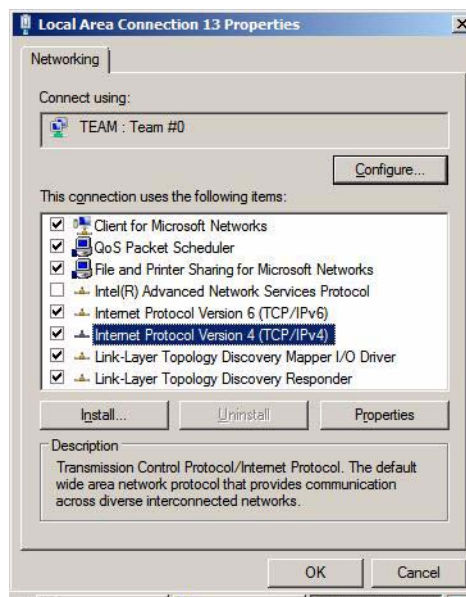


Figure 4.58 [Local Area Network Connection Properties] dialog box

As a result, the adapter activates its link monitoring function, thereby setting management LAN duplication.

Reboot to make the Teaming settings effective.

4.6.2.2 Verifying the services required for PSA operation

The SNMP service is required for running PSA. Add the SNMP service by following the procedure below.

- 1 Click the [Start] menu → [Server Manager].
- 2 In the [Server Manager] window, select [Features] → [Add Features] → [SNMP Services].
- 3 Confirm that the [SNMP Services] check box is selected, and then click the [OK] button.

The Windows Components Wizard is displayed again.

Note: If the check box is not checked, the SNMP service is not installed. Make sure to select the appropriate check box to install the SNMP service.

In the [Windows Component Wizard] window, click the [Next] button, and install the service by following instructions from the wizard.

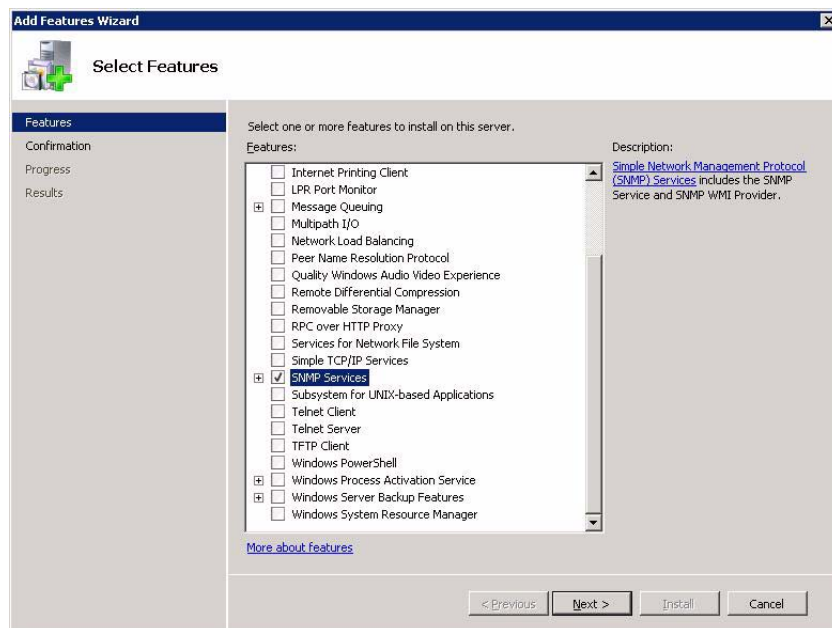


Figure 4.59 [Select Features] window

4.6.3 Installing PSA

Prepare the "PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2008" (C122-E093) that are supplied with the main unit.

- 1 Execute Tools\General\PSA\fjpsaxxxx.exe. (xxxx: version number).
The following window is displayed while the installation procedure is being prepared.

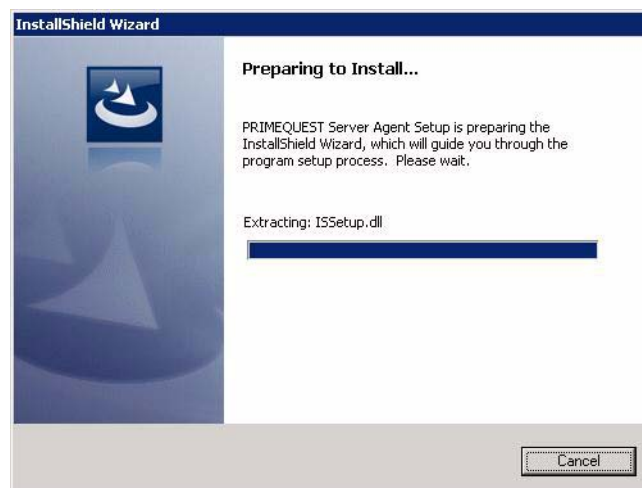


Figure 4.60 Installation preparation window

- 2 When the following window is displayed, indicating that the system is ready for installation, click [Next] to perform installation.

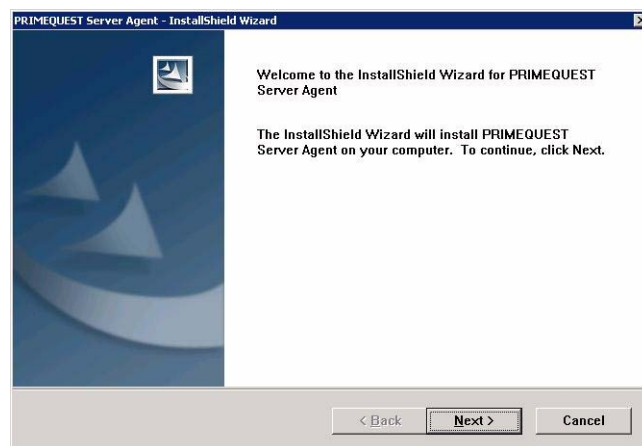


Figure 4.61 Installation window

- 3 Specify the installation destination, and click [Next].
PSA is installed in the Program Files\Fujitsu folder by default. To change the installation destination, click [Browse] and specify the desired folder.

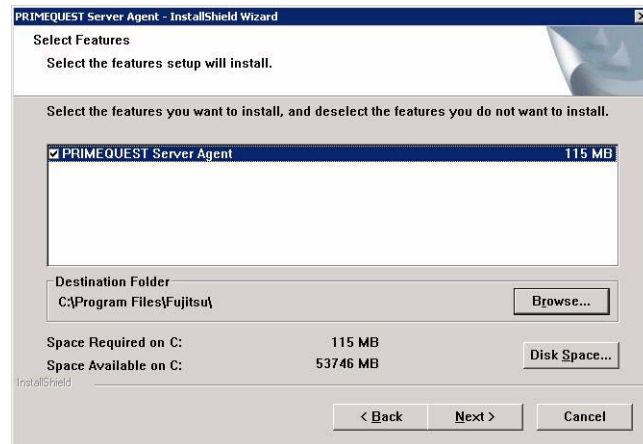


Figure 4.62 [Select Features] window

- 4 When installation is completed, the setup completion window is displayed. Click [Finish].
- 5 If a reboot is necessary, a message is displayed to ask whether you want to restart the PC immediately. Check whether the PC can be restarted. If it can, select the restart option, and click the [Finish] button.

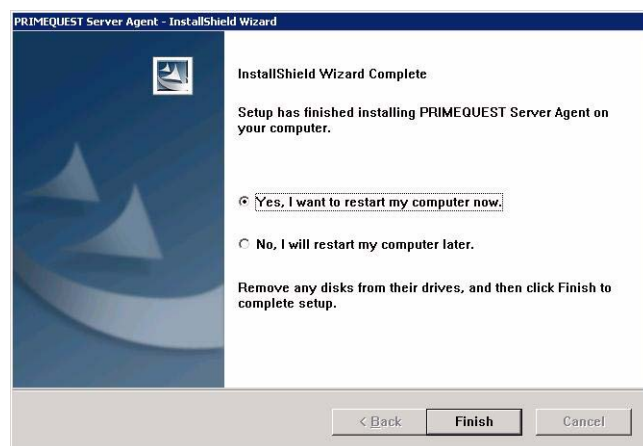


Figure 4.63 [InstallShield Wizard Complete] window

4.6.4 Items automatically set during PSA installation

During PSA installation, the specified values of various parameters for PSA operation are automatically set:

- 1 Service settings
 - PRIMEQUEST Server Agent
 - PRIMEQUEST PEM Command Service
 - PRIMEQUEST PSA Environment Control Service
- 2 Environment variable settings
 - PATH variable
Values for use by PSA are added to the existing PATH variable.
 - FJSVpsa_INSTALLPATH variable
This is a new variable that is added.
- 3 Port setting
The parameter is set to ensure that PSA uses the TCP:24450 port.
- 4 SNMP security setting
Make SNMP Service security settings because PSA must receive SNMP packets from the MMB.
The subsequent processes vary as follows depending on the parameter selected on the [Security] tab in the [Properties] dialog box of [SNMP Service] during PSA installation.
 - If [Accept SNMP packets from any host] was selected:
Make no SNMP security setting.
 - If [Accept SNMP packets from these hosts] was selected:
Make the SNMP security setting unless the IP address of the MMB and localhost parameter are specified.

Note: To change the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts] after PSA installation, or to change the IP address of the MMB, execute the SNMP security setting command (setsnmpsec). For details on this command, see the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

5 Window Management Instrumentation (WMI) setting

PSA collects information on PCI cards and SCSI devices by using WMI, which is installed as standard with Windows.

If the amount of memory and the number of internal handles that WMI uses to collect this information are insufficient because there are many LUNs, such as in RAIDs, change settings to the following values:

- Maximum amount of memory used: 536,870,912 bytes
- Maximum number of internal handles: 65,536

6 Task scheduler settings

To monitor for errors involving the power supply of the expansion file unit and FANs, make the following task scheduler settings:

Task name: File Unit Status Check

Activation interval: 5 minutes

The configuration information is collected when the PSA is started. Error monitoring is then performed based on the collected information until the next time the PSA is started. If an expansion file unit is not connected, configuration information is collected according to the schedule, but the process is completed immediately without error monitoring performed. Therefore, no additional workload is imposed on the system.

4.6.5 Settings after PSA installation

This section describes the settings to be made after PSA installation:

- [Setting the destination of trap sending from the partition \(→ 4.6.5.1\)](#)
- [Setting the destinations of trap and e-mail sending via the MMB \(→ 4.6.5.2\)](#)
- [Windows firewall setting \(→ 4.6.5.3\)](#)
- [Setting Watchdog monitoring after a STOP error \(a fatal system error\) occurs \(→ 4.6.5.4\)](#)
- [Installing the PSBED plug-in driver \(→ 4.6.5.5\)](#)

Notes:

- In the properties for the system log of the event viewer or the application log, do not change the operation that is performed when the maximum log size is reached to "Do not overwrite events (clear log manually)." Otherwise, any error that occurs when the maximum log size is reached is not output to the log, so PSA cannot detect the error.

4.6.5.1 Setting the destination of trap sending from the partition

Note:

- SNMP v.3 is not supported in Windows.
- Perform the tasks for this setting only if the setting is required.
- If partitions are managed by operation management software, this setting is required.

- 1 Click [Start] menu → [Control Panel] → [Administrative Tools].
- 2 Click [Computer Management].
- 3 In the left tree, click [Services and Applications] → [Services].
- 4 In the right pane, click [SNMP Service].
The [SNMP Service] dialog box appears.
- 5 Click the [Trap] tab.
- 6 Enter the desired community name in the [Community Name] field, and click [Add to List].
- 7 Click [Add] in the [Trap Send Destination] area.
- 8 Enter the host name or IP address of the server that will receive traps (for notification), and click [Add].
- 9 Click [OK].
- 10 Click the [Action] menu → [Restart] to restart the SNMP service.

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard SNMP Service trap that is normally used during the SNMP Service restart in step 10. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that standard SNMP Service traps can be received.

On the trap transfer source machine, restart SNMP Service by performing step 10.

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard SNMP Service trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03
pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP
v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap
(0) Uptime: 0:00:00.00
```

4.6.5.2 Setting the destinations of trap and e-mail sending via the MMB

Note:

- Perform the tasks for this setting only if the setting is required.
- If partitions are managed by operation management software, this setting is required.

Destinations for trap and e-mail sending via the MMB are the addresses set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.6.5.3 Windows firewall setting

To run your system with the Windows firewall enabled, specify [Exceptions] for the following ports to guarantee that data can be sent to and received from the MMB through the following ports:

- TCP port used by PSA: 24450 port
- TCP port used for SNMP: 161 port

Remarks: "SNMP Service" is displayed on the [Exceptions] tab of the firewall dialog box. Normally, this port is automatically set as an exception when SNMP Services is installed.

- 1 Click [Control Panel] → [Windows Firewall].
The [Windows Firewall] window opens.
- 2 Click the [Exceptions] tab, and click the [Add Port] button.
The [Add Port] dialog box opens.

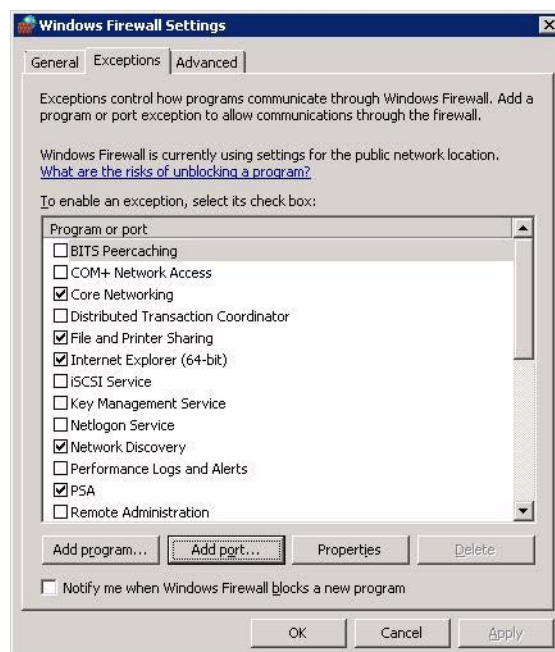


Figure 4.64 [Windows Firewall Settings] dialog box

- 3 Enter the port number used by PSA, and click the [OK] button.

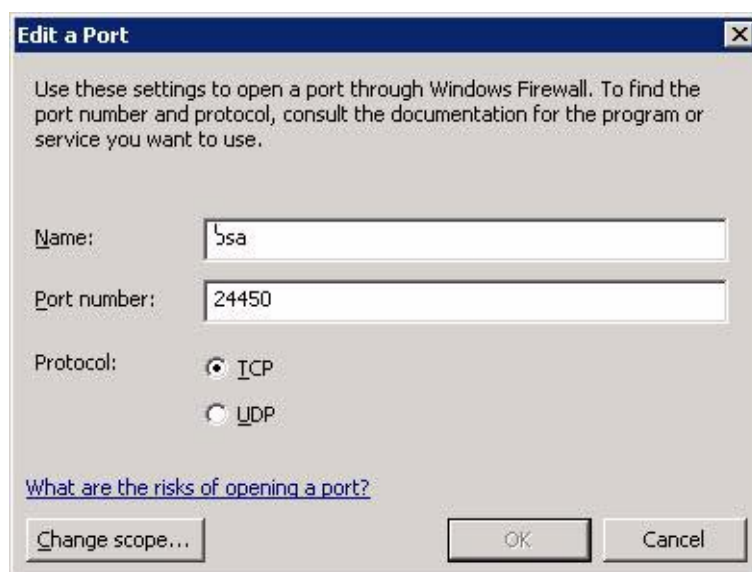


Figure 4.65 [Add a Port] dialog box

- 4 Click the [Add Port] button in the [Windows Firewall] window, and this ends the setting procedure.

4.6.5.4 Setting Watchdog monitoring after a STOP error (a fatal system error) occurs

If a STOP error (a fatal system error) occurs in the system, the results are as follows:

- "Panic" is displayed for "System Progress" of the relevant partition in [Partition]-[Power Control] of the MMB Web-UI.
- A memory dump is collected in the system.

In such cases, to prevent the system from freezing or otherwise becoming non-responsive, monitoring using the Watchdog timer can be set.

When the specified time has elapsed, the MMB executes a Hard Reset, and the OS is rebooted.

Setting procedure

- 1 Open the following file:
[PSA installation folder] \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Example: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf)
- 2 Specify a key value as shown below. The default is 0.
Section: [WATCHDOG]
Key: [TIMER]
Set value (unit: seconds) 0 (Watchdog timer not used)
1 to 6000 (Watchdog timer monitoring time)
Remarks: For the set value, measure the time required for memory dump in the applicable partition and determine the appropriate value. If the required time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog timer not used).
If the set value is shorter than the time required for memory dump processing, the Watchdog timer expires, resulting in execution of a Hard Reset, with the result that the memory dump cannot be collected correctly.

4.6.5.5 Installing the PSHED plug-in driver

The PSHED plug-in driver is required for extending the functions of the Windows Hardware Error Architecture (WHEA).

This driver is not automatically installed and must be installed manually using the batch file (plugin_install.bat) stored in the [PSA-installation-folder]\opt\FJSVpsa\sh\plugin_install.bat folder (e.g., C:\fujitsu\FJSVpsa\opt\FJSVpsa\sh\plugin_install.bat).

Unless this driver is installed, the following functions do not work:

- Inhibiting output of a log to the Event Viewer (Windows Log: System) in the event of a correctable error
- Transition to the panic state in the event of the blue screen of death (BSOD) (MMB Web-UI: [Power Control] page)

Procedure

- 1 Double-click [PSA-installation-folder]\opt\FJSVpsa\sh\plugin_install.bat (e.g., C:\fujitsu\FJSVpsa\opt\FJSVpsa\sh\plugin_install.bat).
- 2 In the [Windows Security] dialog box that appears, click [Install].



Figure 4.66 [Windows Security] dialog box

- 3 Restart the operating system. The driver starts running after the restart of the operating system.

4.6.6 PSA update installation

This section describes the PSA update installation procedure.

Note: If the version of the fix program to be installed is the same as that of the installed PSA, a confirmation dialog box appears. Clicking the [OK] button in the dialog box uninstalls and then reinstalls the PSA.

Remarks: For the procedure for obtaining fix programs, ask your Fujitsu certified engineer or the support center.

(1) Minor update installation

- 1 Save the fix program (fjpsaxxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.



Figure 4.67 Installation preparation window

- 3 When the following window is displayed to indicate that the system is ready for installation, click the [Next] button to perform installation. Program updating is started.

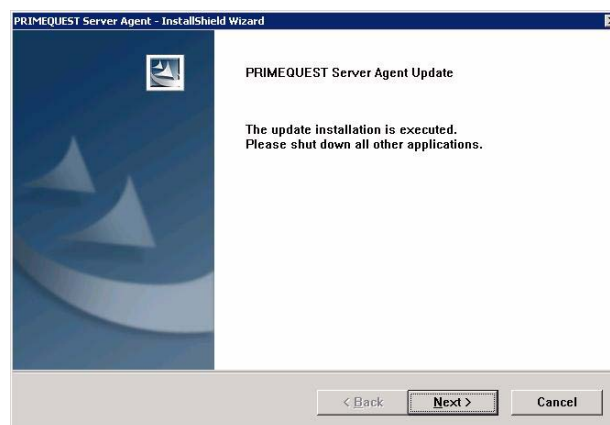


Figure 4.68 Update installation window

- 4 If the PSHED plug-in driver needs to be updated, the [Windows Security] dialog box shown below appears. Click the [Install] button.

After the completion of PSA installation in which the PSHED plug-in driver is updated, confirm that restarting the operating system will cause no problem, and then restart the operating system.



Figure 4.69 [Windows Security] dialog box

- 5 Click the [Finish] button to finish processing.

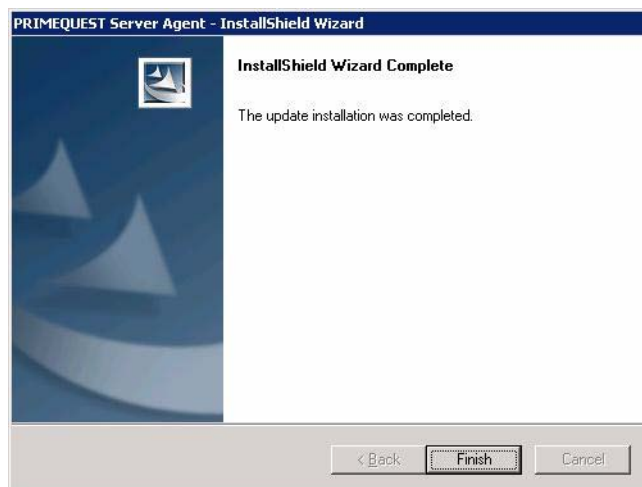


Figure 4.70 Update completion window

- 6 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

(2) Major update installation

- 1 Save the fix program (fjpsaxxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.

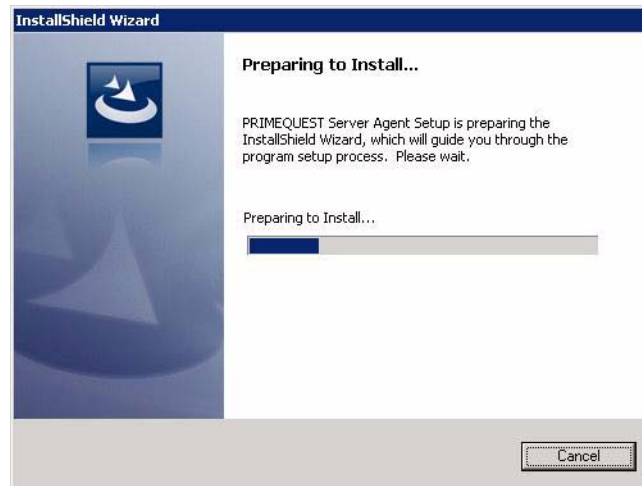


Figure 4.71 Installation preparation window

- 3 When a confirmation message is displayed, click the [OK] button. Uninstallation is started.



Figure 4.72 [Detected previous version of PSA] window

- 4 Installation of the new version begins when uninstallation is completed.

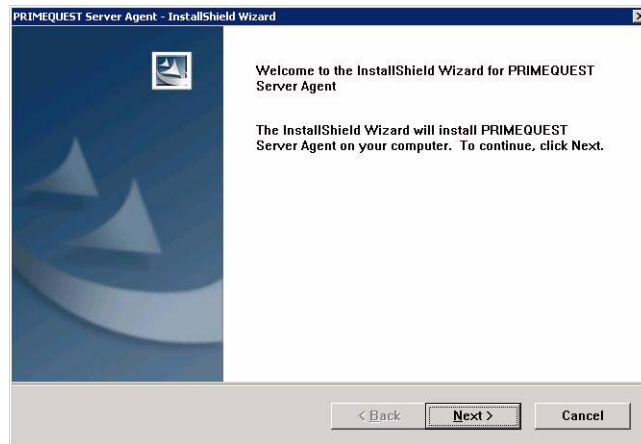


Figure 4.73 Update installation dialog box

- 5 Specify the installation destination, and then click the [Next] button. The default installation destination is "Program Files\Fujitsu." To change the installation destination, click the [Browse] button, and specify the desired installation destination.

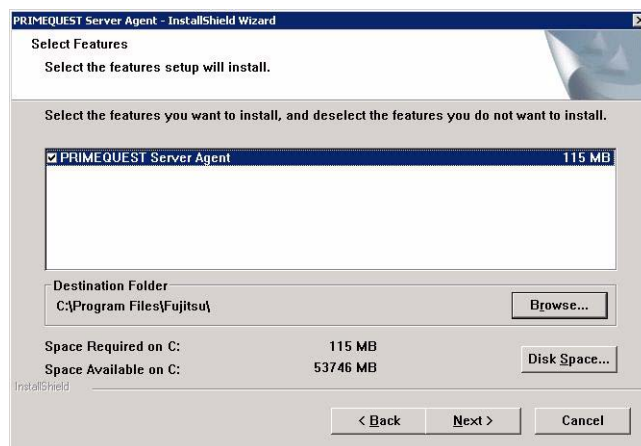


Figure 4.74 [Select Features] dialog box

- 6 If the PSHED plug-in driver needs to be updated, the [Windows Security] dialog box shown below appears. Click the [Install] button.

After the completion of PSA installation in which the PSHED plug-in driver is updated, confirm that restarting the operating system will cause no problem, and then restart the operating system.



Figure 4.75 [Windows Security] dialog box

- 7 Click the [Finish] button to end the wizard.

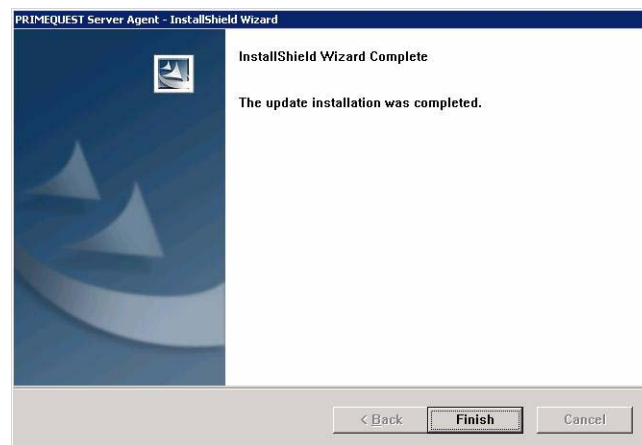


Figure 4.76 Update installation completion dialog box

- 8 If the system needs to be restarted, the wizard displays a dialog box asking whether you want to restart your computer now. Check whether you can restart the computer now without a problem. Unless there would be a problem, select the restart option, and click the [Finish] button.

Note: If an attempt is made to apply a correction program whose version is that same as that of one already installed for PSA, a maintenance dialog box (Figure 4.77) appears. Click [Cancel], and apply the correct version of the correction program.

4.6.7 PSA uninstallation

This section describes the procedure for uninstalling PSA.

- 1 Click [Control Panel] → [Programs and Features].
- 2 Select [PRIMEQUEST Server Agent] from [Currently Installed Programs], and click [Uninstall].

If you click [Change], the following dialog box appears. Select [Remove], and then click [Next].

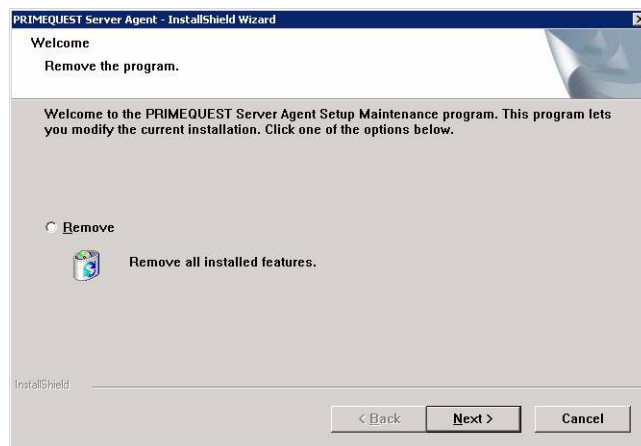


Figure 4.77 Maintenance dialog box

- 3 A removal confirmation message appears. Click the [Yes] button to start uninstallation.



Figure 4.78 Confirmation message dialog box

- 4 In the [Uninstall Complete] dialog box that appears when uninstallation is completed, click the [Finish] button.

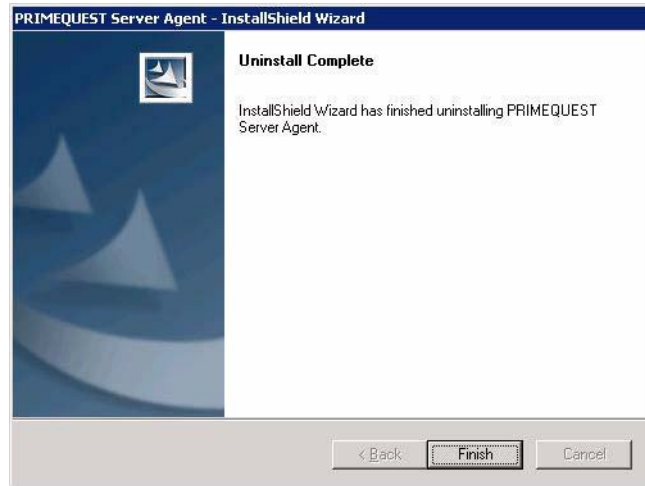


Figure 4.79 [Uninstall Complete] dialog box

- 5 Since the operating system must be restarted to remove the uninstalled PSLED plug-in driver, confirm that restarting the operating system will cause no problem, and then restart the operating system.

4.7 Manual PSA Installation (Windows Server 2008) (PRIMEQUEST 520A/520)

This section describes the procedure for installing PSA under the Windows Server 2008 operating system. Before starting the installation procedure, log in to the system with the administrator privilege.

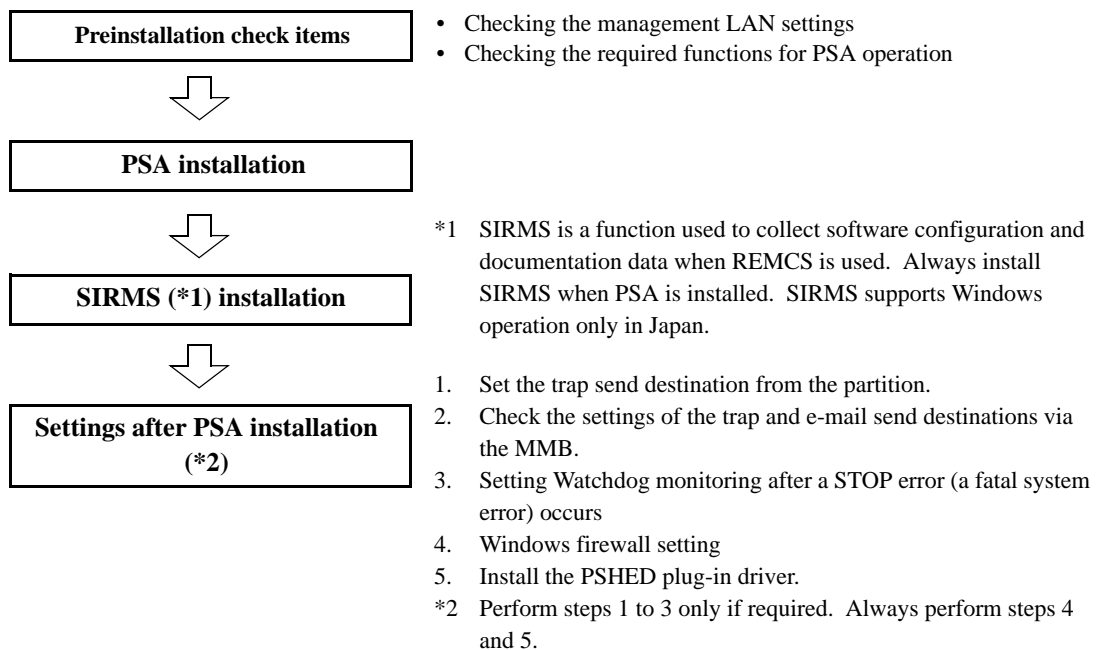
Notes: When using Windows Server 2008 OS, use PSA version 1.15 or later.

Remarks: When you use PRIMEQUEST, you must install PSA. If PSA is not installed, the following restrictions apply:

- I/O (PCI cards, hard disks, etc.) error notification, and trap notification to the administrator are disabled.
- Watchdog system monitoring is disabled.
- Notification of the following errors detected by predictive monitoring, and trap notification to the administrator are disabled:
 - Exceeded threshold of HDD S.M.A.R.T. monitoring
- Partition information cannot be collected with operation management software.
- Software errors are not reported even though a REMCS contract is established.

4.7.1 Installation Workflow

The figure below shows the workflow for PSA installation.



Remarks: If you perform batch installation using the batch installer included in the High-Reliability Tools, this PSA and SIRMS installation work is unnecessary. However, after such a batch installation, the procedures described in the above "Preinstallation check items" and "Settings after PSA installation" sections must be followed.

Notes:

- In the first attempt to open the PSA window from the Web-UI after the system restart following PSA installation, the error message "E_33077 PSA is Not Active. (01:0000)" may be displayed. This may occur because PSA requires a certain amount of time to acquire sensor information for the system. Wait a few minutes, then try to open the window again.
- After changing the IP address of an MMB or management LAN on the partition side, be sure to restart PSA. Otherwise, a PSA screen display error occurs in the Web-UI and detectable errors in PSA cannot be reported.
- Do not stop the Windows service, print spooler service.
The operating system information collection function uses the Windows Management Instrumentation (WMI) to collect the configuration information. However, when the print spooler service is stopped, an error is reported to WMI and configuration information is not collected correctly.

4.7.2 Preinstallation check items

This section describes the items that must be checked before PSA installation.

- [Checking the management LAN settings](#) (→ 4.7.2.1)
- [Verifying the services required for PSA operation](#) (→ 4.7.2.2)

4.7.2.1 Checking the management LAN settings

This section describes how to check the management LAN settings.

For communication of PSA with the MMB via the management LAN, the NIC connected to the management LAN on the partition side must be active.

Note: If you perform batch installation using the batch installer included in the High-Reliability Tools, configure the management LAN after the batch installation is completed.

(1) Verifying the NIC for the management LAN

In Device Manager, display the properties of the network adapters (Intel PRO/100 VE Network Connection) assigned to the management LAN, and check the settings in [Location] on the [General] tab.

Connect the network adapter for the management LAN to MMB as follows:

- MMB: PCI Bus 1, Device 8, Function 0

(2) Setting the network adapter for the management LAN

- 1 Click [Control Panel] → [Network and Sharing Center] → [Manage network connections].
A list of networks is displayed.
- 2 Select the network whose device name is the specified Team name and select [Properties] from the right-click menu.
- 3 Select [Internet Protocol Version 4 (TCP/IPv4)], click the [Properties] button, and specify the IP address, subnet mask, default gateway, and other parameters in the [Properties] dialog box of [Internet Protocol Version 4 (TCP/IPv4)].

4.7.2.2 Verifying the services required for PSA operation

The SNMP service is required for running PSA. Confirm that the SNMP service is installed by following the procedure below.

Remarks: This operation requires the Windows installation DVD.

- 1 Click the [Start] menu → [Server Manager].
- 2 In the [Server Manager] window, select [Features] → [Add Features] → [SNMP Services].
- 3 Confirm that the [SNMP Services] check box is selected, and then click the [OK] button.

The Windows Components Wizard is displayed again.

Note: If the check box is not checked, the SNMP service is not installed. Make sure to select the appropriate check box to install the SNMP service. In the [Windows Component Wizard] window, click the [Next] button, and install the service by following instructions from the wizard.

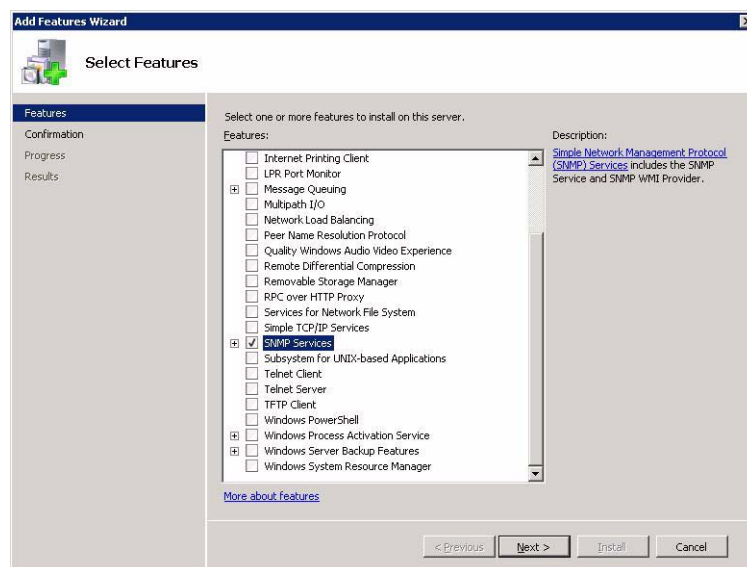


Figure 4.80 [Select Features] window

4.7.3 Installing PSA

Prepare the "PRIMEQUEST Drivers CD for Microsoft® Windows Server® 2008" (C122-E093) that are supplied with the main unit.

- 1 Execute Tools\General\PSA\fjpsaxxxx.exe. (xxxx: version number).
The following window is displayed while the installation procedure is being prepared.

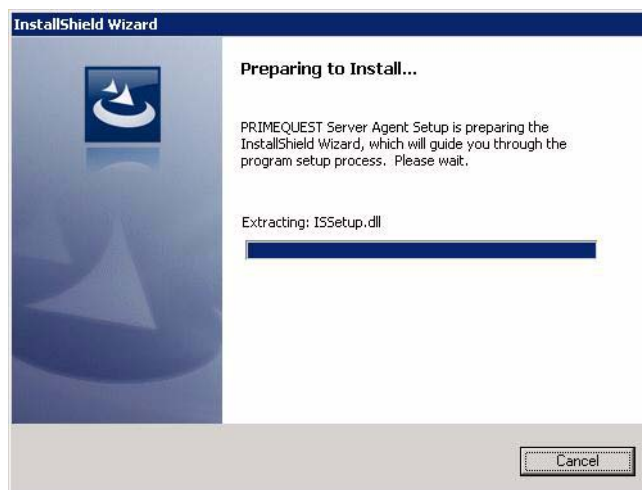


Figure 4.81 Installation preparation window

- 2 When the following window is displayed, indicating that the system is ready for installation, click [Next] to perform installation.

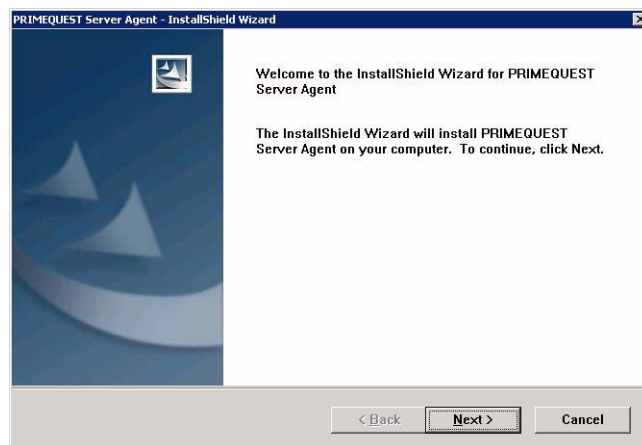


Figure 4.82 Installation window

- 3 Specify the installation destination, and click [Next].
PSA is installed in the Program Files\Fujitsu folder by default. To change the installation destination, click [Browse] and specify the desired folder.

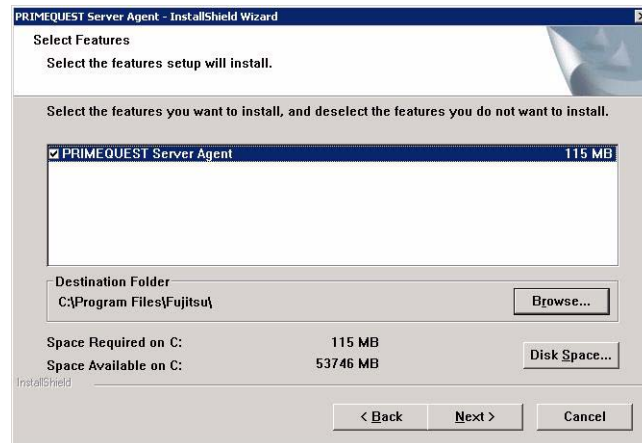


Figure 4.83 [Select Features] window

- 4 When installation is completed, the setup completion window is displayed. Click [Finish].
- 5 If a reboot is necessary, a message is displayed to ask whether you want to restart the PC immediately. Check whether the PC can be restarted. If it can, select the restart option, and click the [Finish] button.

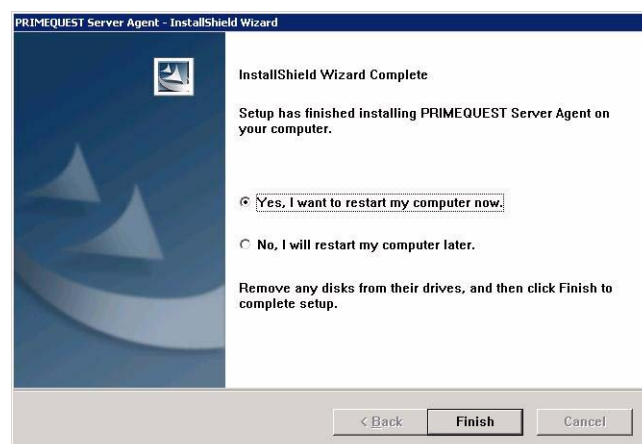


Figure 4.84 Installation completion window

4.7.4 Items automatically set during PSA installation

During PSA installation, the specified values of various parameters for PSA operation are automatically set:

- 1 Service settings
 - PRIMEQUEST Server Agent
 - PRIMEQUEST PEM Command Service
 - PRIMEQUEST PSA Environment Control Service
- 2 Environment variable settings
 - PATH variable
Values for use by PSA are added to the existing PATH variable.
 - FJSVpsa_INSTALLPATH variable
This is a new variable that is added.
- 3 Port setting
The parameter is set to ensure that PSA uses the TCP:24450 port.
- 4 SNMP security setting
Make SNMP Service security settings because PSA must receive SNMP packets from the MMB.
The subsequent processes vary as follows depending on the parameter selected on the [Security] tab in the [Properties] dialog box of [SNMP Service] during PSA installation.
 - If [Accept SNMP packets from any host] was selected:
Make no SNMP security setting.
 - If [Accept SNMP packets from these hosts] was selected:
Make the SNMP security setting unless the IP address of the MMB and localhost parameter are specified.

Note: To change the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts] after PSA installation, or to change the IP address of the MMB, execute the SNMP security setting command (setsnmpsec). For details on this command, see the *PRIMEQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

5 Window Management Instrumentation (WMI) setting

PSA collects information on PCI cards and SCSI devices by using WMI, which is installed as standard with Windows.

If the amount of memory and the number of internal handles that WMI uses to collect this information are insufficient because there are many LUNs, such as in RAIDs, change settings to the following values:

- Maximum amount of memory used: 536,870,912 bytes
- Maximum number of internal handles: 65,536

6 Task scheduler settings

To monitor for errors involving the power supply of the expansion file unit and FANs, make the following task scheduler settings:

Task name: File Unit Status Check

Activation interval: 5 minutes

The configuration information is collected when the PSA is started. Error monitoring is then performed based on the collected information until the next time the PSA is started. If an expansion file unit is not connected, configuration information is collected according to the schedule, but the process is completed immediately without error monitoring performed. Therefore, no additional workload is imposed on the system.

4.7.5 Settings after PSA installation

This section describes the settings to be made after PSA installation:

- [Setting the destination of trap sending from the partition \(→ 4.7.5.1\)](#)
- [Setting the destinations of trap and e-mail sending via the MMB \(→ 4.7.5.2\)](#)
- [Windows firewall setting \(→ 4.7.5.3\)](#)
- [Setting Watchdog monitoring after a STOP error \(a fatal system error\) occurs \(→ 4.7.5.4\)](#)
- [Installing the PSHED plug-in driver \(→ 4.7.5.5\)](#)

Notes:

- In the properties for the system log of the event viewer or the application log, do not change the operation that is performed when the maximum log size is reached to "Do not overwrite events (clear log manually)." Otherwise, any error that occurs when the maximum log size is reached is not output to the log, so PSA cannot detect the error.

4.7.5.1 Setting the destination of trap sending from the partition

Note:

- SNMP v.3 is not supported in Windows.
- Perform the tasks for this setting only if the setting is required.
- This setting is required for linkage with operation management software.

- 1 Click [Start] menu → [Control Panel] → [Administrative Tools].
- 2 Click [Computer Management].
- 3 In the left tree, click [Services and Applications] → [Services].
- 4 In the right pane, click [SNMP Service].
The [SNMP Service] dialog box appears.
- 5 Click the [Trap] tab.
- 6 Enter the desired community name in the [Community Name] field, and click [Add to List].
- 7 Click [Add] in the [Trap Send Destination] area.
- 8 Enter the host name or IP address of the server that will receive traps (for notification), and click [Add].
- 9 Click [OK].

10 Click the [Action] menu → [Restart] to restart the SNMP service.

Verifying the trap transfer destination setting

To verify the trap transfer destination setting, use the standard SNMP Service trap that is normally used during the SNMP Service restart in step 10. Check the reception of this trap to verify the transfer destination setting.

Remarks: A trap receipt application or trap manager must be active at the trap transfer destination to ensure that standard SNMP Service traps can be received.

On the trap transfer source machine, restart SNMP Service by performing step 10.

As a result, the trap receipt application at the trap transfer destination receives the "ColdStart" standard SNMP Service trap.

For example, if the trap transfer destination is a Linux machine, the following message is added to syslog when snmptrapd receives the trap, and this indicates that the trap transfer destination can correctly receive such traps.

```
Aug 17 14:50:03 shaka snmptrapd[2600]: 2005-08-17 14:50:03
pq-server.fujitsu.com [192.168.0.162] (via 192.168.0.162) TRAP, SNMP
v1, community public SNMPv2-SMI::enterprises.211.1.31.1.2.100.3 Cold Start Trap
(0) Uptime: 0:00:00.00
```

4.7.5.2 Setting the destinations of trap and e-mail sending via the MMB

Note:

- Perform the tasks for this setting only if the setting is required.
- This setting is required for linkage with operation management software.

Destinations for trap and e-mail sending via the MMB are the addresses set with the MMB Web UI.

For details, see the *PRIMEQUEST 500A/500/400 Series Installation Manual*.

- See Section 5.1.2, "System SNMP setting." for the MMB trap destination.
- See Section 2.2.3.6, "SMTP settings." for the e-mail destination.

4.7.5.3 Windows firewall setting

To run your system with the Windows firewall enabled, specify [Exceptions] for the following ports to guarantee that data can be sent to and received from the MMB through the following ports:

- TCP port used by PSA: 24450 port
- UDP port used for SNMP: 161 port

Remarks: "SNMP Service" is displayed on the [Exceptions] tab of the firewall dialog box. Normally, this port is automatically set as an exception when SNMP Services is installed.

- 1 Click [Control Panel] → [Windows Firewall].
The [Windows Firewall Settings] window opens.
- 2 Click the [Exceptions] tab, and click the [Add Port] button.
The [Add Port] dialog box opens.

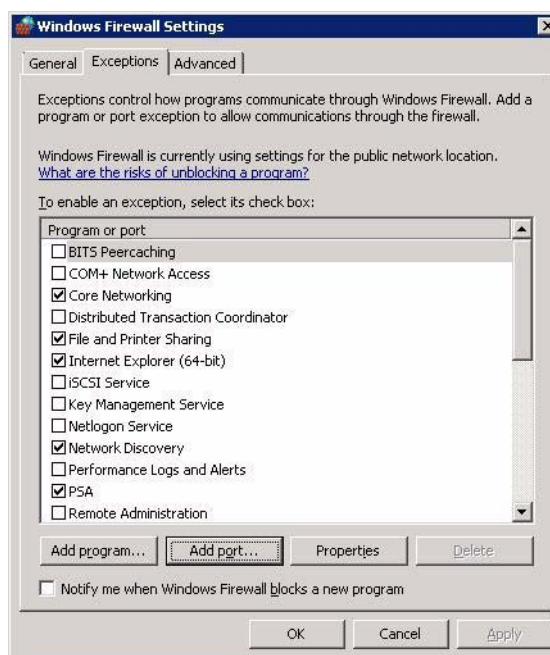


Figure 4.85 [Windows Firewall Settings] dialog box

- 3 Enter the port number used by PSA, and click the [OK] button.

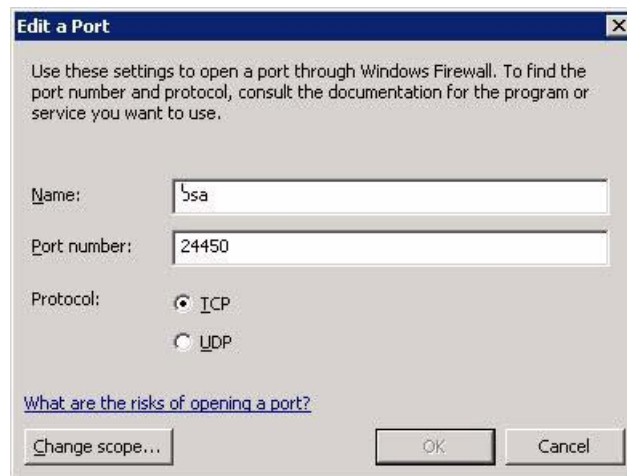


Figure 4.86 [Add a Port] dialog box

- 4 Enter the port number used by SNMP, and click the [OK] button.
- 5 In the [Windows Firewall] window, click the [OK] button, and this ends the setting procedure.

4.7.5.4 Setting Watchdog monitoring after a STOP error (a fatal system error) occurs

If a STOP error (a fatal system error) occurs in the system, the results are as follows:

- "Panic" is displayed for "System Progress" of the relevant partition in [Partition]-[Power Control] of the MMB Web-UI.
- A memory dump is collected in the system.

In such cases, to prevent the system from freezing or otherwise becoming non-responsive, monitoring using the Watchdog timer can be set.

When the specified time has elapsed, the MMB executes a Hard Reset, and the OS is rebooted.

Setting procedure

- 1 Open the following file:
[PSA installation folder] \etc\opt\FJSVpsa\usr\pnwatchdog.conf
(Example: C:\Program Files\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf)
- 2 Specify a key value as shown below. The default is 0.
Section: [WATCHDOG]
Key: [TIMER]
Set value (unit: seconds) 0 (Watchdog timer not used)
1 to 6000 (Watchdog timer monitoring time)
Remarks: For the set value, measure the time required for memory dump in the applicable environment and determine the appropriate value. If the required time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog timer not used).
If the set value is shorter than the time required for memory dump processing, the Watchdog timer expires, resulting in execution of a Hard Reset, with the result that the memory dump cannot be collected correctly.

4.7.5.5 Installing the PSHED plug-in driver

The PSHED plug-in driver is required for extending the functions of the Windows Hardware Error Architecture (WHEA).

This driver is not automatically installed and must be installed manually using the batch file (plugin_install.bat) stored in the [PSA-installation-folder]\opt\FJSVpsa\sh\plugin_install.bat folder (e.g., C:\fujitsu\FJSVpsa\opt\FJSVpsa\sh\plugin_install.bat).

Unless this driver is installed, the following functions do not work:

- Inhibiting output of a log to the Event Viewer (Windows Log: System) in the event of a correctable error
- Transition to the panic state in the event of the blue screen of death (BSOD) (MMB Web-UI: [Power Control] page)

Procedure

- 1 Double-click [PSA-installation-folder]\opt\FJSVpsa\sh\plugin_install.bat (e.g., C:\fujitsu\FJSVpsa\opt\FJSVpsa\sh\plugin_install.bat).
- 2 In the [Windows Security] dialog box that appears, click [Install].



Figure 4.87 [Windows Security] dialog box

- 3 Restart the operating system. The driver starts running after the restart of the operating system.

4.7.6 PSA update installation

This section describes the PSA update installation procedure.

Note: If the version of the fix program to be installed is the same as that of the installed PSA, a confirmation dialog box appears. Clicking the [OK] button in the dialog box uninstalls and then reinstalls the PSA.

Remarks: For the procedure for obtaining fix programs, ask your Fujitsu certified engineer or the support center.

(1) Minor update installation

- 1 Save the fix program (fjpsaxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.



Figure 4.88 Installation preparation window

- 3 When the following window is displayed to indicate that the system is ready for installation, click the [Next] button to perform installation. Program updating is started.

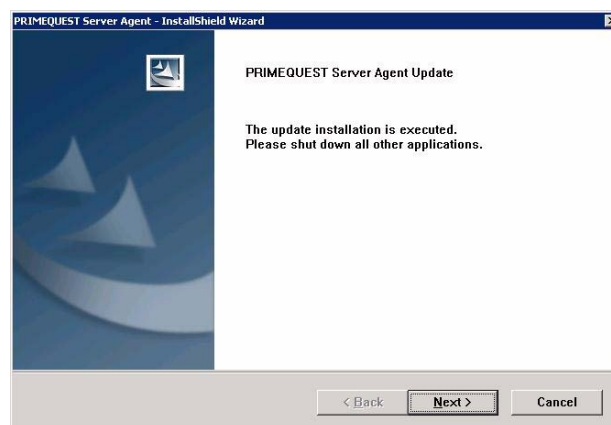


Figure 4.89 Update Installation window

- 4 If the PSHED plug-in driver needs to be updated, the [Windows Security] dialog box shown below appears. Click the [Install] button.

After the completion of PSA installation in which the PSHED plug-in driver is updated, confirm that restarting the operating system will cause no problem, and then restart the operating system.



Figure 4.90 [Windows Security] dialog box

- 5 Click the [Finish] button to finish processing.

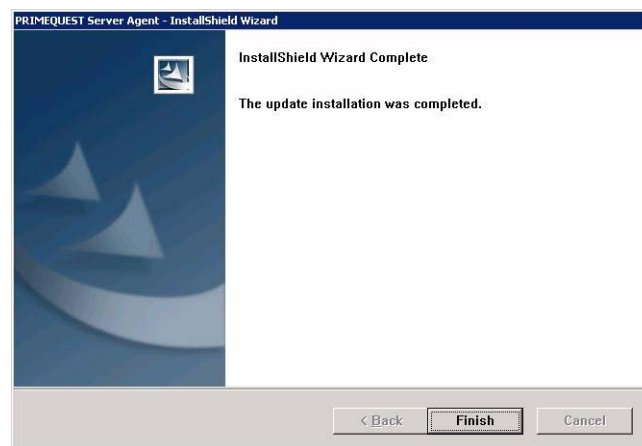


Figure 4.91 Update completion window

- 6 If a restart is necessary, a dialog box is displayed that prompts the user to specify whether to restart the computer. When this dialog box is displayed, confirm that a restart at this time would cause no problem, select the restart option, and click the [Finish] button.

(2) Major update installation

- 1 Save the fix program (fjpsaxxxx.exe) to the desired folder.
- 2 Start the fix program. The following installation preparation window opens.

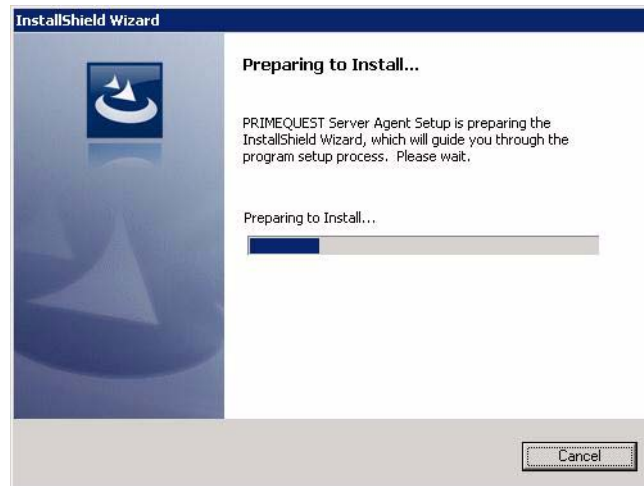


Figure 4.92 Installation preparation window

- 3 When a confirmation message is displayed, click the [OK] button. Uninstallation is started.

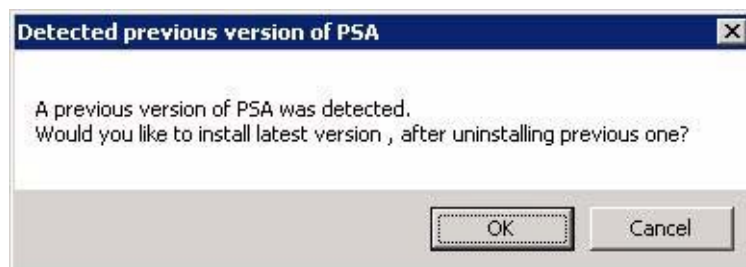


Figure 4.93 [Deleted previous version of PSA] window

- 4 Installation of the new version begins when uninstallation is completed.

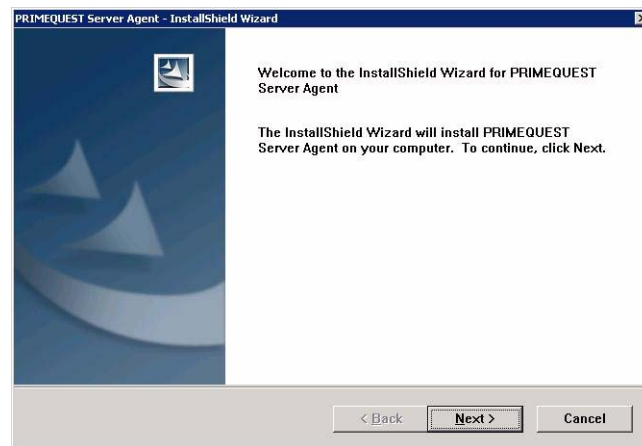


Figure 4.94 Update installation dialog box

- 5 Specify the installation destination, and then click the [Next] button.
The default installation destination is "Program Files\Fujitsu." To change the installation destination, click the [Browse] button, and specify the desired installation destination.

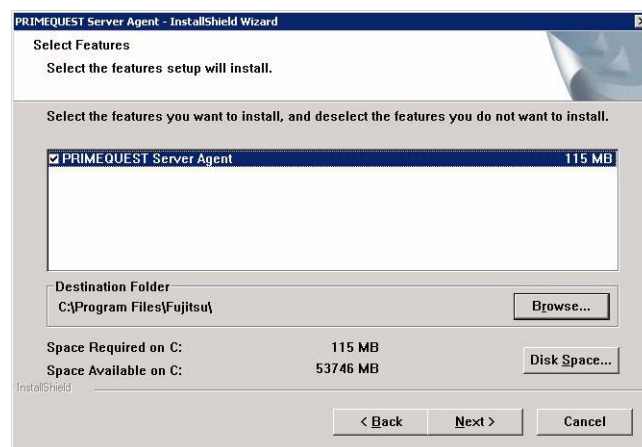


Figure 4.95 [Select Features] dialog box

- 6 If the PSHED plug-in driver needs to be updated, the [Windows Security] dialog box shown below appears. Click the [Install] button.

After the completion of PSA installation in which the PSHED plug-in driver is updated, confirm that restarting the operating system will cause no problem, and then restart the operating system.



Figure 4.96 [Windows Security] dialog box

- 7 Click the [Finish] button to end the wizard.

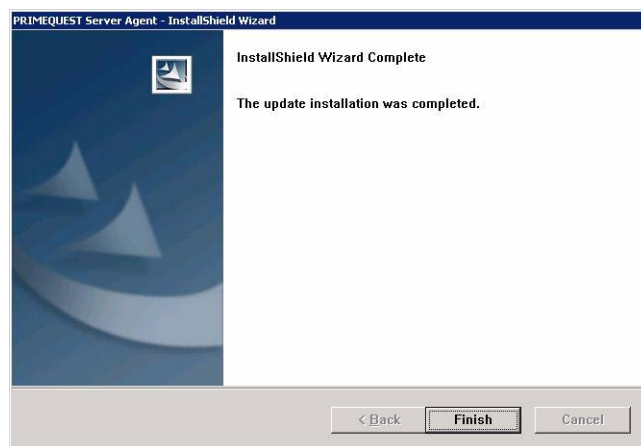


Figure 4.97 Update installation completion dialog box

- 8 If the system needs to be restarted, the wizard displays a dialog box asking whether you want to restart your computer now. Check whether you can restart the computer now without a problem. Unless there would be a problem, select the restart option, and click the [Finish] button.

Note: If an attempt is made to apply a correction program whose version is that same as that of one already installed for PSA, a maintenance dialog box (Figure 4.98) appears. Click [Cancel], and apply the correct version of the correction program.

4.7.7 PSA uninstallation

This section describes the procedure for uninstalling PSA.

- 1 Click [Control Panel] → [Programs and Features].
- 2 Select [PRIMEQUEST Server Agent] from [Currently Installed Programs], and click [Uninstall].

If you click [Change], the following dialog box appears. Select [Remove], and then click [Next].

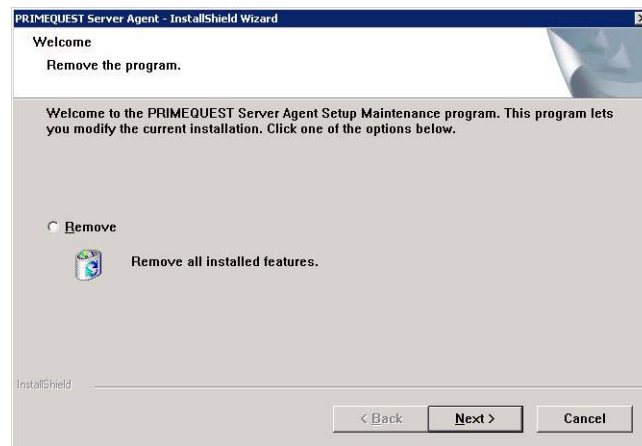


Figure 4.98 Maintenance dialog box

- 3 A removal confirmation message appears. Click the [Yes] button to start uninstallation.



Figure 4.99 Confirmation message dialog box

- 4 In the [Uninstall Complete] dialog box that appears when uninstallation is completed, click the [Finish] button.

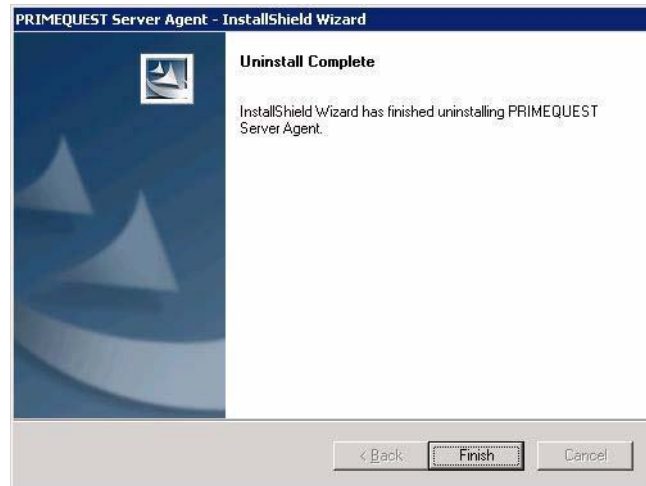


Figure 4.100 [Uninstall Complete] dialog box

- 5 Since the operating system must be restarted to remove the uninstalled PSBED plug-in driver, confirm that restarting the operating system will cause no problem, and then restart the operating system.

CHAPTER 5 Physical Locations and Bus Numbers

5.1 Physical Locations and Bus Numbers of Built-in I/Os of PRIMEQUEST 580A/540A/580/540/480/440

The following tables show the correspondence between each built-in I/O and its "SEG:BUS:DEV.FUNC" in PCI Segment mode and PCI Bus mode.

Table 5.1 Correspondence between physical locations and bus numbers of built-in I/Os (PCI Segment mode)

Home-I/O: Any of IOU#0 to #7

Internal I/O	SEG:BUS:DEV.FUNC	Memo
Home-I/O-BMM#0-USB#0	0000:00:1D.0	USB1.1 (Connected to KVM)
Home-I/O-BMM#0-USB#1	0000:00:1D.1	USB1.1 (Connected to KVM)
Home-I/O-BMM#0-USB#7	0000:00:1D.7	USB2.0 (USB port on the BMM)
Home-I/O-BMM#0-NIC#1	0000:01:00.0	Connected to MMB#1
Home-I/O-BMM#0-VGA	0000:01:01.0	VGA
Home-I/O-BMM#0-NIC#0	0000:01:08.0	Connected to MMB#0
IOU#0-GbE#0-FUNC#0	0000:03:01.0	To GSWB#0 port#1/GTHB#0 0-A
IOU#0-GbE#0-FUNC#1	0000:03:01.1	To GSWB#1 port#1/GTHB#1 0-A
IOU#0-SCSI#0-FUNC#0	0000:04:01.0	HDD#0, HDD#1
IOU#0-SCSI#0-FUNC#1	0000:04:01.1	SCSI port#0
IOU#0-GbE#1-FUNC#0	0000:06:01.0	To GSWB#0 port#2/GTHB#0 0-B
IOU#0-GbE#1-FUNC#1	0000:06:01.1	To GSWB#1 port#2/GTHB#1 0-B
IOU#0-SCSI#1-FUNC#0	0000:07:01.0	HDD#2, HDD#3
IOU#0-SCSI#1-FUNC#1	0000:07:01.1	SCSI port#1
IOU#1-GbE#0-FUNC#0	0001:03:01.0	To GSWB#0 port#3/GTHB#0 0-A
IOU#1-GbE#0-FUNC#1	0001:03:01.1	To GSWB#1 port#3/GTHB#1 0-A
IOU#1-SCSI#0-FUNC#0	0001:04:01.0	HDD#0, HDD#1
IOU#1-SCSI#0-FUNC#1	0001:04:01.1	SCSI port#0
IOU#1-GbE#1-FUNC#0	0001:06:01.0	To GSWB#0 port#4/GTHB#0 0-B
IOU#1-GbE#1-FUNC#1	0001:06:01.1	To GSWB#1 port#4/GTHB#1 0-B
IOU#1-SCSI#1-FUNC#0	0001:07:01.0	HDD#2, HDD#3
IOU#1-SCSI#1-FUNC#1	0001:07:01.1	SCSI port#1
IOU#2-GbE#0-FUNC#0	0002:03:01.0	To GSWB#0 port#5/GTHB#0 0-A

Internal I/O	SEG:BUS:DEV.FUNC	Memo
IOU#2-GbE#0-FUNC#1	0002:03:01.1	To GSWB#1 port#5/GTHB#1 0-A
IOU#2-SCSI#0-FUNC#0	0002:04:01.0	HDD#0, HDD#1
IOU#2-SCSI#0-FUNC#1	0002:04:01.1	SCSI port#0
IOU#2-GbE#1-FUNC#0	0002:06:01.0	To GSWB#0 port#6/GTHB#0 0-B
IOU#2-GbE#1-FUNC#1	0002:06:01.1	To GSWB#1 port#6/GTHB#1 0-B
IOU#2-SCSI#1-FUNC#0	0002:07:01.0	HDD#2, HDD#3
IOU#2-SCSI#1-FUNC#1	0002:07:01.1	SCSI port#1
IOU#3-GbE#0-FUNC#0	0003:03:01.0	To GSWB#0 port#7/GTHB#0 0-A
IOU#3-GbE#0-FUNC#1	0003:03:01.1	To GSWB#1 port#7/GTHB#1 0-A
IOU#3-SCSI#0-FUNC#0	0003:04:01.0	HDD#0, HDD#1
IOU#3-SCSI#0-FUNC#1	0003:04:01.1	SCSI port#0
IOU#3-GbE#1-FUNC#0	0003:06:01.0	To GSWB#0 port#8/GTHB#0 0-B
IOU#3-GbE#1-FUNC#1	0003:06:01.1	To GSWB#1 port#8/GTHB#1 0-B
IOU#3-SCSI#1-FUNC#0	0003:07:01.0	HDD#2, HDD#3
IOU#3-SCSI#1-FUNC#1	0003:07:01.1	SCSI port#1
IOU#4-GbE#0-FUNC#0	0004:03:01.0	To GSWB#0 port#9/GTHB#0 0-A
IOU#4-GbE#0-FUNC#1	0004:03:01.1	To GSWB#1 port#9/GTHB#1 0-A
IOU#4-SCSI#0-FUNC#0	0004:04:01.0	HDD#0, HDD#1
IOU#4-SCSI#0-FUNC#1	0004:04:01.1	SCSI port#0
IOU#4-GbE#1-FUNC#0	0004:06:01.0	To GSWB#0 port#10/GTHB#0 0-B
IOU#4-GbE#1-FUNC#1	0004:06:01.1	To GSWB#1 port#10/GTHB#1 0-B
IOU#4-SCSI#1-FUNC#0	0004:07:01.0	HDD#2, HDD#3
IOU#4-SCSI#1-FUNC#1	0004:07:01.1	SCSI port#1
IOU#5-GbE#0-FUNC#0	0005:03:01.0	To GSWB#0 port#11/GTHB#0 0-A
IOU#5-GbE#0-FUNC#1	0005:03:01.1	To GSWB#1 port#11/GTHB#1 0-A
IOU#5-SCSI#0-FUNC#0	0005:04:01.0	HDD#0, HDD#1
IOU#5-SCSI#0-FUNC#1	0005:04:01.1	SCSI port#0
IOU#5-GbE#1-FUNC#0	0005:06:01.0	To GSWB#0 port#12/GTHB#0 0-B
IOU#5-GbE#1-FUNC#1	0005:06:01.1	To GSWB#1 port#12/GTHB#1 0-B
IOU#5-SCSI#1-FUNC#0	0005:07:01.0	HDD#2, HDD#3
IOU#5-SCSI#1-FUNC#1	0005:07:01.1	SCSI port#1
IOU#6-GbE#0-FUNC#0	0006:03:01.0	To GSWB#0 port#13/GTHB#0 0-A
IOU#6-GbE#0-FUNC#1	0006:03:01.1	To GSWB#1 port#13/GTHB#1 0-A
IOU#6-SCSI#0-FUNC#0	0006:04:01.0	HDD#0, HDD#1
IOU#6-SCSI#0-FUNC#1	0006:04:01.1	SCSI port#0
IOU#6-GbE#1-FUNC#0	0006:06:01.0	To GSWB#0 port#14/GTHB#0 0-B
IOU#6-GbE#1-FUNC#1	0006:06:01.1	To GSWB#1 port#14/GTHB#1 0-B

Internal I/O	SEG:BUS:DEV.FUNC	Memo
IOU#6-SCSI#1-FUNC#0	0006:07:01.0	HDD#2, HDD#3
IOU#6-SCSI#1-FUNC#1	0006:07:01.1	SCSI port#1
IOU#7-GbE#0-FUNC#0	0007:03:01.0	To GSWB#0 port#15/GTHB#0 0-A
IOU#7-GbE#0-FUNC#1	0007:03:01.1	To GSWB#1 port#15/GTHB#1 0-A
IOU#7-SCSI#0-FUNC#0	0007:04:01.0	HDD#0, HDD#1
IOU#7-SCSI#0-FUNC#1	0007:04:01.1	SCSI port#0
IOU#7-GbE#1-FUNC#0	0007:06:01.0	To GSWB#0 port#16/GTHB#0 0-B
IOU#7-GbE#1-FUNC#1	0007:06:01.1	To GSWB#1 port#16/GTHB#1 0-B
IOU#7-SCSI#1-FUNC#0	0007:07:01.0	HDD#2, HDD#3
IOU#7-SCSI#1-FUNC#1	0007:07:01.1	SCSI port#1

Table 5.2 Correspondence between physical locations and bus numbers of built-in I/Os
(PCI Bus mode)

Home-IOU: Any of IOU#0 to #7

Internal I/O	SEG:BUS:DEV.FUNC	Memo
Home-IOU-BMMH#0-USB#0	0000:00:1D.0	USB1.1 (Connected to KVM)
Home-IOU-BMMH#0-USB#1	0000:00:1D.1	USB1.1 (Connected to KVM)
Home-IOU-BMMH#0-USB#7	0000:00:1D.7	USB2.0 (USB port on the BMM)
Home-IOU-BMMH#0-NIC#1	0000:01:00.0	Connected to MMB#1
Home-IOU-BMMH#0-VGA	0000:01:01.0	VGA
Home-IOU-BMMH#0-NIC#0	0000:01:08.0	Connected to MMB#0
IOU#0-GbE#0-FUNC#0	0000:03:01.0	To GSWB#0 port#1/GTHB#0 0-A
IOU#0-GbE#0-FUNC#1	0000:03:01.1	To GSWB#1 port#1/GTHB#1 0-A
IOU#0-SCSI#0-FUNC#0	0000:04:01.0	HDD#0, HDD#1
IOU#0-SCSI#0-FUNC#1	0000:04:01.1	SCSI port#0
IOU#0-GbE#1-FUNC#0	0000:06:01.0	To GSWB#0 port#2/GTHB#0 0-B
IOU#0-GbE#1-FUNC#1	0000:06:01.1	To GSWB#1 port#2/GTHB#1 0-B
IOU#0-SCSI#1-FUNC#0	0000:07:01.0	HDD#2, HDD#3
IOU#0-SCSI#1-FUNC#1	0000:07:01.1	SCSI port#1
IOU#1-GbE#0-FUNC#0	0000:23:01.0	To GSWB#0 port#3/GTHB#0 0-A
IOU#1-GbE#0-FUNC#1	0000:23:01.1	To GSWB#1 port#3/GTHB#1 0-A
IOU#1-SCSI#0-FUNC#0	0000:24:01.0	HDD#0, HDD#1
IOU#1-SCSI#0-FUNC#1	0000:24:01.1	SCSI port#0
IOU#1-GbE#1-FUNC#0	0000:26:01.0	To GSWB#0 port#4/GTHB#0 0-B
IOU#1-GbE#1-FUNC#1	0000:26:01.1	To GSWB#1 port#4/GTHB#1 0-B
IOU#1-SCSI#1-FUNC#0	0000:27:01.0	HDD#2, HDD#3
IOU#1-SCSI#1-FUNC#1	0000:27:01.1	SCSI port#1

Internal I/O	SEG:BUS:DEV.FUNC	Memo
IOU#2-GbE#0-FUNC#0	0000:43:01.0	To GSWB#0 port#5/GTHB#0 0-A
IOU#2-GbE#0-FUNC#1	0000:43:01.1	To GSWB#1 port#5/GTHB#1 0-A
IOU#2-SCSI#0-FUNC#0	0000:44:01.0	HDD#0, HDD#1
IOU#2-SCSI#0-FUNC#1	0000:44:01.1	SCSI port#0
IOU#2-GbE#1-FUNC#0	0000:46:01.0	To GSWB#0 port#6/GTHB#0 0-B
IOU#2-GbE#1-FUNC#1	0000:46:01.1	To GSWB#1 port#6/GTHB#1 0-B
IOU#2-SCSI#1-FUNC#0	0000:47:01.0	HDD#2, HDD#3
IOU#2-SCSI#1-FUNC#1	0000:47:01.1	SCSI port#1
IOU#3-GbE#0-FUNC#0	0000:63:01.0	To GSWB#0 port#7/GTHB#0 0-A
IOU#3-GbE#0-FUNC#1	0000:63:01.1	To GSWB#1 port#7/GTHB#1 0-A
IOU#3-SCSI#0-FUNC#0	0000:64:01.0	HDD#0, HDD#1
IOU#3-SCSI#0-FUNC#1	0000:64:01.1	SCSI port#0
IOU#3-GbE#1-FUNC#0	0000:66:01.0	To GSWB#0 port#8/GTHB#0 0-B
IOU#3-GbE#1-FUNC#1	0000:66:01.1	To GSWB#1 port#8/GTHB#1 0-B
IOU#3-SCSI#1-FUNC#0	0000:67:01.0	HDD#2, HDD#3
IOU#3-SCSI#1-FUNC#1	0000:67:01.1	SCSI port#1
IOU#4-GbE#0-FUNC#0	0000:83:01.0	To GSWB#0 port#9/GTHB#0 0-A
IOU#4-GbE#0-FUNC#1	0000:83:01.1	To GSWB#1 port#9/GTHB#1 0-A
IOU#4-SCSI#0-FUNC#0	0000:84:01.0	HDD#0, HDD#1
IOU#4-SCSI#0-FUNC#1	0000:84:01.1	SCSI port#0
IOU#4-GbE#1-FUNC#0	0000:86:01.0	To GSWB#0 port#10/GTHB#0 0-B
IOU#4-GbE#1-FUNC#1	0000:86:01.1	To GSWB#1 port#10/GTHB#1 0-B
IOU#4-SCSI#1-FUNC#0	0000:87:01.0	HDD#2, HDD#3
IOU#4-SCSI#1-FUNC#1	0000:87:01.1	SCSI port#1
IOU#5-GbE#0-FUNC#0	0000:A3:01.0	To GSWB#0 port#11/GTHB#0 0-A
IOU#5-GbE#0-FUNC#1	0000:A3:01.1	To GSWB#1 port#11/GTHB#1 0-A
IOU#5-SCSI#0-FUNC#0	0000:A4:01.0	HDD#0, HDD#1
IOU#5-SCSI#0-FUNC#1	0000:A4:01.1	SCSI port#0
IOU#5-GbE#1-FUNC#0	0000:A6:01.0	To GSWB#0 port#12/GTHB#0 0-B
IOU#5-GbE#1-FUNC#1	0000:A6:01.1	To GSWB#1 port#12/GTHB#1 0-B
IOU#5-SCSI#1-FUNC#0	0000:A7:01.0	HDD#2, HDD#3
IOU#5-SCSI#1-FUNC#1	0000:A7:01.1	SCSI port#1
IOU#6-GbE#0-FUNC#0	0000:C3:01.0	To GSWB#0 port#13/GTHB#0 0-A
IOU#6-GbE#0-FUNC#1	0000:C3:01.1	To GSWB#1 port#13/GTHB#1 0-A
IOU#6-SCSI#0-FUNC#0	0000:C4:01.0	HDD#0, HDD#1
IOU#6-SCSI#0-FUNC#1	0000:C4:01.1	SCSI port#0

Internal I/O	SEG:BUS:DEV.FUNC	Memo
IOU#6-GbE#1-FUNC#0	0000:C6:01.0	To GSWB#0 port#14/GTHB#0 0-B
IOU#6-GbE#1-FUNC#1	0000:C6:01.1	To GSWB#1 port#14/GTHB#1 0-B
IOU#6-SCSI#1-FUNC#0	0000:C7:01.0	HDD#2, HDD#3
IOU#6-SCSI#1-FUNC#1	0000:C7:01.1	SCSI port#1
IOU#7-GbE#0-FUNC#0	0000:E3:01.0	To GSWB#0 port#15/GTHB#0 0-A
IOU#7-GbE#0-FUNC#1	0000:E3:01.1	To GSWB#1 port#15/GTHB#1 0-A
IOU#7-SCSI#0-FUNC#0	0000:E4:01.0	HDD#0, HDD#1
IOU#7-SCSI#0-FUNC#1	0000:E4:01.1	SCSI port#0
IOU#7-GbE#1-FUNC#0	0000:E6:01.0	To GSWB#0 port#16/GTHB#0 0-B
IOU#7-GbE#1-FUNC#1	0000:E6:01.1	To GSWB#1 port#16/GTHB#1 0-B
IOU#7-SCSI#1-FUNC#0	0000:E7:01.0	HDD#2, HDD#3
IOU#7-SCSI#1-FUNC#1	0000:E7:01.1	SCSI port#1

5.2 Physical Locations and Bus Numbers of Built-in I/Os of PRIMEQUEST 520A/520/420

The following table shows the correspondence between each built-in I/O and its "SEG:BUS:DEV.FUNC" for the PRIMEQUEST 520A/520/420.

The PRIMEQUEST 520A/520/420 supports only PCI Bus mode.

Table 5.3 Correspondence between physical locations and bus numbers of built-in I/Os (PCI Bus mode)

Home-IOU: Either IOU or IOX

Internal I/O	SEG:BUS:DEV.FUNC	Memo
Home-IOU-BMM#0-USB#1	0000:00:1D.1	USB1.1 (Connected to OPL)
Home-IOU-BMM#0-USB#7	0000:00:1D.7	USB2.0 (USB port on the BMM.)
Home-IOU-BMM#0-VGA	0000:01:01.0	VGA
Home-IOU-BMM#0-NIC	0000:01:08.0	Connected to MMB#0
IOU-SCSI#0-FUNC#0	0000:03:01.0	Connected to IOBP (SAS Expander#0)
IOU-GbE#0-FUNC#0	0000:04:01.0	GbE port#0
IOU-GbE#0-FUNC#1	0000:04:01.1	GbE port#1
IOU-SCSI#1-FUNC#0	0000:06:01.0	Connected to IOBP (SAS Expander#1)
IOU-GbE#1-FUNC#0	0000:07:01.0	GbE port#2
IOU-GbE#1-FUNC#1	0000:07:01.1	GbE port#3

5.3 Physical Locations and Bus Numbers of PCI Slots of PRIMEQUEST 580A/540A/580/540/480/440

The following tables show the correspondence between each PCI slot and "SEG:BUS:DEV.FUNC" in PCI Segment mode and PCI Bus mode.

Table 5.4 Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI segment mode)

Classification	Physical location	SEG:BUS:DEV.FUNC		SLOT
IO Unit slot	IOU#0-PCICH#0-FUNC#n	0000:09:01.n	0:9:1.n	0
	IOU#0-PCICH#1-FUNC#n	0000:0B:01.n	0:11:1.n	1
	IOU#0-PCICH#2-FUNC#n	0000:0E:01.n	0:14:1.n	2
	IOU#0-PCICH#3-FUNC#n	0000:10:01.n	0:16:1.n	3
	IOU#1-PCICH#0-FUNC#n	0001:09:01.n	1:9:1.n	16
	IOU#1-PCICH#1-FUNC#n	0001:0B:01.n	1:11:1.n	17
	IOU#1-PCICH#2-FUNC#n	0001:0E:01.n	1:14:1.n	18
	IOU#1-PCICH#3-FUNC#n	0001:10:01.n	1:16:1.n	19
	IOU#2-PCICH#0-FUNC#n	0002:09:01.n	2:9:1.n	32
	IOU#2-PCICH#1-FUNC#n	0002:0B:01.n	2:11:1.n	33
	IOU#2-PCICH#2-FUNC#n	0002:0E:01.n	2:14:1.n	34
	IOU#2-PCICH#3-FUNC#n	0002:10:01.n	2:16:1.n	35
	IOU#3-PCICH#0-FUNC#n	0003:09:01.n	3:9:1.n	48
	IOU#3-PCICH#1-FUNC#n	0003:0B:01.n	3:11:1.n	49
	IOU#3-PCICH#2-FUNC#n	0003:0E:01.n	3:14:1.n	50
	IOU#3-PCICH#3-FUNC#n	0003:10:01.n	3:16:1.n	51
	IOU#4-PCICH#0-FUNC#n	0004:09:01.n	4:9:1.n	64
	IOU#4-PCICH#1-FUNC#n	0004:0B:01.n	4:11:1.n	65
	IOU#4-PCICH#2-FUNC#n	0004:0E:01.n	4:14:1.n	66
	IOU#4-PCICH#3-FUNC#n	0004:10:01.n	4:16:1.n	67
	IOU#5-PCICH#0-FUNC#n	0005:09:01.n	5:9:1.n	80
	IOU#5-PCICH#1-FUNC#n	0005:0B:01.n	5:11:1.n	81
	IOU#5-PCICH#2-FUNC#n	0005:0E:01.n	5:14:1.n	82
	IOU#5-PCICH#3-FUNC#n	0005:10:01.n	5:16:1.n	83
	IOU#6-PCICH#0-FUNC#n	0006:09:01.n	6:9:1.n	96
	IOU#6-PCICH#1-FUNC#n	0006:0B:01.n	6:11:1.n	97
	IOU#6-PCICH#2-FUNC#n	0006:0E:01.n	6:14:1.n	98
	IOU#6-PCICH#3-FUNC#n	0006:10:01.n	6:16:1.n	99
	IOU#7-PCICH#0-FUNC#n	0007:09:01.n	7:9:1.n	112
	IOU#7-PCICH#1-FUNC#n	0007:0B:01.n	7:11:1.n	113
	IOU#7-PCICH#2-FUNC#n	0007:0E:01.n	7:14:1.n	114
	IOU#7-PCICH#3-FUNC#n	0007:10:01.n	7:16:1.n	115

Classification	PCI_Box interface name (PCI slot number)	SEG:BUS:DEV.FUNC		SLOT
PCI_Box/ PCIU	IOU#0-CH#0(Slot#0)	0000:13:01.n	0:19:1.n	4
	IOU#0-CH#0(Slot#1)	0000:15:01.n	0:21:1.n	5
	IOU#0-CH#0(Slot#2)	0000:15:02.n	0:21:2.n	6
	IOU#0-CH#1(Slot#0)	0000:19:01.n	0:25:1.n	7
	IOU#0-CH#1(Slot#1)	0000:1B:01.n	0:27:1.n	8
	IOU#0-CH#1(Slot#2)	0000:1B:02.n	0:27:2.n	9
	IOU#0-CH#2(Slot#0)	0000:1F:01.n	0:31:1.n	10
	IOU#0-CH#2(Slot#1)	0000:21:01.n	0:33:1.n	11
	IOU#0-CH#2(Slot#2)	0000:21:02.n	0:33:2.n	12
	IOU#0-CH#3(Slot#0)	0000:25:01.n	0:37:1.n	13
	IOU#0-CH#3(Slot#1)	0000:27:01.n	0:39:1.n	14
	IOU#0-CH#3(Slot#2)	0000:27:02.n	0:39:2.n	15
	IOU#1-CH#0(Slot#0)	0001:13:01.n	1:19:1.n	20
	IOU#1-CH#0(Slot#1)	0001:15:01.n	1:21:1.n	21
	IOU#1-CH#0(Slot#2)	0001:15:02.n	1:21:2.n	22
	IOU#1-CH#1(Slot#0)	0001:19:01.n	1:25:1.n	23
	IOU#1-CH#1(Slot#1)	0001:1B:01.n	1:27:1.n	24
	IOU#1-CH#1(Slot#2)	0001:1B:02.n	1:27:2.n	25
	IOU#1-CH#2(Slot#0)	0001:1F:01.n	1:31:1.n	26
	IOU#1-CH#2(Slot#1)	0001:21:01.n	1:33:1.n	27
	IOU#1-CH#2(Slot#2)	0001:21:02.n	1:33:2.n	28
	IOU#1-CH#3(Slot#0)	0001:25:01.n	1:37:1.n	29
	IOU#1-CH#3(Slot#1)	0001:27:01.n	1:39:1.n	30
	IOU#1-CH#3(Slot#2)	0001:27:02.n	1:39:2.n	31
	IOU#2-CH#0(Slot#0)	0002:13:01.n	2:19:1.n	36
	IOU#2-CH#0(Slot#1)	0002:15:01.n	2:21:1.n	37
	IOU#2-CH#0(Slot#2)	0002:15:02.n	2:21:2.n	38
	IOU#2-CH#1(Slot#0)	0002:19:01.n	2:25:1.n	39
	IOU#2-CH#1(Slot#1)	0002:1B:01.n	2:27:1.n	40
	IOU#2-CH#1(Slot#2)	0002:1B:02.n	2:27:2.n	41
	IOU#2-CH#2(Slot#0)	0002:1F:01.n	2:31:1.n	42
	IOU#2-CH#2(Slot#1)	0002:21:01.n	2:33:1.n	43
	IOU#2-CH#2(Slot#2)	0002:21:02.n	2:33:2.n	44
	IOU#2-CH#3(Slot#0)	0002:25:01.n	2:37:1.n	45
	IOU#2-CH#3(Slot#1)	0002:27:01.n	2:39:1.n	46
	IOU#2-CH#3(Slot#2)	0002:27:02.n	2:39:2.n	47
	IOU#3-CH#0(Slot#0)	0003:13:01.n	3:19:1.n	52
	IOU#3-CH#0(Slot#1)	0003:15:01.n	3:21:1.n	53
	IOU#3-CH#0(Slot#2)	0003:15:02.n	3:21:2.n	54
	IOU#3-CH#1(Slot#0)	0003:19:01.n	3:25:1.n	55
	IOU#3-CH#1(Slot#1)	0003:1B:01.n	3:27:1.n	56
	IOU#3-CH#1(Slot#2)	0003:1B:02.n	3:27:2.n	57

Classification	PCI_Box interface name (PCI slot number)	SEG:BUS:DEV.FUNC		SLOT
PCI_Box/ PCIU	IOU#3-CH#2(Slot#0)	0003:1F:01.n	3:31:1.n	58
	IOU#3-CH#2(Slot#1)	0003:21:01.n	3:33:1.n	59
	IOU#3-CH#2(Slot#2)	0003:21:02.n	3:33:2.n	60
	IOU#3-CH#3(Slot#0)	0003:25:01.n	3:37:1.n	61
	IOU#3-CH#3(Slot#1)	0003:27:01.n	3:39:1.n	62
	IOU#3-CH#3(Slot#2)	0003:27:02.n	3:39:2.n	63
	IOU#4-CH#0(Slot#0)	0004:13:01.n	4:19:1.n	68
	IOU#4-CH#0(Slot#1)	0004:15:01.n	4:21:1.n	69
	IOU#4-CH#0(Slot#2)	0004:15:02.n	4:21:2.n	70
	IOU#4-CH#1(Slot#0)	0004:19:01.n	4:25:1.n	71
	IOU#4-CH#1(Slot#1)	0004:1B:01.n	4:27:1.n	72
	IOU#4-CH#1(Slot#2)	0004:1B:02.n	4:27:2.n	73
	IOU#4-CH#2(Slot#0)	0004:1F:01.n	4:31:1.n	74
	IOU#4-CH#2(Slot#1)	0004:21:01.n	4:33:1.n	75
	IOU#4-CH#2(Slot#2)	0004:21:02.n	4:33:2.n	76
	IOU#4-CH#3(Slot#0)	0004:25:01.n	4:37:1.n	77
	IOU#4-CH#3(Slot#1)	0004:27:01.n	4:39:1.n	78
	IOU#4-CH#3(Slot#2)	0004:27:02.n	4:39:2.n	79
	IOU#5-CH#0(Slot#0)	0005:13:01.n	5:19:1.n	84
	IOU#5-CH#0(Slot#1)	0005:15:01.n	5:21:1.n	85
	IOU#5-CH#0(Slot#2)	0005:15:02.n	5:21:2.n	86
	IOU#5-CH#1(Slot#0)	0005:19:01.n	5:25:1.n	87
	IOU#5-CH#1(Slot#1)	0005:1B:01.n	5:27:1.n	88
	IOU#5-CH#1(Slot#2)	0005:1B:02.n	5:27:2.n	89
	IOU#5-CH#2(Slot#0)	0005:1F:01.n	5:31:1.n	90
	IOU#5-CH#2(Slot#1)	0005:21:01.n	5:33:1.n	91
	IOU#5-CH#2(Slot#2)	0005:21:02.n	5:33:2.n	92
	IOU#5-CH#3(Slot#0)	0005:25:01.n	5:37:1.n	93
	IOU#5-CH#3(Slot#1)	0005:27:01.n	5:39:1.n	94
	IOU#5-CH#3(Slot#2)	0005:27:02.n	5:39:2.n	95
	IOU#6-CH#0(Slot#0)	0006:13:01.n	6:19:1.n	100
	IOU#6-CH#0(Slot#1)	0006:15:01.n	6:21:1.n	101
	IOU#6-CH#0(Slot#2)	0006:15:02.n	6:21:2.n	102
	IOU#6-CH#1(Slot#0)	0006:19:01.n	6:25:1.n	103
	IOU#6-CH#1(Slot#1)	0006:1B:01.n	6:27:1.n	104
	IOU#6-CH#1(Slot#2)	0006:1B:02.n	6:27:2.n	105
	IOU#6-CH#2(Slot#0)	0006:1F:01.n	6:31:1.n	106
	IOU#6-CH#2(Slot#1)	0006:21:01.n	6:33:1.n	107
	IOU#6-CH#2(Slot#2)	0006:21:02.n	6:33:2.n	108
	IOU#6-CH#3(Slot#0)	0006:25:01.n	6:37:1.n	109
	IOU#6-CH#3(Slot#1)	0006:27:01.n	6:39:1.n	110
	IOU#6-CH#3(Slot#2)	0006:27:02.n	6:39:2.n	111
	IOU#7-CH#0(Slot#0)	0007:13:01.n	7:19:1.n	116

Classification	PCI_Box interface name (PCI slot number)	SEG:BUS:DEV.FUNC		SLOT
PCI_Box	IOU#7-CH#0(Slot#1)	0007:15:01.n	7:21:1.n	117
	IOU#7-CH#0(Slot#2)	0007:15:02.n	7:21:2.n	118
	IOU#7-CH#1(Slot#0)	0007:19:01.n	7:25:1.n	119
	IOU#7-CH#1(Slot#1)	0007:1B:01.n	7:27:1.n	120
	IOU#7-CH#1(Slot#2)	0007:1B:02.n	7:27:2.n	121
	IOU#7-CH#2(Slot#0)	0007:1F:01.n	7:31:1.n	122
	IOU#7-CH#2(Slot#1)	0007:21:01.n	7:33:1.n	123
	IOU#7-CH#2(Slot#2)	0007:21:02.n	7:33:2.n	124
	IOU#7-CH#3(Slot#0)	0007:25:01.n	7:37:1.n	125
	IOU#7-CH#3(Slot#1)	0007:27:01.n	7:39:1.n	126
	IOU#7-CH#3(Slot#2)	0007:27:02.n	7:39:2.n	127
PCI_Box/ PEXU	IOU#0-CH#0,1(Slot#0)	0000:14:00.n	0:20:0.n	4
	IOU#0-CH#0,1(Slot#1)	0000:16:00.n	0:22:0.n	5
	IOU#0-CH#2,3(Slot#0)	0000:20:00.n	0:32:0.n	10
	IOU#0-CH#2,3(Slot#1)	0000:22:00.n	0:34:0.n	11
	IOU#1-CH#0,1(Slot#0)	0001:14:00.n	1:20:0.n	20
	IOU#1-CH#0,1(Slot#1)	0001:16:00.n	1:22:0.n	21
	IOU#1-CH#2,3(Slot#0)	0001:20:00.n	1:32:0.n	26
	IOU#1-CH#2,3(Slot#1)	0001:22:00.n	1:34:0.n	27
	IOU#2-CH#0,1(Slot#0)	0002:14:00.n	2:20:0.n	36
	IOU#2-CH#0,1(Slot#1)	0002:16:00.n	2:22:0.n	37
	IOU#2-CH#2,3(Slot#0)	0002:20:00.n	2:32:0.n	42
	IOU#2-CH#2,3(Slot#1)	0002:22:00.n	2:34:0.n	43
	IOU#3-CH#0,1(Slot#0)	0003:14:00.n	3:20:0.n	52
	IOU#3-CH#0,1(Slot#1)	0003:16:00.n	3:22:0.n	53
	IOU#3-CH#2,3(Slot#0)	0003:20:00.n	3:32:0.n	58
	IOU#3-CH#2,3(Slot#1)	0003:22:00.n	3:34:0.n	59
	IOU#4-CH#0,1(Slot#0)	0004:14:00.n	4:20:0.n	68
	IOU#4-CH#0,1(Slot#1)	0004:16:00.n	4:22:0.n	69
	IOU#4-CH#2,3(Slot#0)	0004:20:00.n	4:32:0.n	74
	IOU#4-CH#2,3(Slot#1)	0004:22:00.n	4:34:0.n	75
	IOU#5-CH#0,1(Slot#0)	0005:14:00.n	5:20:0.n	84
	IOU#5-CH#0,1(Slot#1)	0005:16:00.n	5:22:0.n	85
	IOU#5-CH#2,3(Slot#0)	0005:20:00.n	5:32:0.n	90
	IOU#5-CH#2,3(Slot#1)	0005:22:00.n	5:34:0.n	91
	IOU#6-CH#0,1(Slot#0)	0006:14:00.n	6:20:0.n	100
	IOU#6-CH#0,1(Slot#1)	0006:16:00.n	6:22:0.n	101
	IOU#6-CH#2,3(Slot#0)	0006:20:00.n	6:32:0.n	106
	IOU#6-CH#2,3(Slot#1)	0006:22:00.n	6:34:0.n	107
	IOU#7-CH#0,1(Slot#0)	0007:14:00.n	7:20:0.n	116
	IOU#7-CH#0,1(Slot#1)	0007:16:00.n	7:22:0.n	117
	IOU#7-CH#2,3(Slot#0)	0007:20:00.n	7:32:0.n	122
	IOU#7-CH#2,3(Slot#1)	0007:22:00.n	7:34:0.n	123

Remarks:

- The PCI_Box part of the table shows the relationship between PCI_Box interface names in IO Units and slot numbers.

Each PCI slot number in () corresponds to a slot number (PCICS#) in a PCI_Box/PCIU connected to a PCI_Box interface or a slot number (PEXUS#) in a PCI_Box/PEXU connected to a PCI_Box interface.

Example:

PCI_Box#1 - PCIU#2 is connected to IOU#5 - CH#2.

The slot number of the card in PCI_Box#1 - PCIU#2 - PCICS#1 is 91.

- "n" indicates the function number.

Table 5.5 Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI Bus mode)

Classification	Physical location	SEG:BUS:DEV.FUNC		SLOT
IO Unit slot	IOU#0-PCICH#0-FUNC#n	0000:09:01.n	0:9:1.n	0
	IOU#0-PCICH#1-FUNC#n	0000:0B:01.n	0:11:1.n	1
	IOU#0-PCICH#2-FUNC#n	0000:0E:01.n	0:14:1.n	2
	IOU#0-PCICH#3-FUNC#n	0000:10:01.n	0:16:1.n	3
	IOU#1-PCICH#0-FUNC#n	0000:29:01.n	0:41:1.n	16
	IOU#1-PCICH#1-FUNC#n	0000:2B:01.n	0:43:1.n	17
	IOU#1-PCICH#2-FUNC#n	0000:2E:01.n	0:46:1.n	18
	IOU#1-PCICH#3-FUNC#n	0000:30:01.n	0:48:1.n	19
	IOU#2-PCICH#0-FUNC#n	0000:49:01.n	0:73:1.n	32
	IOU#2-PCICH#1-FUNC#n	0000:4B:01.n	0:75:1.n	33
	IOU#2-PCICH#2-FUNC#n	0000:4E:01.n	0:78:1.n	34
	IOU#2-PCICH#3-FUNC#n	0000:50:01.n	0:80:1.n	35
	IOU#3-PCICH#0-FUNC#n	0000:69:01.n	0:105:1.n	48
	IOU#3-PCICH#1-FUNC#n	0000:6B:01.n	0:107:1.n	49
	IOU#3-PCICH#2-FUNC#n	0000:6E:01.n	0:110:1.n	50
	IOU#3-PCICH#3-FUNC#n	0000:70:01.n	0:112:1.n	51
	IOU#4-PCICH#0-FUNC#n	0000:89:01.n	0:137:1.n	64
	IOU#4-PCICH#1-FUNC#n	0000:8B:01.n	0:139:1.n	65
	IOU#4-PCICH#2-FUNC#n	0000:8E:01.n	0:142:1.n	66
	IOU#4-PCICH#3-FUNC#n	0000:90:01.n	0:144:1.n	67
	IOU#5-PCICH#0-FUNC#n	0000:A9:01.n	0:169:1.n	80
	IOU#5-PCICH#1-FUNC#n	0000:AB:01.n	0:171:1.n	81
	IOU#5-PCICH#2-FUNC#n	0000:AE:01.n	0:174:1.n	82
	IOU#5-PCICH#3-FUNC#n	0000:B0:01.n	0:176:1.n	83
	IOU#6-PCICH#0-FUNC#n	0000:C9:01.n	0:201:1.n	96
	IOU#6-PCICH#1-FUNC#n	0000:CB:01.n	0:203:1.n	97
	IOU#6-PCICH#2-FUNC#n	0000:CE:01.n	0:206:1.n	98
	IOU#6-PCICH#3-FUNC#n	0000:D0:01.n	0:208:1.n	99
	IOU#7-PCICH#0-FUNC#n	0000:E9:01.n	0:233:1.n	112
	IOU#7-PCICH#1-FUNC#n	0000:EB:01.n	0:235:1.n	113
	IOU#7-PCICH#2-FUNC#n	0000:EE:01.n	0:238:1.n	114
	IOU#7-PCICH#3-FUNC#n	0000:F0:01.n	0:240:1.n	115

Classification	PCI_Box interface name (PCI slot number)	SEG:BUS:DEV.FUNC		SLOT
PCI_Box/ PCIU	IOU#0-CH#0(Slot#0)	0000:13:01.n	0:19:1.n	4
	IOU#0-CH#0(Slot#1)	0000:15:01.n	0:21:1.n	5
	IOU#0-CH#0(Slot#2)	0000:15:02.n	0:21:2.n	6
	IOU#0-CH#1(Slot#0)	0000:19:01.n	0:25:1.n	7
	IOU#0-CH#1(Slot#1)	0000:1B:01.n	0:27:1.n	8
	IOU#0-CH#1(Slot#2)	0000:1B:02.n	0:27:2.n	9
	IOU#1-CH#0(Slot#0)	0000:33:01.n	0:51:1.n	20
	IOU#1-CH#0(Slot#1)	0000:35:01.n	0:53:1.n	21
	IOU#1-CH#0(Slot#2)	0000:35:02.n	0:53:2.n	22
	IOU#1-CH#1(Slot#0)	0000:39:01.n	0:57:1.n	23
	IOU#1-CH#1(Slot#1)	0000:3B:01.n	0:59:1.n	24
	IOU#1-CH#1(Slot#2)	0000:3B:02.n	0:59:2.n	25
	IOU#2-CH#0(Slot#0)	0000:53:01.n	0:83:1.n	36
	IOU#2-CH#0(Slot#1)	0000:55:01.n	0:85:1.n	37
	IOU#2-CH#0(Slot#2)	0000:55:02.n	0:85:2.n	38
	IOU#2-CH#1(Slot#0)	0000:59:01.n	0:89:1.n	39
	IOU#2-CH#1(Slot#1)	0000:5B:01.n	0:91:1.n	40
	IOU#2-CH#1(Slot#2)	0000:5B:02.n	0:91:2.n	41
	IOU#3-CH#0(Slot#0)	0000:73:01.n	0:115:1.n	52
	IOU#3-CH#0(Slot#1)	0000:75:01.n	0:117:1.n	53
	IOU#3-CH#0(Slot#2)	0000:75:02.n	0:117:2.n	54
	IOU#3-CH#1(Slot#0)	0000:79:01.n	0:121:1.n	55
	IOU#3-CH#1(Slot#1)	0000:7B:01.n	0:123:1.n	56
	IOU#3-CH#1(Slot#2)	0000:7B:02.n	0:123:2.n	57
	IOU#4-CH#0(Slot#0)	0000:93:01.n	0:147:1.n	68
	IOU#4-CH#0(Slot#1)	0000:95:01.n	0:149:1.n	69
	IOU#4-CH#0(Slot#2)	0000:95:02.n	0:149:2.n	70
	IOU#4-CH#1(Slot#0)	0000:99:01.n	0:153:1.n	71
	IOU#4-CH#1(Slot#1)	0000:9B:01.n	0:155:1.n	72
	IOU#4-CH#1(Slot#2)	0000:9B:02.n	0:155:2.n	73
	IOU#5-CH#0(Slot#0)	0000:B3:01.n	0:179:1.n	84
	IOU#5-CH#0(Slot#1)	0000:B5:01.n	0:181:1.n	85
	IOU#5-CH#0(Slot#2)	0000:B5:02.n	0:181:2.n	86
	IOU#5-CH#1(Slot#0)	0000:B9:01.n	0:185:1.n	87
	IOU#5-CH#1(Slot#1)	0000:BB:01.n	0:187:1.n	88
	IOU#5-CH#1(Slot#2)	0000:BB:02.n	0:187:2.n	89
	IOU#6-CH#0(Slot#0)	0000:D3:01.n	0:211:1.n	100
	IOU#6-CH#0(Slot#1)	0000:D5:01.n	0:213:1.n	101
	IOU#6-CH#0(Slot#2)	0000:D5:02.n	0:213:2.n	102

Classification	PCI_Box interface name (PCI slot number)	SEG:BUS:DEV.FUNC		SLOT
PCI_Box/ PCIU	IOU#6-CH#1(Slot#0)	0000:D9:01.n	0:217:1.n	103
	IOU#6-CH#1(Slot#1)	0000:DB:01.n	0:219:1.n	104
	IOU#6-CH#1(Slot#2)	0000:DB:02.n	0:219:2.n	105
	IOU#7-CH#0(Slot#0)	0000:F3:01.n	0:243:1.n	116
	IOU#7-CH#0(Slot#1)	0000:F5:01.n	0:245:1.n	117
	IOU#7-CH#0(Slot#2)	0000:F5:02.n	0:245:2.n	118
	IOU#7-CH#1(Slot#0)	0000:F9:01.n	0:249:1.n	119
	IOU#7-CH#1(Slot#1)	0000:FB:01.n	0:251:1.n	120
	IOU#7-CH#1(Slot#2)	0000:FB:02.n	0:251:2.n	121
PCI_Box/ PEXU	IOU#0-CH#0,1(Slot#0)	0000:14:00.n	0:20:0.n	4
	IOU#0-CH#0,1(Slot#1)	0000:16:00.n	0:32:0.n	5
	IOU#1-CH#0,1(Slot#0)	0000:34:00.n	0:52:0.n	20
	IOU#1-CH#0,1(Slot#1)	0000:36:00.n	0:54:0.n	21
	IOU#2-CH#0,1(Slot#0)	0000:54:00.n	0:84:0.n	36
	IOU#2-CH#0,1(Slot#1)	0000:56:00.n	0:86:0.n	37
	IOU#3-CH#0,1(Slot#0)	0000:74:00.n	0:116:0.n	52
	IOU#3-CH#0,1(Slot#1)	0000:76:00.n	0:118:0.n	53
	IOU#4-CH#0,1(Slot#0)	0000:94:00.n	0:148:0.n	68
	IOU#4-CH#0,1(Slot#1)	0000:96:00.n	0:150:0.n	69
	IOU#5-CH#0,1(Slot#0)	0000:B4:00.n	0:180:0.n	84
	IOU#5-CH#0,1(Slot#1)	0000:B6:00.n	0:182:0.n	85
	IOU#6-CH#0,1(Slot#0)	0000:D4:00.n	0:212:0.n	100
	IOU#6-CH#0,1(Slot#1)	0000:D6:00.n	0:214:0.n	101
	IOU#7-CH#0,1(Slot#0)	0000:F4:00.n	0:244:0.n	116
	IOU#7-CH#0,1(Slot#1)	0000:F6:00.n	0:246:0.n	117

Remarks:

- The PCI_Box part of the table shows the relationship between PCI_Box interface names in IO Units and slot numbers.

Each PCI slot number in () corresponds to a slot number (PCICS#) in a PCI_Box/PCIU connected to a PCI_Box interface or a slot number (PEXUS#) in a PCI_Box/PEXU connected to a PCI_Box interface.

Example:

PCI_Box#1 - PCIU#2 is connected to IOU#5 - CH#1.

The slot number of the card in PCI_Box#1 - PCIU#2 - PCICS#1 is 88.

- "n" indicates the function number.

5.4 Physical Locations and Bus Numbers of PCI Slots of PRIMEQUEST 520A/520/420

Table 5.6 Relationship between physical mounting locations and bus numbers in PRIMEQUEST-series machines (PCI Bus mode)

Classification	Physical location	SEG:BUS:DEV.FUNC		SLOT
IO Unit slot	IOU-PCIC#0-FUNC#n	0000:0A:00.n	0:10:0.n	0
	IOU-PCIC#1-FUNC#n	0000:0C:00.n	0:12:0.n	1
	IOU-PCIC#2-FUNC#n	0000:16:00.n	0:22:0.n	2
	IOU-PCIC#3-FUNC#n	0000:18:00.n	0:24:0.n	3
	IOU-PCIC#4-FUNC#n	0000:21:01.n	0:33:1.n	4
	IOU-PCIC#5-FUNC#n	0000:23:01.n	0:35:1.n	5
	IOU-PCIC#6-FUNC#n	0000:27:01.n	0:39:1.n	6
	IOU-PCIC#7-FUNC#n	0000:29:01.n	0:41:1.n	7
PCI_Box/PCIU	IOX-CH#0(Slot#0)	0000:49:01.n	0:73:1.n	16
	IOX-CH#0(Slot#1)	0000:4B:01.n	0:75:1.n	17
	IOX-CH#0(Slot#2)	0000:4B:02.n	0:75:2.n	18
	IOX-CH#1(Slot#0)	0000:4F:01.n	0:79:1.n	19
	IOX-CH#1(Slot#1)	0000:51:01.n	0:81:1.n	20
	IOX-CH#1(Slot#2)	0000:51:02.n	0:81:2.n	21
	IOX-CH#2(Slot#0)	0000:55:01.n	0:85:1.n	22
	IOX-CH#2(Slot#1)	0000:57:01.n	0:87:1.n	23
	IOX-CH#2(Slot#2)	0000:57:02.n	0:87:2.n	24
	IOX-CH#3(Slot#0)	0000:5B:01.n	0:91:1.n	25
	IOX-CH#3(Slot#1)	0000:5D:01.n	0:93:1.n	26
	IOX-CH#3(Slot#2)	0000:5D:02.n	0:93:2.n	27
PCI_Box/PEXU	IOX-CH#0,1(Slot#0)	0000:4A:00.n	0:74:0.n	16
	IOX-CH#0,1(Slot#1)	0000:4C:00.n	0:76:0.n	17
	IOX-CH#2,3(Slot#0)	0000:56:00.n	0:86:0.n	22
	IOX-CH#2,3(Slot#1)	0000:58:00.n	0:88:0.n	23

Remarks:

- The PCI_Box part of the table shows the relationship between PCI_Box interface names in IOXs and slot numbers. Each PCI slot number in () corresponds to a slot number (PCICS#) in a PCI_Box/PCIU connected to a PCI_Box interface or a slot number (PEXUS#) in a PCI_Box/PEXU connected to a PCI_Box interface.
Example:
PCI_Box#1 - PCIU#2 is connected to IOX - CH-1. The slot number of the card in PCI_Box#1 - PCIU#2 - PCICS#1 is 20.
- The PRIMEQUEST 520A/520/420 supports only PCI Bus mode.
- "n" indicates the function number.

CHAPTER 6 Management LAN Reconfiguration Required at the Time of BMM Replacement

If the BMM hardware is replaced, the management LAN needs to be reconfigured.

Note: BMM replacement is a Fujitsu certified service engineer task. If BMM replacement is required, contact your Fujitsu certified service engineer before reconfiguring the management LAN.

The management LAN reconfiguration procedure required at the time of BMM replacement varies with the model in use and the operating system installed in the partition. Confirm the correct procedure before starting reconfiguration work.

Red Hat

- For PRIMEQUEST 580A/540A/580/540/480/440 (bonding or GLS sharing) (→ See [6.1.1](#))
- For PRIMEQUEST 520A/520/420 (→ See [6.1.2](#))

SUSE 9

- For PRIMEQUEST 580A/540A/580/540/480/420 (bonding in use) (→ Reconfiguration not required)
- For PRIMEQUEST 580A/540A/580/540/480/420 (GLS in use) (→ See [6.2.2](#))
- For PRIMEQUEST 520A/520/420 (→ See [6.2.3](#))

SUSE 10

Contact your Fujitsu certified service engineer.

Windows Server 2003

- For PRIMEQUEST 580A/540A/580/540/480/440 (→ See [6.3.1](#))
- For PRIMEQUEST 520A/520/420 (→ No reconfiguration required)

6.1 Red Hat

6.1.1 For PRIMEQUEST 580A/540A/580/540/480/440 (bonding or GLS sharing)

- 1 Shut down the partition.
- 2 Check and write down the MAC address of the NIC for the management LAN before replacing the BMM.

As shown in [Figure 6.1](#), the MAC address is displayed as that of BMM#n (NIC#0, NIC#1) in the MMB Web-UI [IOU#X] window ([System] → [IOU] → [IOU#X]).

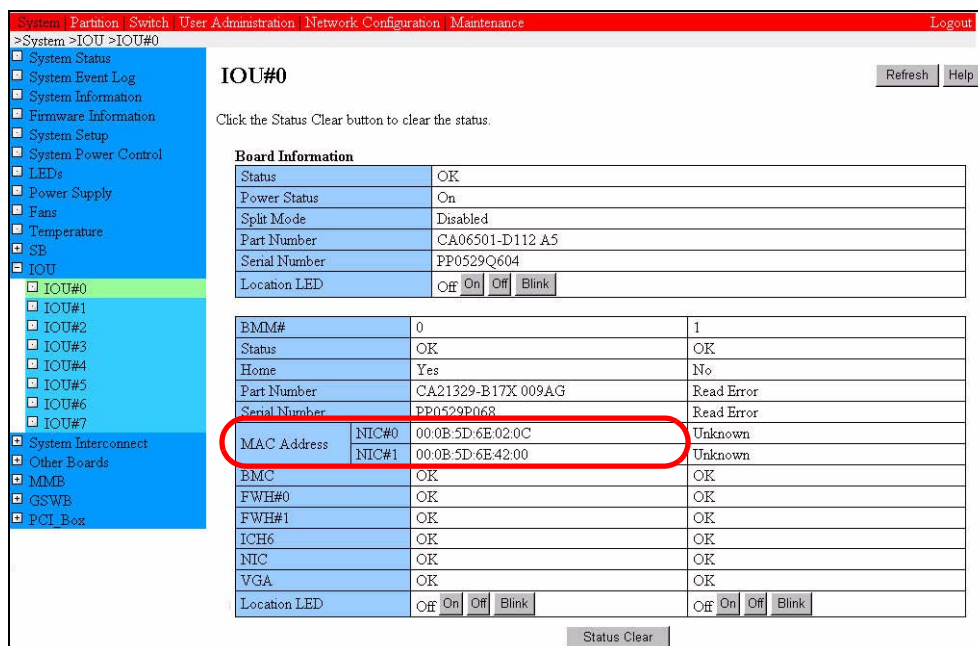


Figure 6.1 [IOU#x] window (PRIMEQUEST 580A/540A/580/540/480/440)

- 3 Replace the BMM.
Note: BMM replacement is a Fujitsu certified service engineer task.
- 4 Start up the partition in single-user mode.
For information on starting up in single-user mode, refer to [6.6, "Notes on Startup in Linux Single-User Mode."](#)

- 5 Search for the two ifcfg files containing the MAC addresses confirmed in step 2. The MAC address is contained in the "HWADDR" section of the ifcfg file. The ifcfg file is located in /etc/sysconfig/network-scripts/ifcfg-eth<N> (where eth<N> is the interface name).

Example: If the interface for the management LAN is eth0:

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

The following line matches the MAC address confirmed in step 2.

```
HWADDR=00:0B:5D:6E:02:0C
```

Example: If the interface for the management LAN is eth1

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
```

The following line matches the MAC address confirmed in step 2.

```
HWADDR=00:0B:5D:6E:42:00
```

- 6 Confirm the new MAC address of the NIC for the management LAN. The MAC address is displayed as that of BMM#n (NIC#0, NIC#1) in the MMB Web-UI [IOU#X] window ([System] → [IOU] → [IOU#X]).
- 7 Using an editor such as vi, change the MAC address in the ifcfg file. Edit the two ifcfg files found in step 5.

Example: If the management LAN NICs are as follows:

Table 6.1 Correspondence between management LAN NICs

ifcfg file	NIC name	Old MAC address	New MAC address
ifcfg-eth0	NIC#1	00:0B:5D:6E:02:0C	00:0B:5D:6E:01:57
ifcfg-eth1	NIC#0	00:0B:5D:6E:42:00	00:0B:5D:6E:01:59

Example: If the management LAN interface is eth0:

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Change the following line:

```
HWADDR=00:0B:5D:6E:02:CC
```

to

```
HWADDR=00:0B:5D:6E:01:57
```

Example: If the management LAN interface is eth1:

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth1
```

Change the following line:

```
HWADDR=00:0B:5D:6E:42:00
```

to

```
HWADDR=00:0B:5D:6E:01:59
```

Note: When the MAC addresses are changed, the relationship between the ifcfg file name and NIC name must be left unchanged. (In the example above, do not write the new MAC address 00:0B:5D:6E:01:59 for NIC#0 in ifcfg-eth0.)

- 8 Reboot the partition.

/sbin/reboot

- 9 At booting, Kudzu might start up. If it does, follow the instructions provided in [6.5, "Action Required When Kudzu Starts Up."](#)

6.1.2 For PRIMEQUEST 520A/520/420

- 1 Shut down the partition.
- 2 Check and write down the MAC address of the NIC for the management LAN before replacing the BMM.

The MAC address is displayed as that of BMM#n in the MMB Web-UI [IOU] window ([System] → [IOU] → [IOU] or [IOX]).

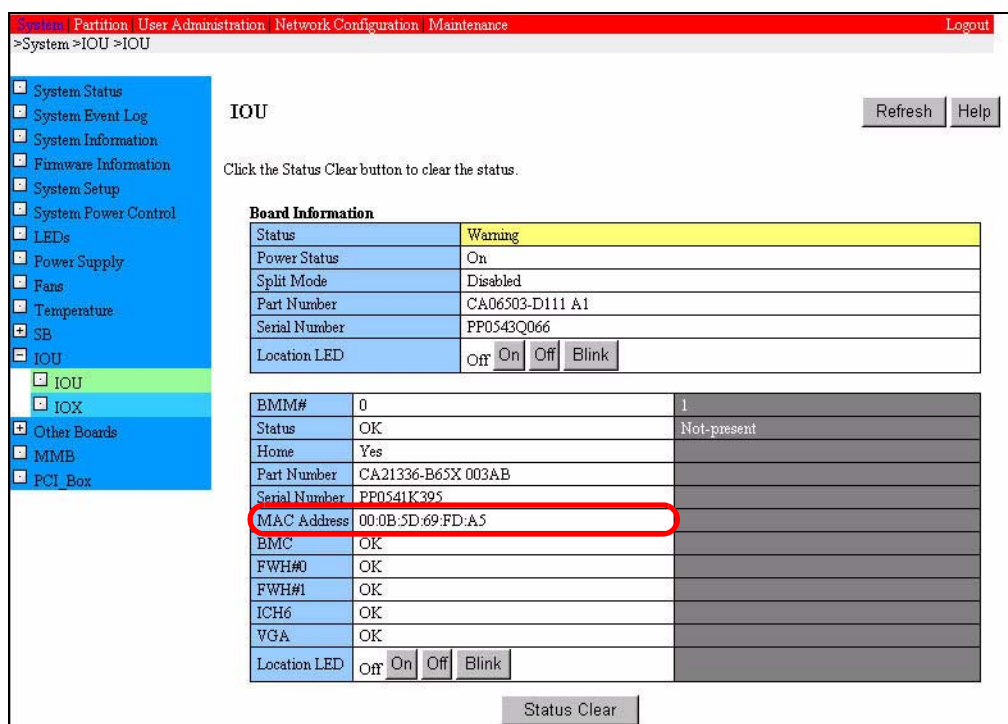


Figure 6.2 IOU/IOX information window (PRIMEQUEST 520A/520/420)

- 3 Replace the BMM
Note: BMM replacement is a Fujitsu certified service engineer task.
- 4 Start up the partition in single-user mode.
For information on starting up in single-user mode, refer to [6.6, "Notes on Startup in Linux Single-User Mode."](#)
- 5 Search for the ifcfg file containing the MAC address confirmed in step 2. The MAC address is contained in the "HWADDR" section of the ifcfg file. The ifcfg file is located in /etc/sysconfig/network-scripts/ifcfg-eth<N> (where eth<N> is the interface name).
Example: If the interface for the management LAN is eth0:

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

The following line matches the MAC address confirmed in step (2).

```
HWADDR=00:0B:5D:69:FD:A5
```

- 6 Confirm the new MAC address of the NIC for the management LAN. The MAC address is displayed as that of BMM#n in the MMB Web-UI [IOU#X] window ([System] → [IOU] or [IOX]).
- 7 On an editor such as vi, change the MAC address in the ifcfg file. Edit the ifcfg file found in step 5.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Change the following line:

```
HWADDR=00:0B:5D:69:FD:A5
```

to

```
HWADDR=00:0B:5D:6F:80:44
```

- 8 Reboot the partition.

```
# /sbin/reboot
```

- 9 At booting, Kudzu might start up. If it does, follow the instructions provided in [6.5, "Action Required When Kudzu Starts Up."](#)

6.2 SUSE 9

6.2.1 For PRIMEQUEST 580A/540A/580/540/480/440 (bonding in use)

Reconfiguration is not required.

6.2.2 For PRIMEQUEST 580A/540A/580/540/480/440 (GLS in use)

- 1 Shut down the partition.
- 2 Check and write down the MAC address of the NIC for the management LAN before replacing the BMM.
As shown in [Figure 6.1](#), the MAC address is displayed as that of BMM#n (NIC#0, NIC#1) in the MMB Web-UI [IOU#X] window ([System] → [IOU] → [IOU#X]).
- 3 Replace the BMM
Note: BMM replacement is a Fujitsu certified service engineer task.
- 4 Start up the partition in single-user mode.
For information on starting up in single-user mode, refer to [6.6, "Notes on Startup in Linux Single-User Mode."](#)
- 5 Search for the two ifcfg files for the management LAN and write down their settings.
The path for the ifcfg file is /etc/sysconfig/network/ifcfg-eth-id-<old-MAC-address>.
- 6 Delete the two files found in step 5.
- 7 Confirm the new MAC address of the management LAN NIC. The MAC address is also displayed as the MAC address (NIC#0, NIC#1) of BMM#n in the MMB Web-UI [IOU#X] window.
- 8 Execute the following command and record the name of the NIC for the management LAN. The bus numbers of the NIC for the management LAN are 0000:01:08.0 and 0000:01:00.0.

Input format:

```
/sbin/lspci -s <Management-LAN-bus-number>
```

Example: In this case, the card name is Intel Corporation 82557/8/9
[Ethernet Pro 100].

```
# /sbin/lspci -s 0000:01:00.0
01:00.0 Ethernet controller: Intel Corporation 82557/8/9
[Ethernet Pro 100] (rev 10)
```

- 9 Activate YaST. From the menu, select [Network Devices] → [Network Card] to go to the network card selection window. In this window, select the card (NIC for the management LAN) with the name confirmed in step 8, reconfigure the settings required, and then exit YaST.

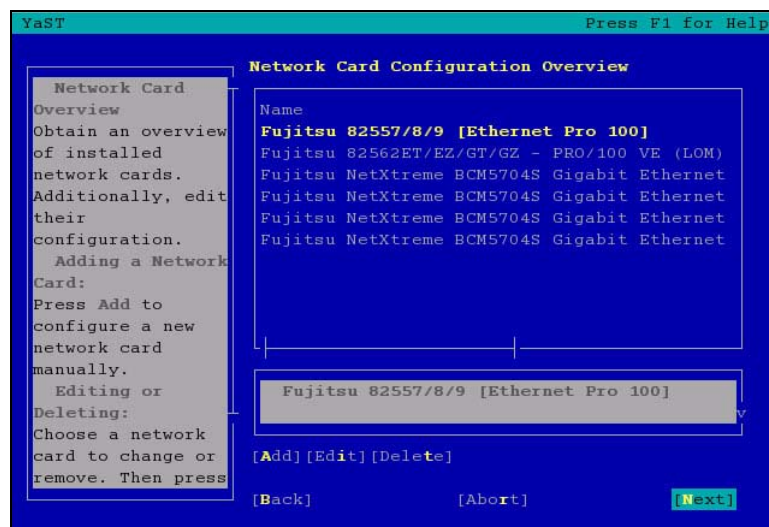


Figure 6.3 Sample screenshot of YaST screen

Note: What is displayed in the above field may not completely match the name confirmed in step 8, may begin with "Fujitsu," and may only be part of the card name depending on the YaST specification. In such a case, select a card if its identification displayed begins with "Fujitsu" and the remaining part matches the name confirmed in step 8.

- 10 Configure settings that cannot be configured in YaST, such as PERSYSTENT_NAME, by directly editing the ifcfg file using an editor or similar method. The path for the ifcfg file is /etc/sysconfig/network/ifcfg-eth-id-<new-MAC-address>.
- 11 Reboot the partition.

```
# /sbin/reboot
```

6.2.3 For PRIMEQUEST 520A/520/420

- 1 Shut down the partition.
- 2 Check and write down the MAC address of the NIC for the management LAN before replacing the BMM.

The MAC address is displayed as that of BMM#n in the MMB Web-UI [IOU] window ([System] → [IOU] → [IOU] or [IOX]).

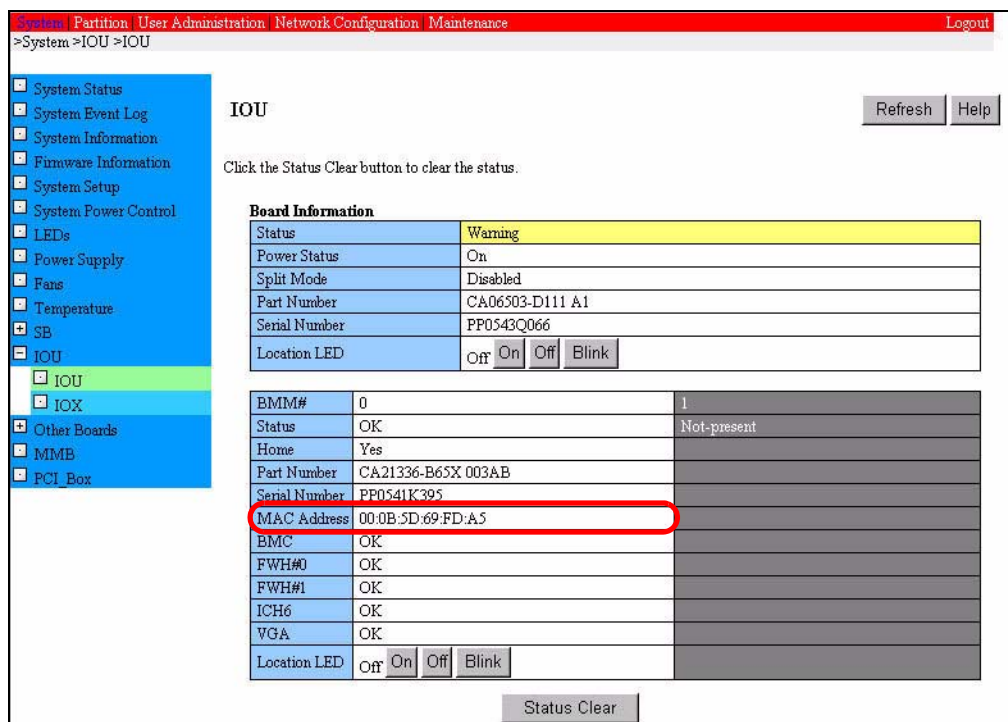


Figure 6.4 [IOU] window (PRIMEQUEST 520A/520/420)

- 3 Replace the BMM.
Note: BMM replacement is a Fujitsu certified service engineer task.
- 4 Start up the partition in single-user mode.
For information on starting up in single-user mode, refer to [6.6, "Notes on Startup in Linux Single-User Mode."](#)
- 5 Search for the ifcfg file for the management LAN and write down the settings.
The path for the ifcfg file is /etc/sysconfig/network/ifcfg-eth-id-<old-MAC-address>.
- 6 Delete the file found in step 5.
- 7 Confirm the new MAC address of the NIC for the management LAN. The MAC address is displayed as that of BMM#n in the MMB Web-UI [IOU] or [IOX] window ([System] → [IOU] → [IOU] or [IOX]).

- 8 Execute the following command and record the name of the NIC for the management LAN. The bus number of the NIC for the management LAN is "0000:01:08.0."

Input format:

```
/sbin/lspci -s <Management-LAN-bus-number>
```

Example: In this case, the card name is Intel Corporation 82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller.

```
# /sbin/lspci -s 0000:01:08.0
0000:01:08.0 Ethernet controller: Intel Corporation 82562ET/EZ/GT/GZ -
PRO/100 VE (LOM) Ethernet Controller (rev 04)
```

- 9 Activate YaST. From the menu, select [Network Devices] → [Network Card] to go to the network card selection window.
In this window, select the card (NIC for the management LAN) with the name confirmed in step 8, reconfigure the settings required, and then exit YaST.
Note: What is displayed in the field may not completely match the name confirmed in step 8, may begin with "Fujitsu," and may only be part of the card name depending on the YaST specification. In such a case, select a card if its identification displayed begins with "Fujitsu" and the remaining part matches the name confirmed in step 8.
- 10 Configure settings that cannot be configured in YaST, such as PERSYSTENT_NAME, by directly editing the ifcfg file using an editor or a similar method. The path for the ifcfg file is /etc/sysconfig/network/ifcfg-eth-id-<new-MAC-address>.
- 11 Reboot the partition.

```
# /sbin/reboot
```


6.3 Windows Server 2003

6.3.1 For PRIMEQUEST 580A/540A/580/540/480/440

Note: This procedure needs to include steps performed to once delete the teaming settings of the management LAN before replacing the BMM and reconfigure the teaming settings after replacing the BMM. When the teaming settings are deleted, the team name, IP address, subnet mask, default gateway, and other settings for the management LAN network interface are deleted. Therefore, obtain a backup copy of these settings before deleting the teaming settings.

Confirming the team name

Select [Control Panel] → [Network Connections] and confirm the team name (example: Team #0) assigned to the management LAN.

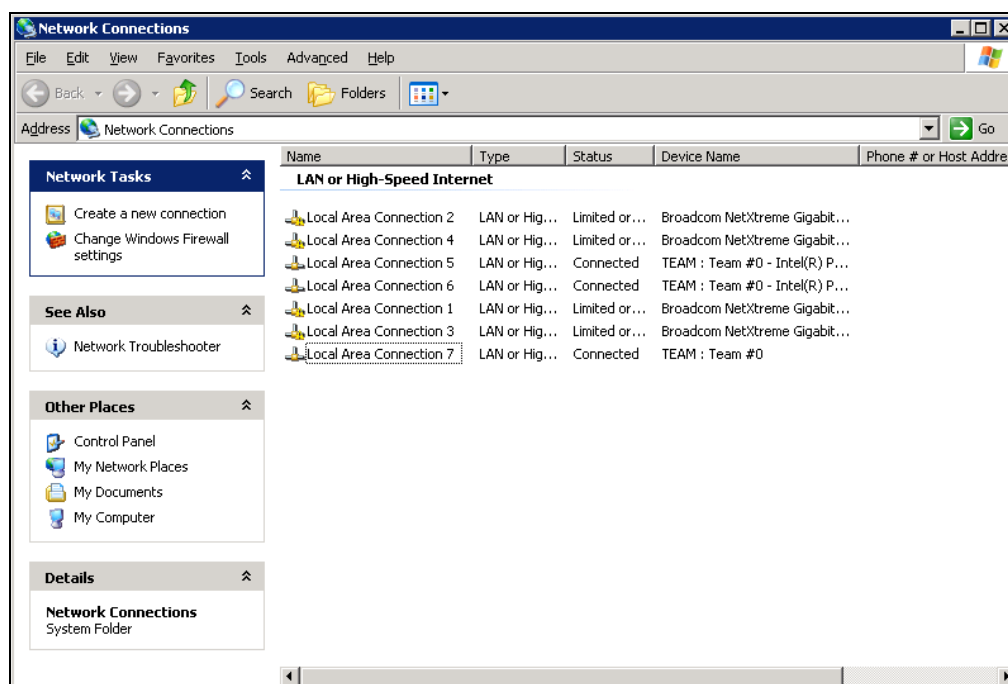


Figure 6.5 Network interface list

Confirming the IP address, subnet mask, default gateway, and other settings

Select the interface that is assigned the management LAN team name, click the right mouse button, and then select [Properties] from the menu.

Select [Internet Protocol (TCP/IP)] and click the [Properties] button. In the [Internet Protocol (TCP/IP) Properties] dialog box, confirm the IP address, subnet mask, default gateway, and other settings.

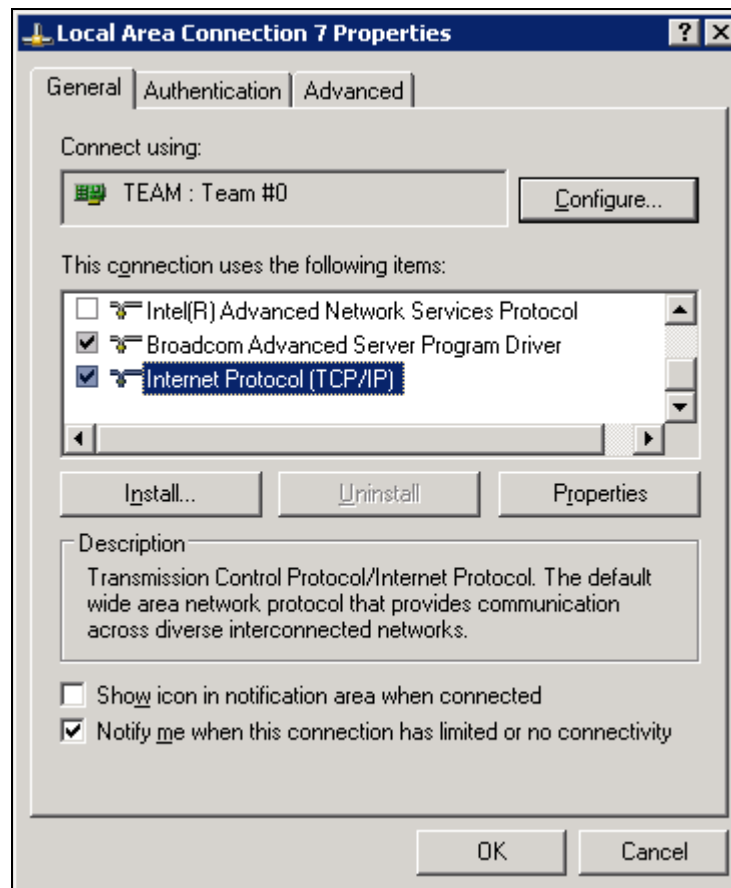


Figure 6.6 [Local Area Connection Properties] dialog box

BMM replacement procedure

- 1 Delete the teaming settings.

Select [Control Panel] → [Administrative Tools] → [Computer Management] → [Device Manager].

- 2 Open [Network adapters] and click the device [TEAM: xxxx] that is assigned to the management LAN team.

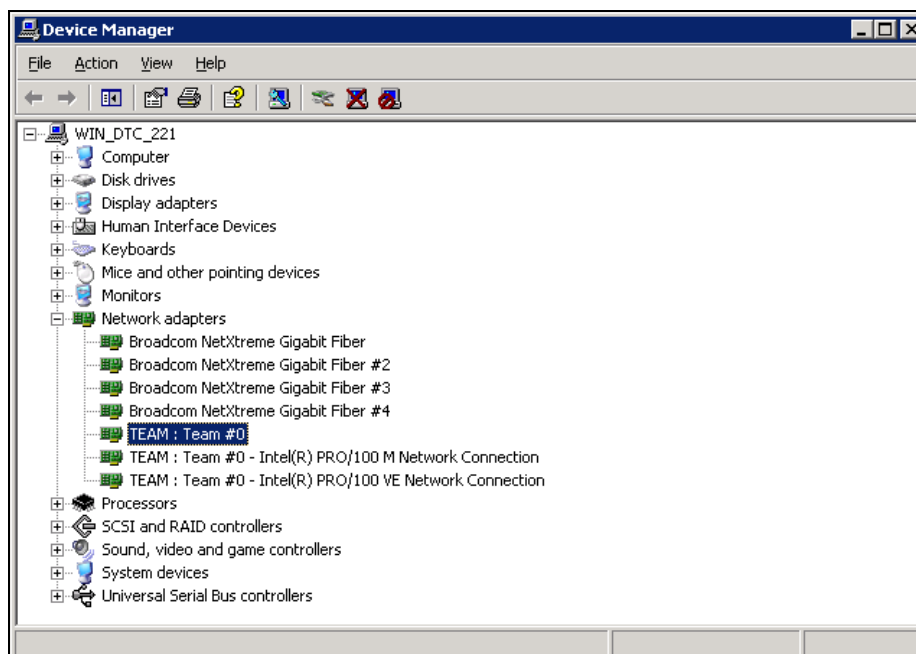


Figure 6.7 [Device Manager] window

- 3 The [TEAM: Team #x Properties] dialog box appears. Click the [Settings] tab and click the [Remove Team] button.

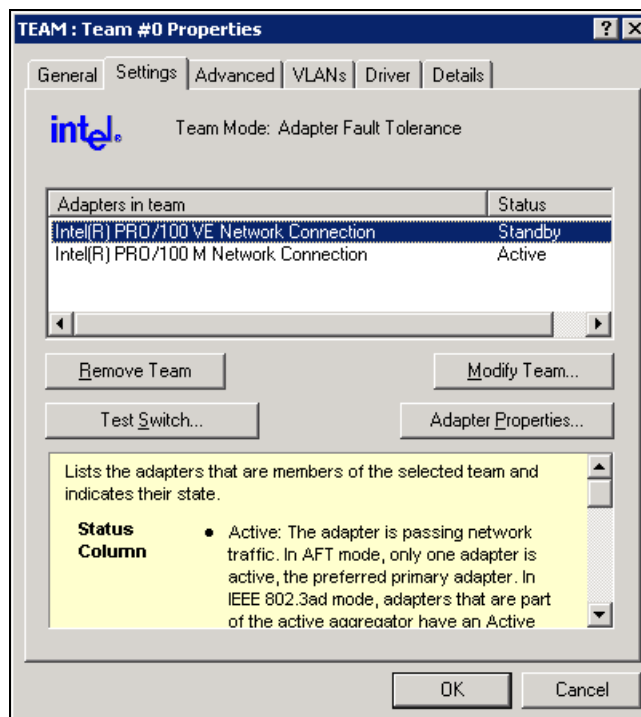


Figure 6.8 [Team #x Properties] dialog box

- 4 A confirmation dialog box appears. Click [Yes].

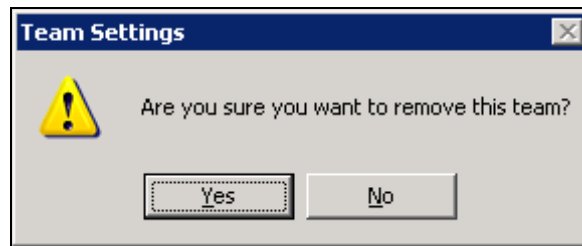


Figure 6.9 [Team Settings] dialog box

- 5 Confirm that the management LAN teaming device (such as Team #0) has been deleted.

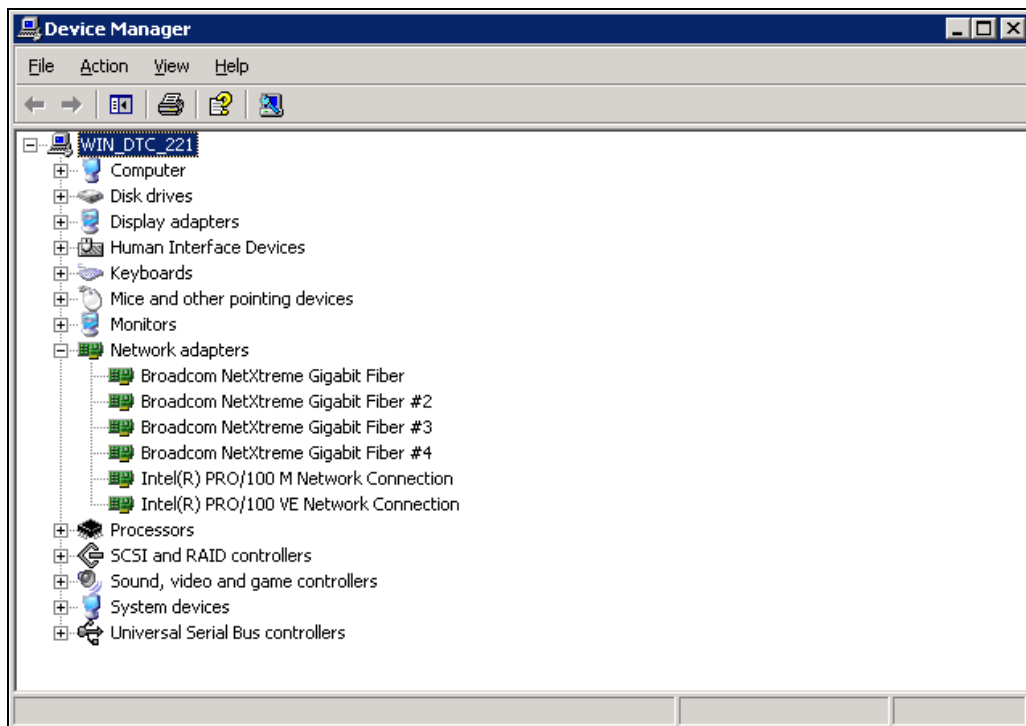


Figure 6.10 [Device Manager] window

- 6 Shut down the partition.
- 7 Replace the BMM.

Note: BMM replacement is a Fujitsu certified service engineer task.

- 8 After replacing the BMM, start up the partition and reconfigure the management LAN teaming settings. For information on the subsequent steps, refer to 4.5, "PSA Installation (Windows Server 2003) (PRIMEQUEST 580A/540A/580/540/480/440)" and Section 4.5.1, "Checking the management LAN settings" in the *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN).
If the network adapter name displayed here in Device Manager is different from that prior to the BMM replacement, restore the original device name by following the steps described in 6.4, ["Procedure for Restoring Settings If the Network Adapter Name Is Changed."](#)

6.3.2 For PRIMEQUEST 520A/520/420

Reconfiguration is not required.

6.4 Procedure for Restoring Settings If the Network Adapter Name Is Changed

When the BMM is replaced, the management LAN interface network adapter name may be changed if the revision of the higher-order device is changed. If it is, perform the following procedure because you may encounter a problem, such as failure in setting IP addresses that were used in the previous environment.

Note:

This setting is required only in Windows.

6.4.1 Confirming the Old Settings

- 1 Select [Start] → [Accessories] → [Command Prompt].
- 2 Enter "set DEVMGR_SHOW_NONPRESENT_DEVICES=1" to set the environment variable and enter "start devmgmt.msc" to activate Device Manager.
- 3 From the [View] menu of Device Manager, select [Show hidden devices].
The unused devices are displayed semitransparently.
- 4 Record the old setting information, including especially the following items:
Number appended to each adapter name, connected bus number, and function number.

6.4.2 Changing the Adapter Names

Perform the following steps related to the items with semitransparently displayed adapter names, starting with adapter names without any appended numbers and proceeding in ascending order of appended numbers.

- 1 Find ordinarily displayed adapter names with the same bus number and function number as those of semitransparently displayed adapter names and delete these pairs once.
- 2 Select [Scan for hardware changes] from the [Action] menu of Device Manager.
This allows you to restore the settings in such a manner that the newly recognized NIC is correctly associated with the slot that has been used so far.
- 3 If necessary, configure individual device properties.

6.5 Action Required When Kudzu Starts Up

In Red Hat, Kudzu may start at the time of a reboot subsequent to reconfiguration. If it does, perform the following steps. Neglecting this instruction may cause your reconfiguration to be deleted and the management LAN to be unusable.

- 1 Press any key when the [Welcome to Kudzu] screen is displayed.



Figure 6.11 [Welcome to Kudzu] screen

- 2 As shown below, select one of the options for the pre-replacement management LAN NIC (first) configuration.
Because the settings have already been changed here, select [Keep Configuration] and proceed.
Remarks: This screen is not displayed in the case of PRIMEQUEST 520A/520/420.



Figure 6.12 [Hardware Removed] screen

- 3 Similarly, select one of the options for the pre-replacement management LAN NIC (second) configuration.
- Because the settings have already been changed here, select [Keep Configuration] and proceed.

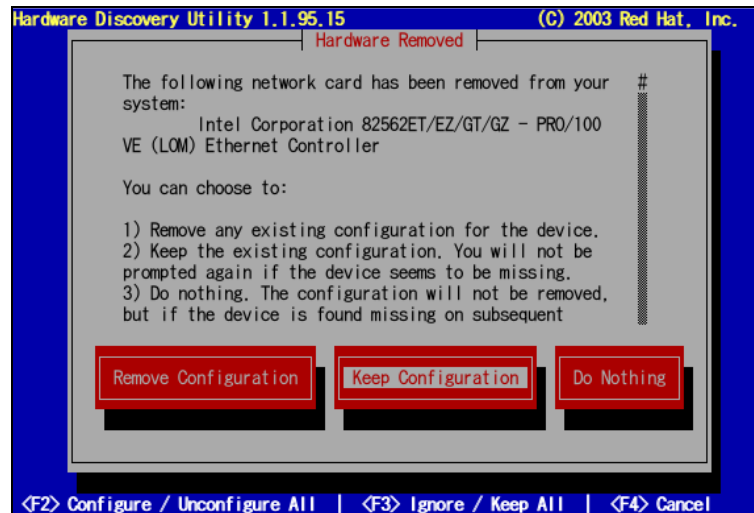


Figure 6.13 [Hardware Removed] screen

- 4 As shown below, select one of the options for the post-replacement management LAN NIC (first) configuration.
- Because the settings have already been changed here, select [Ignore] and proceed.
- Remarks: This screen is not displayed in the case of PRIMEQUEST 520A/520/420.

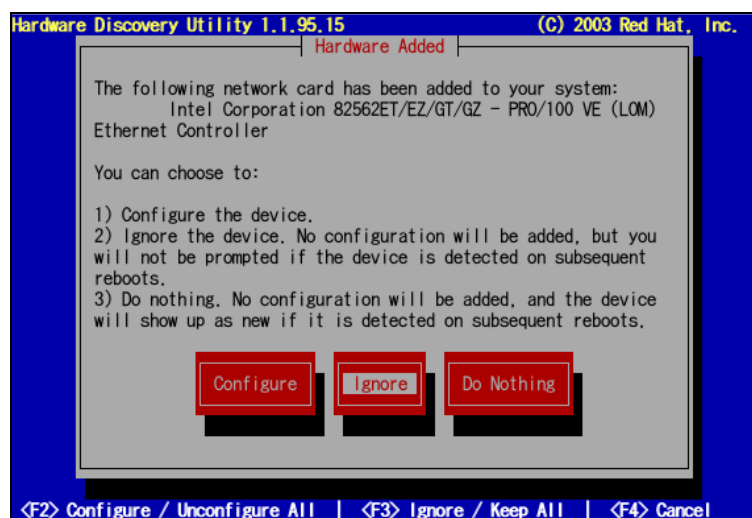


Figure 6.14 [Hardware Added] screen

- 5 Similarly, select one of the options for the post-replacement management LAN NIC (second) configuration.
Because the settings have already been changed here, select [Ignore] and proceed.



Figure 6.15 [Hardware Added] screen

6.6 Notes on Startup in Linux Single-User Mode

Similar to Red Hat SUSE, when you start up the partition in Linux single-user mode, be sure to specify the boot command line options `single` and `rw`. The meanings of these options are as follows:

Table 6.2 Explanation of boot command line options

Option	Meaning
<code>single</code>	Startup in single-user mode
<code>rw</code>	Root disk mounting in read/write mode

Note: If you do not specify the `rw` option, the root disk may be mounted in read-only mode. Note that this disables you from performing some operations in single-user mode.

Usage example: If the boot image name is "linux":

```
ELILO boot : linux single rw
```


CHAPTER 7 REMCS

7.1 Use of REMCS Service

This appendix provides an outline of the REMCS service. A certified service engineer configures the settings for using the REMCS service.

7.1.1 Mode of connection to the REMCS Center

The mode of connection to the REMCS Center varies depending on the user's network or server configuration. The mode of connection must be decided on in advance.

PRIMEQUEST series machines support the connection modes shown below. In any connection mode, only SMTP is used to communicate with the REMCS Center.

- Internet connection (e-mail)

Servers communicate on a one-to-one basis with the REMCS Center via the Internet.

[Figure 7.1](#) shows a configuration that has a network connected to the user port.

Remarks:

DNS settings at the MMB reference destination must be made to specify the SMTP server by FQDN at your site. This is not true when the SMTP server is specified in an IP address.

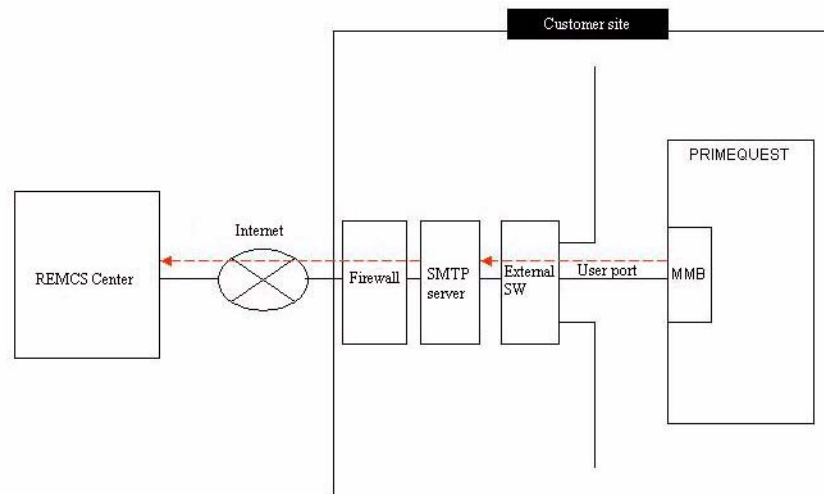


Figure 7.1 Internet Connection (using network connected to user port)

Figure 7.2 shows the format that uses the REMCS port as an example to use a network other than the network connected to the user port. The SMTP server of an ISP (Internet Service Provider) cannot be specified.

Remarks:

- The REMCS port must be set with the [set remcs] command from the MMB CLI (Command Line Interface).
- Be sure to specify the SMTP server in an IP address.

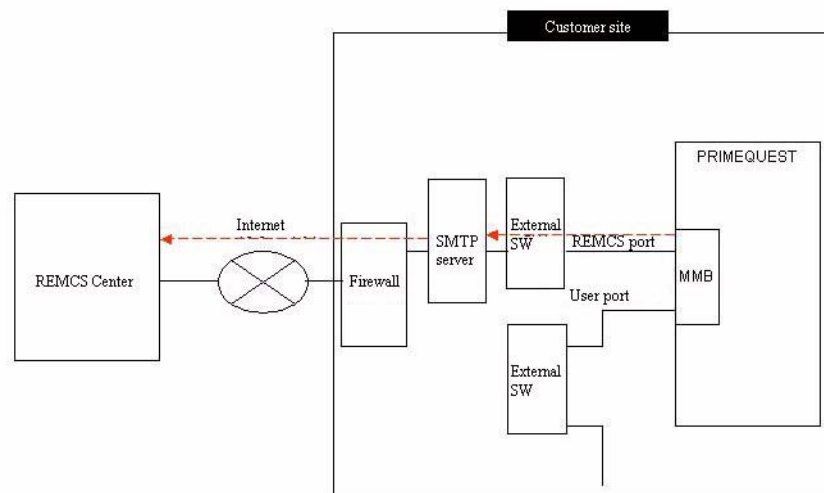


Figure 7.2 Internet connection (using REMCS port)

- P-P connection (ISDN: e-mail)

Servers communicate on a point-to-point (P-P) basis with the REMCS Center through an ISDN line as shown in [Figure 7.3](#) . The ISDN router is connected directly to the REMCS port or to the HUB (router) to make a dedicated LAN with other devices.

Remarks:

- The REMCS port must be set with the [set remcs] command from the MMB CLI (Command Line Interface).
- Be sure to specify the SMTP server in an IP address.

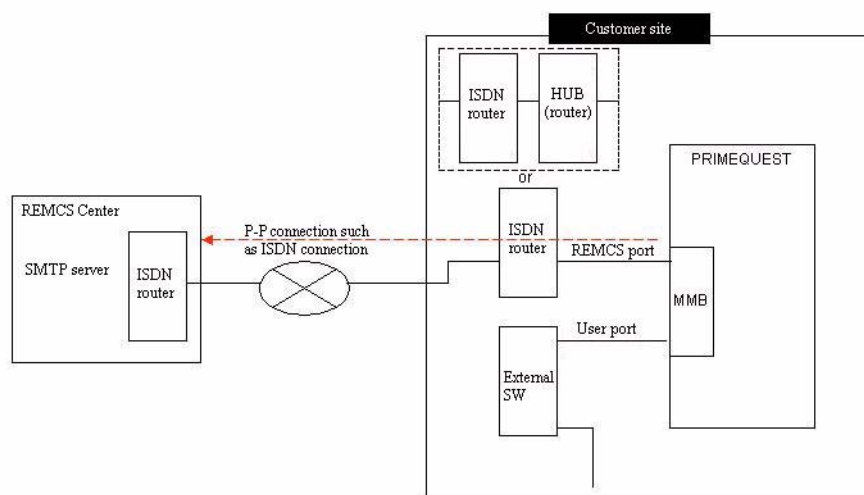


Figure 7.3 P-P connection

- P-P connection (VPN: e-mail)

Servers communicate on a point-to-point (P-P) basis with the REMCS Center through a broadband line such as ADSL as shown in [Figure 7.4](#). The broadband router is connected directly to the REMCS port or to the HUB (router) to make a dedicated LAN with other devices.

Remarks:

- The REMCS port must be set with the [set remcs] command from the MMB CLI (Command Line Interface).
- Be sure to specify the SMTP server in an IP address.

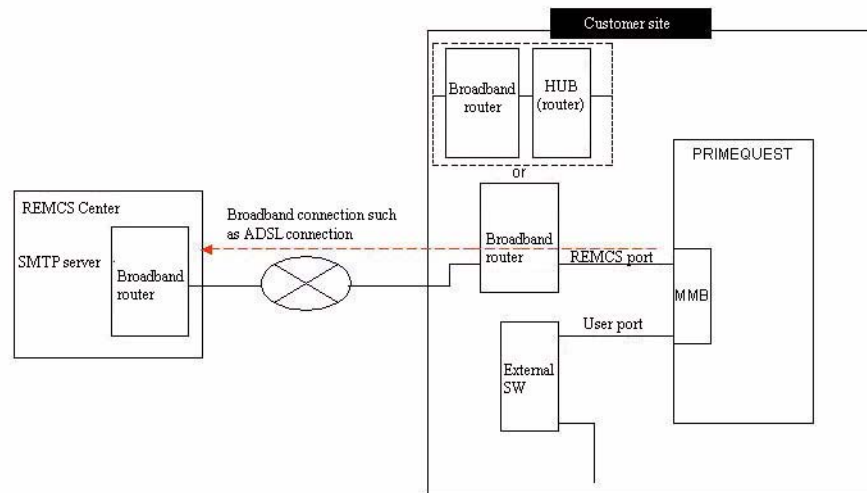


Figure 7.4 P-P (VPN) connection

7.1.2 Service startup procedure

To start the service, the user must be registered with the REMCS Center (registration).

Registration means to register customer information with the REMCS Center.

The procedure is explained below.

This procedure can be omitted if a certified service engineer has already completed the registration procedure on behalf of the customer, using the information obtained from the customer during product installation.

Perform registration as follows:

- 1 Start REMCS.
- 2 Set the connection mode.
- 3 Set up the environment.
- 4 Set customer information.
- 5 Execute registration.
- 6 Check connection

The screen transition flow for initial setup is shown below:

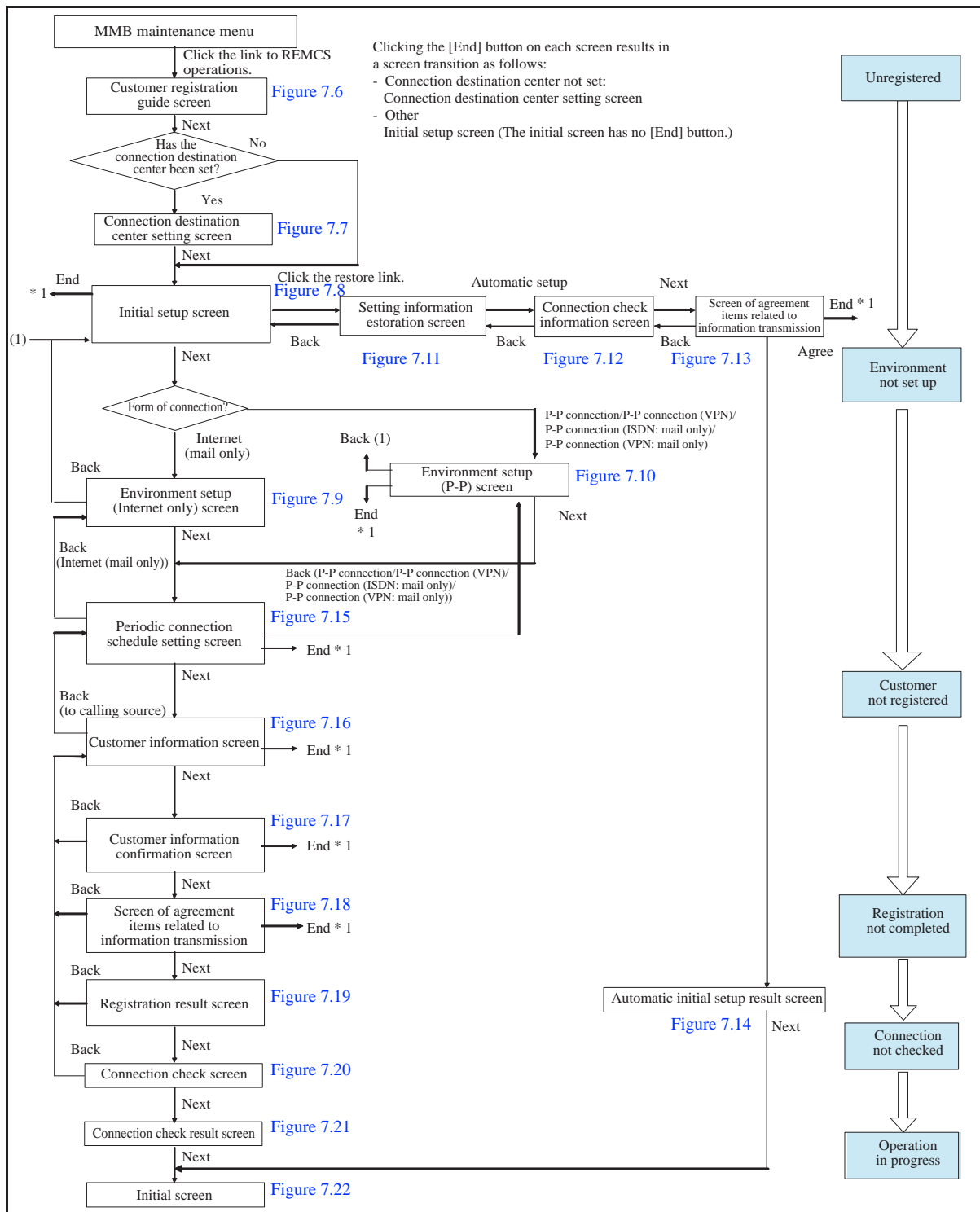


Figure 7.5 Workflow for registration with the REMCS center

The following types of information must be prepared for registration:

- 1 Warranty policy (containing the type name, check code, and serial number)
This is used for the confirmation of the machine ID displayed under the screen.
Display form example: MachineID 00-PQ400-containing the type name-check code-serial number
- 2 FQDN or IP address of the mail server used
For specifying FQDN, the DNS server must be specified in [Network] → [Network Interface] of the MMB Web-UI.
- 3 Transmission source mail address (must be qualified for external transmission)
- 4 Whether Email Split by the mail server is enabled or disabled
Check whether Email Split by your mail server is enabled or disabled.

To connect to the REMCS center using the REMCS port, the REMCS port must be set in advance from the MMB CLI. Prepare and set an IP address, sub-net mask, gateway address, and destination SMTP server address to be assigned to the REMCS port.

- Command

Setting command: Sets the REMCS port.

Note:

When the REMCS connection is made with P-P, the < gateway address > and the <SMTP address> settings is not required.

In this case, specify 0.0.0.0 for <gateway address> and <SMTP address>.

```
set remcs <ip address> <netmask> <gateway address> <SMTP address>
```

Display command: Displays the settings of the REMCS port.

```
show remcs
```

For details on each command, see Chapter 6, "CLI Operation" in the *PRIEMQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

Notes:

- Do not perform registration during maintenance operation.
- If the same IP address as that of a partition is set for using the REMCS port, communication between the PSA of said partition and the MMB is disconnected.

(1) Starting REMCS

Start REMCS from the menu by going to "Maintenance" - "REMCS" and selecting "REMCS" on the MMB Web-UI.

The screen shown in [Figure 7.6](#) appears if registration of customer information has not been finished. Registration requires the following settings:

- Connection mode
- Environment
- Periodic connection
- Customer information
- Registration
- Connection check

Note that the REMCS service cannot start if these settings are not complete.

If registration has already been finished, the "REMCS operation" screen in [Figure 7.22](#) appears instead. See [Section 7.1.3, "REMCS service operation procedure."](#)

Connection type Environment Customer information Registration Connection check EXIT

Customer Information Registration Instructions

Customer and Configuration (Hardware and Software) information will be sent automatically to the REMCS Center (Registration).

This information will be used solely and expressly for the support and maintenance of your system and will not be offered to any third party. Moreover, this information will be sent in encrypted form by the REMCS Agent.

If you agree with the above terms, proceed by clicking [Next] to register.

Next

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 UNUSED Internet Connection(Mal Only)

Figure 7.6 "Customer Information Registration Instructions" screen

- 1 Click the [Next] button.

The "The change of the connection point REMCS Center information" screen appears.

(2) Setting the connection mode

Select the target REMCS Center on the screen in [Figure 7.7](#).

The target REMCS Center varies depending on the country where the product is installed.

This screen does not appear if the REMCS Center has already been confirmed.

Connection type Environment Customer information Registration Connection check [EXIT](#)

Selecting REMCS Center

REMCS Center: USA-FCS

Save

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.7 "Selecting REMCS Center" screen

- 1 Click the [Next] button.
The target REMCS Center is registered, and the "Initial Settings" screen for environment setup appears.

(3) Setting up the environment

Set up the environment on the screen shown in [Figure 7.8](#). Setting up the environment means to set "Mode of connection to the REMCS Center," as explained in [7.1.1](#).

It is also possible to set the environment reading the set up information (environmental information such as SMTP server address, sender E-Mail address, etc... and customer information such as the customer name, administrator E-Mail address, etc...) which is a backup created from another cabinet or a backup one has previously created.

Even after the REMCS service has already started, the user can change the connection mode by clicking "Initial Settings" in the "REMCS operation" screen in [Figure 7.22](#).

Figure 7.8 "Initial Settings" screen

To make new settings

- 1 Select the connection mode from the following:
 - Internet connection (e-mail only): Default mode
 - P-P connection (ISDN: e-mail only): ISDN-based connection
 - P-P connection (VPN: e-mail only): Broadband connection such as an ADSL connection
- 2 Click the [Next] button.

The connection mode is registered and the relevant setting screen appears.

When settings already exist

If the following types of registration settings for the REMCS service have been backed up from another server, registration can be performed automatically by restoring the backup information.

- Customer information: rm_bkcus.def
- Environment information: rm_bkenv.def

- 1 Click [Restore of the setup information].
The setup information restoration screen appears.

(3-1) Environment setup (Internet)

When "Internet connection (e-mail only)" is selected for the connection mode on the "Initial Settings" screen, the screen shown in [Figure 7.9](#) appears so that the user can make settings for e-mail transmission over the Internet.

Even after the REMCS service has already started, the user can change the connection mode by clicking "Initial Settings" on the "REMCS operation" screen in [Figure 7.22](#).

* Connection type Environment Customer information Registration Connection check [EXIT](#)

Internet(Mail Only) connection environment settings

SMTP Server

Sender E-mail Address

Authentication type

AUTH SMTP type (valid only for AUTH SMTP)

UserID (Required if certification selected above.)

Password (Required if certification selected above.)

POP Server (Required if using POP before SMTP.)

Partial mail setting: ☒ Divide into 64Kbyte transmissions. ☐ Do not divide.

MachineID: 00-PQ400-MC5AOP111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.9 "Internet (Mail Only) connection environment settings" screen

- 1 Enter the following data:
 - SMTP server: Enter the SMTP server name or IP address with alphanumeric characters and/or symbols.
 - Sender E-Mail address: Enter the sender e-mail address with alphanumeric characters and/or symbols.
 - Certification type: Select one from No Certification, POP Before SMTP, and AUTH SMTP.
 - AUTH SMTP feature: This item is enabled when certification type AUTH SMTP is selected. Select one from AUTO (default), CRAM-MD5, PLAIN, and LOGIN.
 - User ID: Enter the user ID of the authentication server with alphanumeric characters and/or symbols.
 - Password: Enter the password of the authentication server with alphanumeric characters and/or symbols.
 - POP server: Enter the POP server name or IP address with alphanumeric characters and/or symbols when certification type POP Before SMTP is selected.
 - Partial mail setting: Select whether to split mail into packets.
By default, [Divide into 64Kbyte transmissions] is selected. However, if the mail server does not support Email Split, select [Do not divide].
- 2 Click the [Next] button.

The registration of the connection mode is finished, and the "Periodical Connection settings" screen appears.

(3-2) Environment setup (P-P or P-P (VPN))

If "P-P connection (ISDN: e-mail only)" or "P-P connection (VPN: e-mail only)" is specified as the connection mode in the [Init Setup] window, the screen shown in [Figure 7.10](#) appears so that e-mail transmission information can be specified.

Even after the REMCS service has already started, the user can change the connection mode by clicking "Connection Environment" in the "REMCS operation" screen shown in [Figure 7.22](#).

Figure 7.10 "Point-to-Point Connection environment settings" screen

- 1 Enter the following data:
 - SMTP/PROXY Server: Enter the SMTP/PROXY server name or IP address with alphanumeric characters and/or symbols.
 - Sender E-mail Address: Enter the sender e-mail address with alphanumeric characters and/or symbols.
 - Partial mail setting: Select whether to split mail into packets.
By default, [Divide into 64Kbyte transmissions] is selected. However, if the mail server does not support Email Split, select [Do not divide].
 - 2 Click the [Next] button.
- The registration of the connection mode is finished, and the "Periodical Connection settings" screen appears.

(3-3) Environment setup (restoration of settings)

The screen shown in [Figure 7.11](#) appears when "Restore of the setup information" is clicked on the "Initial Settings" screen. The specified setting files can be restored and used for automatic environment setup. The setting files that can be used are the backups of the local setting files or the backups of setting files of another unit.

The screenshot shows a web-based interface for restoring settings. At the top, there is a navigation bar with tabs: "Connection type", "Environment", "Customer information", "Registration", and "Connection check". A blue "EXIT" link is located to the right of the "Connection check" tab. The main content area has a title "Restore from setting file" in a box. Below this, there are two rows of input fields. The first row is labeled "Environment Information file" and the second is labeled "Customer Information file". Each row has a text input field followed by a "Browse" button. At the bottom of the main content area, there are three buttons: "Back", "Restore", and "AutoSetting". The footer of the screen contains two pieces of information: "MachineID: 00-PQ400-MC5AOP111U-FL-TEST000001" on the left and "UNUSED P.P Connection(Mail Only)" on the right.

Figure 7.11 "Restore from setting file" screen

- 1 Specify the following files that have been backed up on a PC on which a Web browser is running or on a file server:
 - Environment setup file: rm_bkenv.def
 - Customer information file: rm_bkcus.def
- 2 Click the [Restore] button to restore the setting files.
- 3 Click the [AutoSetting] button to display the [Connection check information] window. Check the settings relating to the transmission destination of connection results.

Figure 7.12 [Connection check result] screen

- [Notification of the result to the administrator]: Specifies whether the customer's administrator must be notified of the results.
- [Notification of the result to the installer]: Specifies whether the user who performed the check must be notified of the results. If [Notification] is selected, this user's mail address must be specified in [E-mail address for receiving results].

- 4 Click the [Next] button to execute automatic registration. The "Information Transmit Agreement" screen appears.

The screenshot shows a web-based interface for the REMCS system. At the top, there is a navigation bar with the following tabs: "Connection type", "Environment", "Customer information", "Registration", and "Connection check". A blue "EXIT" link is located to the right of the "Connection check" tab. The main content area is titled "Information Transmit Agreement". Below the title, there is a text box containing the following text:

If you agree with the following terms, click [Agree] button.
By clicking [Agree] button, Registration information will be sent to the REMCS Center.
Customer Information and Machine Information (Hardware and Software) will be sent to the REMCS Center.
And, if a hardware failure occurs, machine information will be sent automatically to the REMCS Center.
This information will be used solely and expressly for the support and maintenance of your system and will not be offered to any third party.
Moreover, this information will be sent in encrypted form by the REMCS Agent.

Below the text box, there are three buttons: "Back", "Agree", and "End". At the bottom of the screen, there is a status bar with the following text: "MachineID: 00-PQ400-MC5AOP111U-FL-TEST000001" and "UNUSED P-P Connection(Mal Only)".

Figure 7.13 "Information Transmit Agreement" screen (automatic setting)

- 5 Confirm the agreement items and click the [Agree] button.
Registration of customer information is finished, and the "Automatic setting status" screen appears.

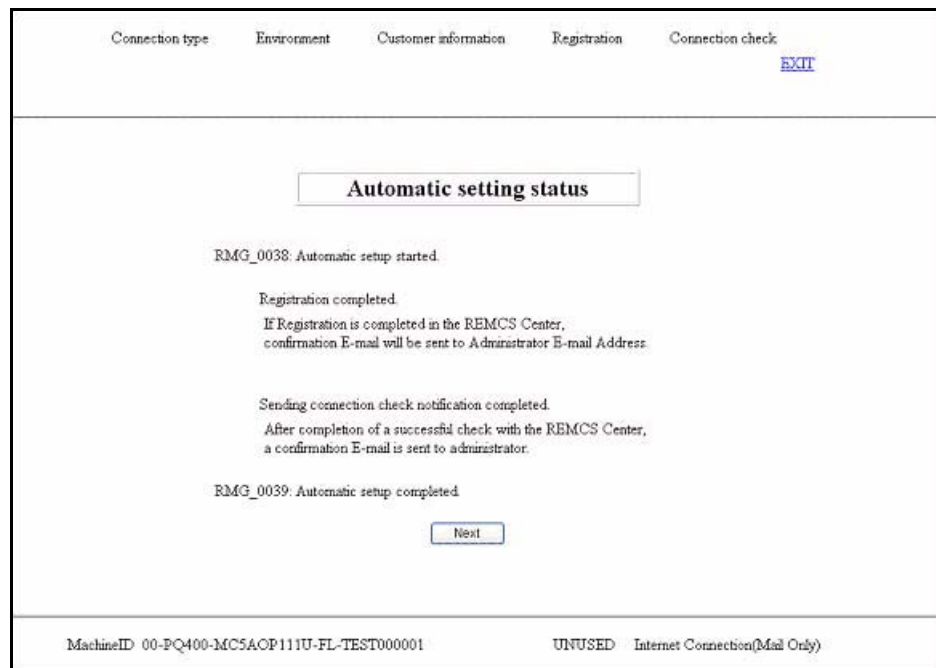


Figure 7.14 "Automatic setting status" screen

- 6 Click the [Next] button.
Registration is finished, and the "REMCS operation" screen appears.

(4) Setting up a periodic connection schedule

Set up a periodic connection schedule using the screen shown in [Figure 7.15](#).

Even after the REMCS service has already started, the periodic connection schedule can be changed by clicking "Periodic Connection" in the "REMCS operation" screen shown in [Figure 7.22](#).

Figure 7.15 "Periodical Connection settings" screen

- 1 Enter the following data:
The default selections are "every week" and "10:00-15:00." Change the values only if required.
 - Connection period: Select either "every day", "every day (excluding Sunday)", "every day (excluding Saturday and Sunday)", or "every week".
 - Day of the week: If "every week" is specified for the period, specify the day of the week (Sunday to Saturday).
 - Connection duration: Specify the operation start time and end time.
- 2 Click the [Next] button.
Registration of the period connection schedule is finished, and the "Customer Information" screen appears.
If the [End] button is clicked, the screen returns to "Initial Settings" without saving the settings.

(5) Setting customer information

Enter customer information.

Even after the REMCS service has already started, the customer information can be changed by clicking "Customer Information" in the "REMCS operation" screen shown in [Figure 7.22](#).

Figure 7.16 "Customer Information" screen

- Notes on data entry
- Do not use special characters, such as &, in the e-mail settings.
- Do not use &, ", ', <, >, /, _, or blank characters for a unique unit name

Table 7.1 Customer information entry items

Y: Required N: Optional

Entry item	Max. number of digits	Entry requirement	Explanation
Company Name	30	Y	Enter your company name.
Department/Division	20	Y	Enter your section/department name.
Address	30	Y	Enter your address.
Building	20	N	Enter the building name of your company.
Administrator Name	20	Y	Enter your server administrator name.
Admin E-mail Address	60	Y	Enter the e-mail address of your server administrator using alphanumeric characters and/or symbols. Registration mails and error notification mails are sent to this e-mail address.
ZIP/Postal Code	(*1)	N	Enter the postal code of your company location using digits and a hyphen '-' where applicable.
Phone Number	20	Y	Enter your telephone number using digits and hyphens where applicable.
Fax Number	20	N	Enter your fax number using digits and hyphens '-' where applicable.
Machine Unique Name	32	N	Enter the unique name of your machine using alphanumeric characters and/or symbols.
Country Name	2	Y	Enter the country name of the installation site in alphabetic characters. (Enter JP when the product is installed in Japan. Lowercase letters are automatically converted into uppercase letters when saved.) (Enter a country name listed in the ISO-3166 code list A (2). Enter 99 for a country not appearing in this list.)
Machine Installation Site	30	N	Enter the installation site. (No need to enter if it is the same as "Address")
Machine Installation Building	20	N	Enter the name of the building. (No need to enter if it is the same as "Address")
FE E-Mail Address	60	N	Enter the FE e-mail address using alphanumeric characters and/or symbols. Mails indicating completion of connection confirmation are also sent to this e-mail address.

*1 The number of digits of the postal code depends on the country in which the PRIMEQUEST series machines are installed.

- 1 Enter data for the entry items listed in [Table 7.1](#).
- 2 Click the [Next] button.

Registration of customer information is finished, and the "Customer Information Review" screen appears.

If the [End] button is clicked, the screen returns to "Initial Settings" without saving the settings.

* Connection type * Environment * Customer information Registration Connection check

[EXIT](#)

Customer Information Review

Confirm customer information.

Company Name * Fujitsu
 Department/Division LA
 Address * USA
 Building
 Administrator Name * abc
 E-mail Address * sbc@us.fujitsu.com
 Zip/Postal Code
 Phone Number * 012-345-6789
 Fax Number
 Machine Unique Name
 Country Name * US
 Machine Installation Site
 Machine Installation Building
 FE's E-mail Address

Back Next End

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.17 "Customer Information Review" screen

3 Click the [Next] button.

Registration of customer information is finished, and the "Information Transmit Agreement" screen appears.

The "Information Transmit Agreement" screen also appears if the [AutoSetting] button on the "Restore from setting file" screen is clicked for automatic setup.

* Connection type * Environment * Customer information Registration Connection check

[EXIT](#)

Information Transmit Agreement

If you agree with the following terms, click [Agree] button.
By clicking [Agree] button, Registration information will be sent to the REMCS Center.
Customer Information and Machine Information (Hardware and Software) will be sent to the REMCS Center.
And, if a hardware failure occurs, machine information will be sent automatically to the REMCS Center.
This information will be used solely and expressly for the support and maintenance of your system and will not be offered to any third party.
Moreover, this information will be sent in encrypted form by the REMCS Agent.

Back Agree End

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.18 "Information Transmit Agreement" screen

4 Confirm the items on this screen and click the [Agree] button.

Registration of customer information is finished, and the "Registration result" screen appears.

(6) Registration

When registration is finished, the execution result is displayed as shown in [Figure 7.19](#).

The screenshot shows a web-based interface for the REMCS service. At the top, there is a navigation bar with five tabs: '* Connection type', '* Environment', '* Customer information', '* Registration', and 'Connection check'. The '* Registration' tab is currently selected. To the right of the 'Connection check' tab is a blue link labeled 'EXIT'. Below the navigation bar, the main content area has a title 'Registration result' in a box. Below this title, a message states: 'If Registration is successfully completed in the REMCS Center, a confirmation E-mail will be sent to Administrator E-mail Address.' At the bottom of the main content area, there are three buttons: 'Back', 'Next', and 'End'. The 'Next' button is highlighted. At the very bottom of the screen, there is a status bar with two pieces of information: 'MachineID 00-PQ400-MC5AOP111U-FL-TEST000001' and 'UNUSED Internet Connection(Mail Only)'.

Figure 7.19 "Registration result" screen

- 1 Click the [NEXT] button to go to (7) Checking connection.

(7) Checking connection

- 1 The "Connection check" screen is displayed. Check the settings relating to the transmission destination of connection check results.

The screenshot shows a web-based interface for a 'Connection check'. At the top, there is a navigation bar with links: '* Connection type', '* Environment', '* Customer information', '* Registration', and 'Connection check'. An 'EXIT' link is also present. The main heading is 'Connection check'. Below it, a note states: 'Executes connection check with the REMCS Center. Please be sure to check the diagnostic results E-mail sent from the REMCS Center. Transmission time is dependant on network speed.' The central form contains two notification sections. The first section, 'Notification of the result to the administrator. (sbc@us.fujitsu.com)', has two radio buttons: 'Notification' (selected) and 'Do not notify'. The second section, 'Notification of the result to the installer.(In case of sending except for administrator, please check it)', has three radio buttons: 'Notification (normal format)', 'Notification for cell phone (simple format)', and 'Do not notify' (selected). Below these is a text input field for 'E-mail address for receiving results.'. At the bottom of the form are three buttons: 'Back', 'Check', and 'End'. The footer of the page displays 'MachineID 00-PQ400-MC5AOP111U-FL-TEST000001' and 'UNUSED Internet Connection(Mail Only)'.

Figure 7.20 "Connection check" screen

- [Notification of the result to the administrator]: Specifies whether the customer's administrator must be notified of the results.
- [Notification of the result to the installer]: Specifies whether the user who performed the check must be notified of the results.

If [Notification] is selected, this user's mail address must be specified in [E-mail address for receiving results].

- 2 Click the [Check] button to execute connection check processing. The "Result of connection check" screen is displayed.

* Connection type * Environment * Customer information * Registration * Connection check [EXIT](#)

Result of connection check

RMG_0058: Connection check notification completed.

After completion of a successful check with the REMCS Center,
a confirmation E-mail is sent to administrator.

[Next](#)

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only)

Figure 7.21 "Result of connection check" screen

- 3 Click the [Next] button.
The connection check is completed, and the "REMCS operation" screen shown in [Figure 7.22](#) is displayed.

7.1.3 REMCS service operation procedure

When registration with the REMCS Center is complete or if registration is canceled halfway, the "REMCS operation" screen shown in [Figure 7.22](#) appears. It also appears when REMCS is started from the MMB Web-UI after confirmation of connection to the REMCS Center has been completed.

From the menu on the left side of this screen, select the function to be executed.

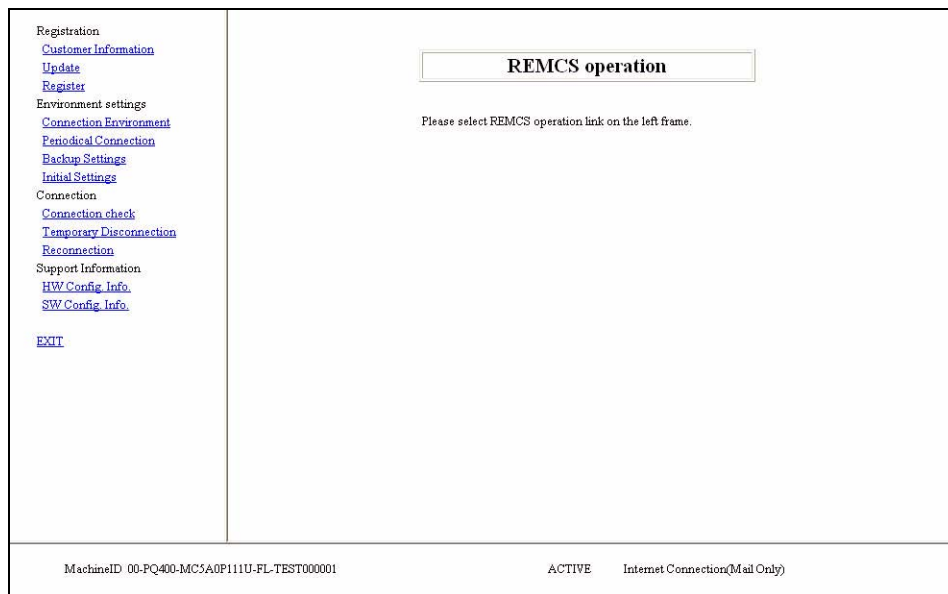


Figure 7.22 "REMCS operation" screen

Table 7.2 Explanation of items on REMCS initial screen

Menu item	Explanation
Customer information	Correct customer information.
Update registration	Update registration.
Registration	Normally not used. Use this item when so instructed by the support center.
Connection information	Display or update connection information.
Periodical connection information	Set or change the periodic connection schedule.
Setup information backup	Back up settings.
Initial Setup	Set or change the connection mode.
Connection confirmation	Confirm the connection to the REMCS Center.
Center connection stop	Suspend the connection to the REMCS Center, such as for maintenance.
Center connection reopening	Resume the connection to the center.

Menu item	Explanation
HW Config. Info. is transmitted	Transmit hardware configuration information.
SW Config. Info. is transmitted	Transmit software configuration information.
REMCS Operation End	End REMCS operation.

Customer Information

Use this item to check the customer information entered during registration or to change customer information such as, for example, the administrator or address.

- 1 Go to "REMCS operation" screen shown in [Figure 7.22](#) and click "Customer Information". The "Customer Information" screen appears.
- 2 To simply confirm the customer information, click the [End] button. To update the information, update the information and click the [Next] button.
The "Customer Information Review" screen appears.
- 3 Check the information. If no problem is found, click the [Next] button.
The "Information Transmit Agreement" screen appears.
If a problem is found and it needs to be corrected, click the [Back] button to return to the "Customer Information Review" screen and correct the problem.
- 4 After checking the environment and verifying that e-mail transmission is possible, click the [Agree] button.
The entered information is automatically transmitted to the REMCS Center.
After completion of transfer to e-mail, the "Registration result" screen appears.
- 5 Click the [Next] button. The "REMCS operation" screen is redisplayed.
 - E-mail reporting the completion of registration is sent to the administrator's e-mail address entered on the "Customer Information" screen.
 - Any attempt to update user registration information before the arrival of the e-mail reporting completion of registration is invalid. Perform update processing, if necessary, after the arrival of the e-mail containing the completion report.

Update Registration

Use this item if registration with the REMCS Center has not been finished after updating the information on the "Customer Information" screen.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Update".
The "Information Transmit Agreement" screen appears.
- 2 After checking the environment and verifying that e-mail transmission is possible, click the [Agree] button.
The entered information is automatically transmitted to the REMCS Center.
After completion of transfer, the "Registration result" screen appears.

- 3 Click the [Next] button. The "REMCS operation" shown in [Figure 7.22](#) is redisplayed.
 - E-mail reporting the completion of registration is sent to the administrator's e-mail address entered on the "Customer Information" screen.
 - Any attempt to update user registration information before the arrival of the e-mail reporting completion of registration is invalid. Perform update processing, if necessary, after the arrival of the e-mail with the completion report.

Registration

This function is not used for normal operation. Use it only when so instructed by the support center.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Registration".

The "Information Transmit Agreement" screen appears.
- 2 After checking the environment and verifying that e-mail transmission is possible, click the [Agree] button.

The entered information is automatically transmitted to the REMCS Center.
After completion of transfer, the "Registration result" screen appears.
- 3 Click the [Next] button. The "REMCS operation" shown in [Figure 7.22](#) is redisplayed.
 - E-mail reporting the completion of registration is sent to the administrator's e-mail address entered on the "Customer Information" screen.
 - Any attempt to update user registration information before the arrival of the e-mail reporting completion of registration is invalid. Perform update processing, if necessary, after the arrival of the e-mail with the completion report.

Connection information

Use this item to display the current connection information or change the settings such as those for the mail server.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Connection Environment".

The screen displayed depends on the connection mode used. For Internet connection (e-mail only), the screen shown in [Figure 7.23](#) appears.

If "P-P connection (ISDN: e-mail only)" or "P-P connection (VPN: e-mail only)" is specified, the screen shown in [Figure 7.24](#) appears.

For information on the operation that can be performed on each screen, see the following:

For Internet connection (e-mail only) connection:

See [\(3-1\) Environment setup \(Internet\)](#).

For "P-P connection (ISDN: e-mail only)" or "P-P connection (VPN: e-mail only)":

See [\(3-2\) Environment setup \(P-P or P-P \(VPN\)\)](#).

- 2 Confirm the information displayed. If information changed, click the [Next] button.

The information is updated and the "REMCS operation" screen shown in [Figure 7.22](#) appears again.

To simply confirm the information, click the [End] button to return to the "REMCS operation" screen shown in [Figure 7.22](#).

Registration
[Customer Information](#)
[Update](#)
[Register](#)
 Environment settings
[Connection Environment](#)
[Periodical Connection](#)
[Backup Settings](#)
[Initial Settings](#)
 Connection
[Connection check](#)
[Temporary Disconnection](#)
[Reconnection](#)
 Support Information
[HW Config Info](#)
[SW Config Info](#)
[EXIT](#)

Internet(Mail Only) connection environment settings

SMTP Server
 Sender E-mail Address
 Authentication type: No certification
 AUTH SMTP type: Invalidity (valid only for AUTH SMTP)
 UserID (Required if certification selected above.)
 Password (Required if certification selected above.)
 POP Server (Required if using POP before SMTP.)
 Partial mail setting: ☒ Divide into 64Kbyte transmissions. ☐ Do not divide.

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only)

Figure 7.23 "A setup of an environment of the Internet (Only mail)" screen

Registration

[Customer Information](#)

[Update](#)

[Register](#)

Environment settings

[Connection Environment](#)

[Periodical Connection](#)

[Backup Settings](#)

[Initial Settings](#)

Connection

[Connection check](#)

[Temporary Disconnection](#)

[Reconnection](#)

Support Information

[HW Config Info](#)

[SW Config Info](#)

[EXIT](#)

Point-to-Point Connection environment settings

SMTP/PROXY Server

Sender E-mail Address

Partial mail setting

☒ Divide into 64Kbyte transmissions. ☐ Do not divide.

Next

End

MachineID 00-PQ400-MC5AOP1111U-FL-TEST000001

ACTIVE P-P Connection(VEN:Mail Only)

Figure 7.24 "Point-to-Point Connection environment settings" screen

Periodical connection information

Use this item to display or change the periodical connection schedule.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Periodical Connection".

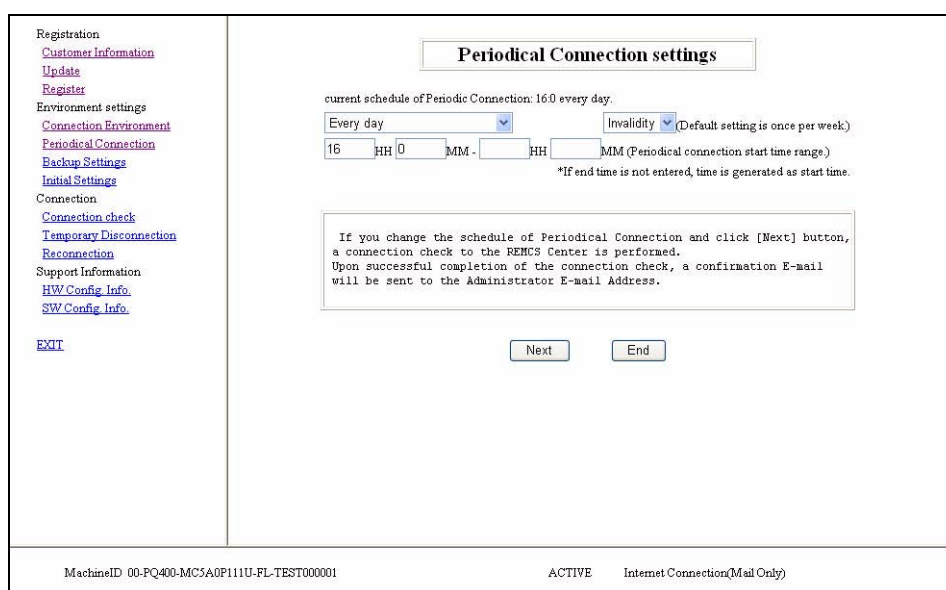
The "Periodical Connection settings" screen shown in [Figure 7.25](#) appears.

For information on screen operation, see [Section 7.1.2](#), (4), "Setting up a periodic connection schedule."

- 2 If necessary, change the periodical connection schedule and click the [Next] button. A connection check to report the schedule to the REMCS Center is performed, then the "REMCS operation" screen shown in [Figure 7.22](#) appears again.

To simply confirm information, click the [End] button to return to the "REMCS operation" screen shown in [Figure 7.22](#)

E-mail reporting the completion of connection confirmation is sent to the administrator's e-mail address entered on the "Customer Information" screen.



Periodical Connection settings

current schedule of Periodic Connection: 16:0 every day

Every day Invalidity (Default setting is once per week)

16 HH 0 MM - HH MM (Periodical connection start time range.)

*If end time is not entered, time is generated as start time.

If you change the schedule of Periodical Connection and click [Next] button, a connection check to the REMCS Center is performed. Upon successful completion of the connection check, a confirmation E-mail will be sent to the Administrator E-mail Address.

MachineID 00-PQ400-MC5A0P111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only)

Figure 7.25 "Periodical Connection settings" screen

Setup information backup

Use this item to back up customer information and environment settings to local files.

The settings thus backed up can be used, regardless of the OS, for processing to start the REMCS service on other servers.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Backup Settings".

The "Backup file setting" screen shown in [Figure 7.26](#) appears.

- 2 Click "Backup to local file."

A dialog box for specifying file names and storage locations appears. Specify the following:

Customer information: rm_bkcus.def

Environment information: rm_bkenv.def

- 3 Click the [End] button to return to the "REMCS operation" shown in [Figure 7.22](#).



Figure 7.26 "Backup file setting" screen

Initial Settings

Use this item to change the current connection mode to another mode.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Initial Settings".

The "Initial Settings" screen shown in [Figure 7.27](#) appears.

For information on screen operation, see [Section 7.1.2, \(3\), "Setting up the environment."](#)

- 2 If the connection mode is changed and the [Next] button is clicked, the previous information is abandoned and the unit status becomes "unset." The user must set up information again, as in [Section 7.1.2, \(3\), "Setting up the environment"](#) and perform service start operation.

Registration Customer Information Update Register Environment settings Connection Environment Periodical Connection Backup Settings Initial Settings Connection Connection check Temporary Disconnection Reconnection Support Information HW Config Info SW Config Info EXIT	<div style="text-align: center;">Initial Settings</div> <div style="text-align: center;">Restore from setting file</div> <div> Connection type: Internet Connection(Mail Only) ▼ </div> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> If you click [Restore from setting file] link, you need to do Initial Settings. </div> <div style="text-align: center;"> Next End </div>
MachineID 00-PQ400-MC5A0P111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only)	

Figure 7.27 "Initial Settings" screen during operation

Connection check

Use this item to check the status of connection to the REMCS Center.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Connection check".

The "Connection check" screen shown in [Figure 7.28](#) appears.

- 2 Check the settings relating to the transmission destination of connection results, and click the [Connection Check] button.

Connection check

Executes connection check with the REMCS Center. Please be sure to check the diagnostic results E-mail sent from the REMCS Center. Transmission time is dependant on network speed.

Notification of the result to the administrator. (sbc@us.fujitsu.com)

☒ Notification ☐ Do not notify.

Notification of the result to the installer.(In case of sending except for administrator, please check it)

☐ Notification (normal format) ☐ Notification for cell phone (simple format).

☒ Do not notify.

E-mail address for receiving results

MachineID 00-PQ400-MC5AOP111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only)

Figure 7.28 [Connection check] screen

- 3 The "Result of connection check" screen (Figure 7.29) is displayed. Click the [Next] button to return to the REMCS initial screen shown in Figure 7.22.



Figure 7.29 "Result of connection check" screen

The mail that reports the completion of the connection check is sent to the e-mail address of the result notification destination displayed on the "Connection check" screen.

Center connection stop

Use this item to suspend the connection to the REMCS Center.

- When periodical connection is disabled due to server maintenance or holidays, the connection to the REMCS Center should be suspended.
 - No communication is performed with the REMCS Center while the connection to the REMCS Center is suspended.
 - To restart system operation after the connection to the REMCS Center is suspended, "Reconnection" must be used.
- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Temporary Disconnection". The "Temporary Disconnection" screen shown in [Figure 7.30](#) appears.
 - 2 Click the [Send] button.

A confirmation dialog box appears, and a notification about connection suspension is sent to the REMCS Center.

After processing is finished, the result is displayed in a pop-up window and the "REMCS operation" screen shown in [Figure 7.22](#) is redisplayed.

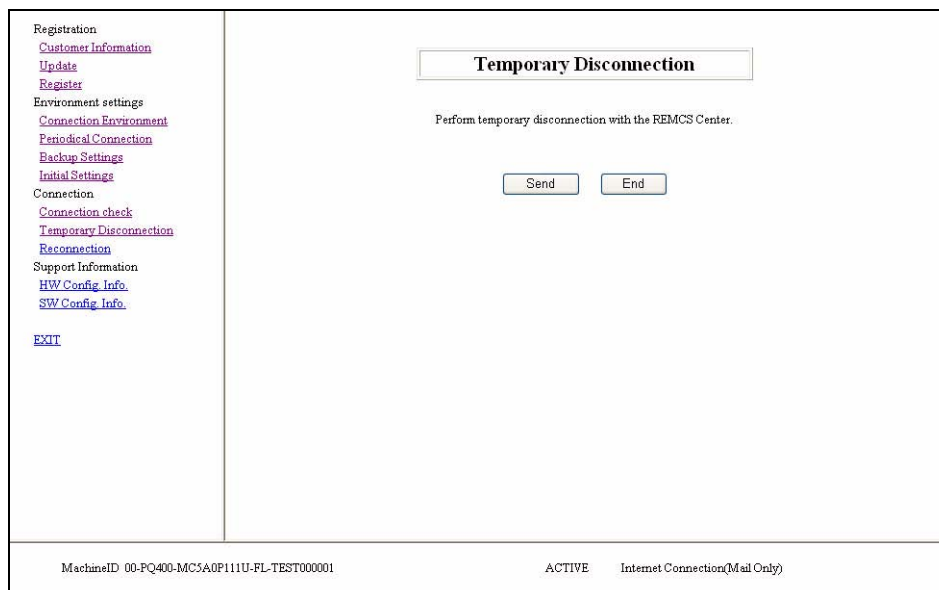


Figure 7.30 "Temporary Disconnection" screen

Center connection reopening

Use this item to resume a connection to the REMCS Center that has been suspended.

Executing this operation while the server operation status is "connection suspended" changes the status to "in operation."

Executing it while the server operation status is "during maintenance/connection suspended" changes the status to "during maintenance."

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "Reconnection". The screen shown in [Figure 7.31](#) appears.
- 2 Click the [Send] button.

A send confirmation dialog box appears, and a notification about connection resumption is sent to the REMCS Center.

After processing is finished, the result is displayed in a pop-up window and the "REMCS operation" screen shown in [Figure 7.22](#) is redisplayed.

<p>Registration</p> <p>Customer Information</p> <p>Update</p> <p>Register</p> <p>Environment settings</p> <p>Connection Environment</p> <p>Periodical Connection</p> <p>Backup Settings</p> <p>Initial Settings</p> <p>Connection</p> <p>Connection check</p> <p>Temporary Disconnection</p> <p>Reconnection</p> <p>Support Information</p> <p>HW Config. Info.</p> <p>SW Config. Info.</p> <p>EXIT</p>	<div style="border: 1px solid black; padding: 5px; margin: 0 auto; width: 150px;"> Reconnection </div> <p>Reconnection with the REMCS Center.</p> <div style="display: flex; justify-content: center; gap: 20px; margin-top: 10px;"> <input type="button" value="Send"/> <input type="button" value="End"/> </div>
<div style="display: flex; justify-content: space-between;"> MachineID 00-PQ400-MC5A0P111U-FL-TEST000001 ACTIVE Internet Connection(Mail Only) </div>	

Figure 7.31 "Reconnection" screen

Sending hardware configuration information

Use this item to transmit server hardware configuration information to the REMCS Center.

- 1 Click "HW Config Info" in the menu on the "REMCS operation" screen shown in [Figure 7.22](#). The screen shown in [Figure 7.32](#) appears.
- 2 Click the [Send] button.

A send confirmation dialog box appears, and software configuration information is sent to the REMCS Center.

After processing is finished, the result is displayed in a pop-up window and the "REMCS operation" screen shown in [Figure 7.22](#) is redisplayed.

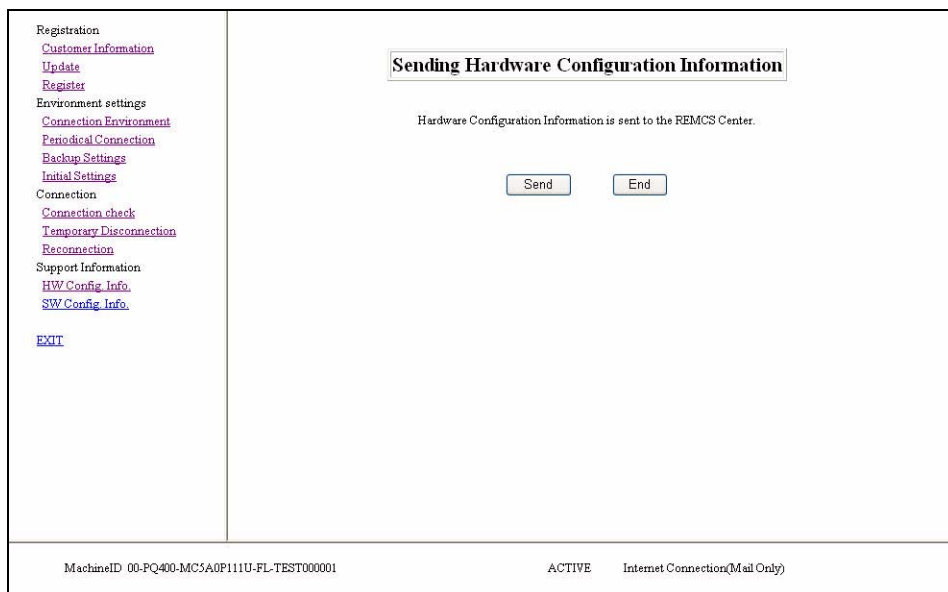


Figure 7.32 "Sending Hardware Configuration Information" screen

Sending software configuration information

Use this item to transmit server software configuration information to the REMCS Center.

- 1 Go to the menu of the "REMCS operation" screen shown in [Figure 7.22](#) and click "SW Config Info". The screen shown in [Figure 7.33](#) appears.
- 2 Click the [Send] button.

A send confirmation dialog box appears, and software configuration information is sent to the REMCS Center.

After processing is finished, the result is displayed in a pop-up window and the "REMCS operation" screen shown in [Figure 7.22](#) is redisplayed.

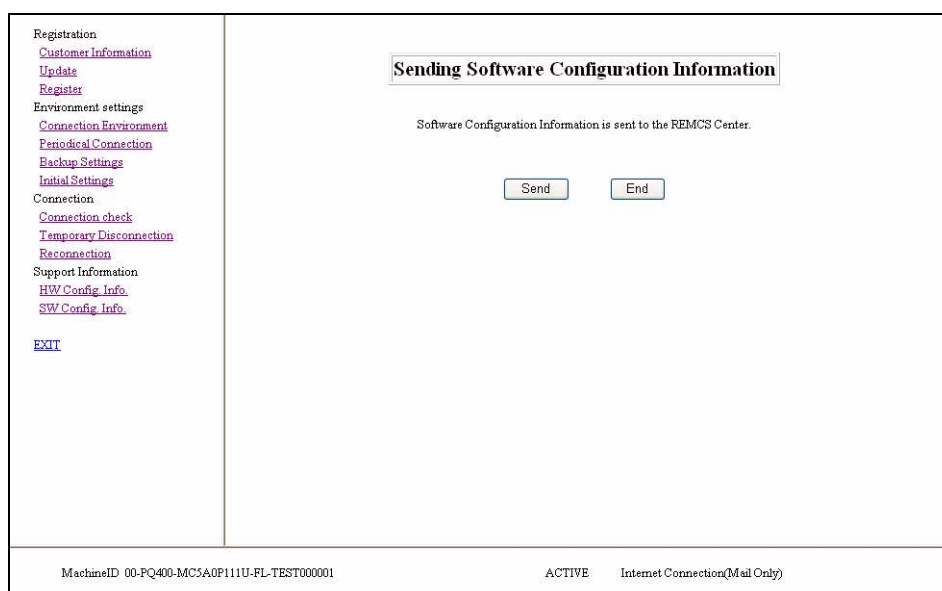


Figure 7.33 "Sending Software Configuration Information" screen

Remarks:

There may be a delay before the partition is updated to reflect the software configuration information. Therefore, the latest information may not be displayed immediately after software replacement.

7.1.4 Detail Setup of REMCS

The Detail Setup function can be used to provide detail settings such as for the transmission retry count and timeout triggers to avoid transmission problems, changing the REMCS Center to connect to, or switching the unit name to be displayed.

Normally, this function need not be used. Use it only when so instructed by a certified service engineer or the support center.

To use this function, go to the MMB Web-UI menu and select [Maintenance] → [REMCS] → [Detail Setup].

The "REMCS FE operation" screen shown in [Figure 7.34](#) appears.

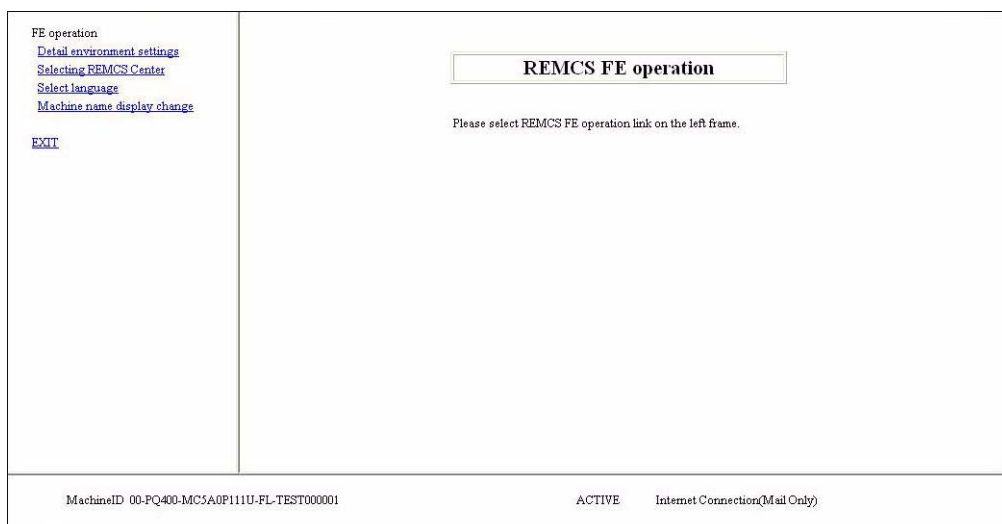


Figure 7.34 "REMCS FE operation" screen

Table 7.3 Explanation of items on FE operation initial screen

Menu item	Explanation
Environment details information	Set the communication timeout triggers, the number of retries, etc., that are applicable when the Internet is used.
Connection center information	Change the REMCS Center to connect to.
Japanese/English switching	Toggle between Japanese and English as the display language.
Switching of indication of a device name	Toggle between the unit ID and the unique name for the display of unit names in the Web-GUI.

Environment details information

Use this item to change the settings for the communication environment applicable when the Internet is used.

The screen that appears varies depending on the connection mode authentication type: either the screen shown in [Figure 7.35](#) or the screen shown in [Figure 7.36](#) will appear.

Set this information very carefully because wrong settings may prevent event transmission to the REMCS Center.

Figure 7.35 "Environment settings" screen (POP Before SMTP authentication)

Figure 7.36 "Environment settings" screen (other than POP Before SMTP authentication)

Table 7.4 Explanation of items on environment detail setting screen

Y: Required

Entry item	Max. number of digits	Entry requirement	Explanation
E-Mail timeout	4	Y	Specify the e-mail timeout in seconds using numeric characters. (Enter a value from 60 to 3600.)
E-Mail retry count	2	Y	Enter the e-mail retry count in numeric characters.
E-Mail retry interval	3	Y	Enter the e-mail retry interval in numeric characters. (1 to 600)
E-Mail partial size	3	Y	Enter the mail packet size in numeric characters. (10 to 100 KB)
SMTP port No.	5	Y	Enter the SMTP server port number in numeric characters. The default is 25 (Well Known Port). (1 to 65535)
POP authentication timeout	4	Y	Specify the POP3 authentication timeout in seconds using numeric characters. (60 to 3600)
Standby by time after the POP Cert	4	Y	Enter the wait time (in milliseconds) until mail transmission begins after POP3 authentication. Specify a value in numeric characters (1000 ms is recommended). (0 to 30000)
POP port No.	5	Y	Enter the POP3 authentication server port number in numeric characters. The default is 110 (Well Known Port). (1 to 65535)

- 1 Go to the menu of the "REMCS FE operation" screen and click "Environment details information".
The screen shown in [Figure 7.35](#) or [Figure 7.36](#) appears depending on the current settings.
- 2 Click the [Regist] button.
A confirmation dialog box appears. Provide an affirmative answer to register the settings.
After processing is finished, the result is displayed in a pop-up window and the "REMCS FE operation" screen appears.

Connection center information

Use this item to change the REMCS Center to connect to.

- 1 Go to the menu of the "REMCS FE operation" screen and click "Selecting REMCS Center". The screen shown in [Figure 7.37](#) appears.
- 2 Select the target REMCS Center. No data is entered directly in this field. The user needs to select one from the dropdown list. The default is the current REMCS Center.
- 3 Click the [Regist] button.
A confirmation dialog box appears. Provide an affirmative answer to register the settings.
After processing is finished, the result is displayed in a pop-up window and the "REMCS FE operation" screen appears.

FE operation
[Detail environment settings](#)
[Selecting REMCS Center](#)
[Select language](#)
[Machine name display change](#)
[EXIT](#)

Selecting REMCS Center

REMCS Center: USA-FCS

Save End

MachineID 00-PQ400-MC5A0P111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.37 "Selecting REMCS Center" screen

Japanese/English switching

Use this item to toggle between Japanese and English as the display language.

- 1 Go to the menu of the "REMCS FE operation" screen and click "Select language". The screen shown in [Figure 7.38](#) appears.
- 2 Select Japanese or English. The default is the current setting.
- 3 Click the [Regist] button.

A confirmation dialog box appears. Provide an affirmative answer to register the settings.

After processing is finished, the result is displayed in a pop-up window and the "REMCS FE operation" screen appears.

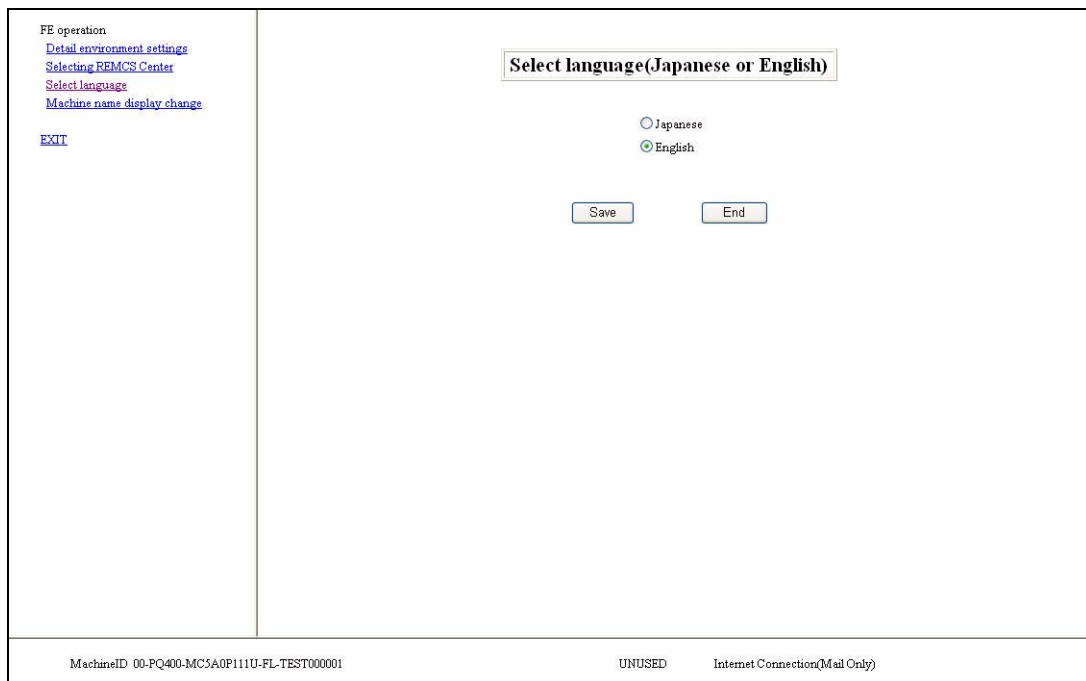


Figure 7.38 "Select language (Japanese or English)" screen

Switching of indication of a device name

Use this item to toggle between the machine ID and the unique name for the display of unit names in the Web-GUI. (The unique unit name is defined on the "The input of the customer information" screen.)

- 1 Go to the menu of the "REMCS FE operation" screen and click "Machine name display change". The screen shown in [Figure 7.39](#) appears.
- 2 Specify the unit name to be displayed in the status display frame. The default is the current setting.
- 3 Click the [Regist] button.

A confirmation dialog box appears. Provide an affirmative answer to register the settings.

After processing is finished, the result is displayed in a pop-up window and the "REMCS FE operation" screen appears.

FE operation
[Detail environment settings](#)
[Selecting REMCS Center](#)
[Select language](#)
[Machine name display change](#)
[EXIT](#)

Select to Display Machine ID or Machine Unique Name

☒ Machine ID
☐ Machine Unique Name

Save End

MachineID 00-PQ400-MC5A0P111U-FL-TEST000001 UNUSED Internet Connection(Mail Only)

Figure 7.39 "Select to Display Machine ID or Machine Unique Name" screen

7.1.5 REMCS messages

This section explains the major error messages displayed on individual screens. In the actual message, the "(xxx)"-part is replaced by character strings such as for return values.

"Initial Settings" screen (See [Figure 7.8.](#))

Table 7.5 Messages on initial setting screen

Message code	Message	Response
RMG_0025	Failed to set connection mode. (xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0027	Failed to change Machine status. (xxx)	

"Restore from setting file" screen (See [Figure 7.11.](#))

Table 7.6 Messages on setting information restoration screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0027	Failed to change Machine status. (xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0032	Specified file can not restore.	Specify a valid file.
RMG_0033	Invalid directory name specified.	Specify a valid directory.
RMG_0036	Required entry.	Enter data correctly.
RMG_0096	Connection type mismatch. Environment information restore is unable to execute.	Specify a file using the same connection type.
RMG_0118	Failed to restore REMCS environment. (xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0142	The file doesn't exist in the selected directory.	Specify the directory containing the file. Specify a valid file and reexecute.
RMG_0143	Invalid REMCS environment information file.	
RMG_0144	Invalid customer information file.	

"Automatic setting status" screen (See Figure 7.14.)

Table 7.7 Messages on automatic-setting result screen

Message code	Message	Response
RMG_0040	Automatic setup failed.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.

"Internet (Mail Only) connection environment settings" screen (See Figure 7.9.)

Table 7.8 Messages on environment setting (Internet - mail only) screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0016	Input value is out of range.	
RMG_0018	Failed to get registration data.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0030	Specify server name/user ID/password all when you specify POP server	Specify the POP server correctly.
RMG_0031	Specify user ID/password all when you specify AUTH SMTP.	Specify AUTH SMTP authentication information correctly.
RMG_0036	Required entry.	Enter the data.
RMG_0041	Failed to setting Machine status.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0043	Failed to set REMCS environment (Internet connection(Mail only)).(xxx)	Check the specified FQDN or IP address of the SMTP server. Check also whether the network condition is normal.
RMG_0056	Connection confirmation notification completed.(xxx)	Check whether the network connection is operational.
RMG_0181	Invalid E-mail address specified.	Enter data correctly.

"Point-to-Point Connection environment settings" screen (See [Figure 7.10.](#))

Table 7.9 Messages on environment setting (P-P) screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0018	Failed to get registration data.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0028	Input all items.	Specify all items.
RMG_0041	Failed to setting Machine status.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0056	Failed in the connection confirmation notification.(xxx)	Check whether the network connection is operational.
RMG_0080	Failed to set REMCS environment(P-P).(xxx)	Check the specified FQDN or IP address of the SMTP server. Check also whether the network is operational.
RMG_0181	Invalid E-mail address specified.	Enter data correctly.

"Periodical Connection settings" screen (See [Figure 7.15.](#))

Table 7.10 Messages on periodic-connection scheduling screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0016	Input value is outside the range.	
RMG_0018	Failed to get registration data.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0027	Failed to change Machine status.(xxx)	
RMG_0036	Required entry.	Enter the data.
RMG_0048	Invalid periodical connection schedule date specified.	Check the operation start time. Specify a valid time.
RMG_0051	Failed to register the periodical connection schedule.(xxx)	Check whether the network connection is operational.
RMG_0052	Failed to set the periodical connection schedule.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0056	Failed in the connection confirmation notification.(xxx)	Check whether the network connection is operational.
RMG_0186	Failed to send notice of changing agent information.	Check whether the network connection is operational.
RMG_0187	Failed to send agent information.	Check whether the network connection is operational.

"Customer Information" screen (See Figure 7.16.)

Table 7.11 Messages on customer information screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0018	Failed to get registration data.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0036	Required entry.	Enter the data.
RMG_0065	Failed to get customer information.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0068	Invalid character specified in company name.	Check the characters that can be specified, and correct the specification.
RMG_0069	Invalid character specified in department/division.	
RMG_0070	Invalid character specified in address.	
RMG_0071	Invalid character specified in building name.	
RMG_0072	Invalid character specified in administrator name.	
RMG_0073	Invalid character specified in machine installation site.	
RMG_0074	Invalid character specified in machine installation building.	Enter data correctly.
RMG_0181	Invalid E-mail address specified.	

"Customer Information Review" screen (See [Figure 7.17.](#))

Table 7.12 Messages on customer information screen

Message code	Message	Response
RMG_0077	Failed to register customer information.(xxx)	Check whether HOSTNAME is specified in the MMB NetworkInterface settings. Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.

"Information Transmit Agreement" screen (See [Figure 7.18.](#))

Table 7.13 Messages on agreement item screen for information transmission

Message code	Message	Response
RMG_0056	Failed in the connection confirmation notification.(xxx)	Check whether the network connection is operational.

"Registration result" screen (See [Figure 7.19.](#))

Table 7.14 Messages on registration result screen

Message code	Message	Response
RMG_0085	Registration failed.(xxx)	Check whether the network connection is operational.
RMG_0088	Registration (Update) failed.(xxx)	

"Backup file settings" screen (See [Figure 7.26.](#))

Table 7.15 Messages on setting information backup screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0018	Failed to get registration data.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0033	Invalid directory name specified.	Specify a valid directory name.
RMG_0036	Required entry.	Enter the data.
RMG_0122	Failed to backup REMCS environment.(xxx)	Check the backup destination for a space shortage and write protection.
RMG_0124	Failed to create REMCS environment backup file.(xxx)	

"Connection check" screen (See [Figure 7.20](#)/[Figure 7.28](#))/ "Connection check information" screen (See [Figure 7.12.](#))

Table 7.16 Messages on connection check screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0041	Failed to setting Machine status.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0056	Failed in the connection confirmation notification.(xxx)	Check whether the network connection is operational.
RMG_0181	Invalid E-mail address specified.	Enter data correctly.
RMG_0182	Enter E-mail address of administrator or installer.	Specify a valid setting.
RMG_0183	Specify E-mail address for delivery of the REMCS setup confirmation.	Enter data correctly.

"Result of connection check" screen (See [Figure 7.21](#)/[Figure 7.29](#).)

Table 7.17 Messages on connection check result screen

Message code	Message	Response
RMG_0041	Failed to setting Machine status.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0056	Failed in the connection confirmation notification.(xxx)	Check whether the network connection is operational.

"Temporary Disconnection" screen/"Reconnection" screen (See [Figure 7.31](#).)

Table 7.18 Messages on stop/restart center connection screen

Message code	Message	Response
RMG_0041	Failed to get Machine status.(xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0092	Registration has not been executed, Setup is incomplete.	Wait for completion of registration before execution.

"Sending Hardware Configuration Information" screen (See [Figure 7.32](#).)

Table 7.19 Messages on hardware configuration information transmission screen

Message code	Message	Response
RMG_0133	Failed to send hardware configuration information.(xxx)	Check whether the network connection is operational.

"Sending Software Configuration Information" screen (See [Figure 7.33](#).)

Table 7.20 Messages on software configuration information transmission screen

Message code	Message	Response
RMG_0135	Failed to send software configuration information. (xxx)	Check whether the network connection is operational.

"Environment settings" screen (See [Figure 7.35](#) and [Figure 7.36](#).)

Table 7.21 Messages on environment detail setting screen

Message code	Message	Response
RMG_0015	Invalid entry.	Enter a valid value.
RMG_0016	Input value is out of range.	
RMG_0018	Failed to get registration data. (xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0021	Failed to register REMCS environment data. (xxx)	
RMG_0036	Required entry.	Enter data correctly.

"Selecting REMCS Center" screen (See [Figure 7.37](#).)

Table 7.22 Messages on connection-destination center change screen

Message code	Message	Response
RMG_0018	Failed to get registration data. (xxx)	Retry execution. If execution still fails, close the REMCS screen, reopen it, and then perform execution again. If the same symptom still remains, call the support center.
RMG_0027	Failed to change Machine status. (xxx)	
RMG_0097	Failed to read connection point list file. (xxx)	
RMG_0099	Failed to change REMCS Center. (xxx)	
RMG_0150	Failed to read setting file. (xxx)	
RMG_0172	Failed to get Destination information. (xxx)	

Communication error messages (SMTP communication)

The table below lists the error messages displayed on the screen when errors occur during communication processing. Each communication error message includes a recommended action so the user can take action accordingly. If the same symptom recurs even after the indicated action is taken, call the support center. The RL and SS-Agent values included in each message indicate internal information.

Table 7.23 Communication error messages (SMTP communication)

Message code	Message
RMG_2000	(SMTP) There is no valid E-Mail address. The E-Mail address is not set up correctly. RL:xxx, SS-Agent:xxx
RMG_2003	(SMTP) Communication timeout error was detected. Please try again after several minutes. When you do not solve the trouble, please check the network between the mail (SMTP) server, and check whether the SMTP server is running. RL:xxx, SS-Agent:xxx
RMG_2004	(SMTP) An error was detected by the specified mail (SMTP) server. Please improve environment with reference to the following messages. (Message from the SMTP server) xxxxxxxxxxxxxxxxxxxxxxxx RL:xxx, SS-Agent:xxx
RMG_2005	(SMTP) Unable to connect the specified mail (SMTP) Server. Error was detected during communication to the specified mail (SMTP) server. The following causes can be considered. <ul style="list-style-type: none"> • The SMTP server name is wrong. • A DNS server is not specified for the MMB. • When the DNS server is used, the DNS server is not running. • The problem of the network between mail (SMTP) server. (Message from the SMTP server) xxxxxxxxxxxxxxxxxxxxxxxx RL:xxx, SS-Agent:xxx
RMG_2006	(SMTP) Unable to connect the specified mail (SMTP) Server. Error was detected during communication to the specified mail (SMTP) server. The following causes can be considered. <ul style="list-style-type: none"> • The SMTP server name is wrong. • A DNS server is not specified for the MMB. • When the DNS server is used, the DNS server is not running. • The problem of the network between mail (SMTP) server. (Message from the SMTP server) xxxxxxxxxxxxxxxxxxxxxxxx RL:xxx, SS-Agent:xxx

Message code	Message
RMG_2007	<p>(SMTP) An error was detected between the mail (POP3) server. POP before SMTP authentication failed. The following causes can be considered.</p> <ul style="list-style-type: none"> • The POP3 server name is wrong. • User name is wrong. • Password is wrong. <p>(Message from the POP3 server) XXXXXXXXXXXXXXXXXXXXX RL:xxx, SS-Agent:xxx</p>
RMG_2008	<p>(SMTP) An error was detected between the mail (POP3) server. An error was detected during communication to the specified POP3 server. The following causes can be considered.</p> <ul style="list-style-type: none"> • The POP3 server name is wrong. • A DNS server is not specified for the MMB. • When the DNS server is used, the DNS server is not running. • The problem of the network between POP3 server. <p>(Message from the POP3 server) XXXXXXXXXXXXXXXXXXXXX RL:xxx, SS-Agent:xxx</p>
RMG_2009	<p>(SMTP) An error was detected between the mail (POP3) server. The timeout error occurred in communication with a POP3 server. The following causes can be considered.</p> <ul style="list-style-type: none"> • The problem of the network between POP3server. • POP3 server is not running. <p>RL:xxx, SS-Agent:xxx</p>
RMG_2010	<p>(SMTP) An error was detected between the mail (POP3) server. The POP3 server name is wrong, or the POP3 server is not running. The following causes can be considered.</p> <ul style="list-style-type: none"> • The POP3 server name is wrong. • A DNS server is not specified for the MMB. • When the DNS server is used, the DNS server is not running. • The problem of the network between POP3 server. <p>(Message from the POP3 server) XXXXXXXXXXXXXXXXXXXXX RL:xxx, SS-Agent:xxx</p>

Message code	Message
RMG_2011	<p>(SMTP) The error was detected during communication to the specified mail (SMTP) server.</p> <p>Authentication failed on SMTP server.</p> <p>The user name or password is wrong, so it cannot authenticate on SMTP server.</p> <p>(Message from the POP3 server)</p> <p>xxxxxxxxxxxxxxxxxxxxxx</p> <p>RL:xxx, SS-Agent:xxx</p>
RMG_2012	<p>(SMTP) An error was detected during communication to the specified mail (SMTP)</p> <p>The specified SMTP server does not support SMTP AUTH. Or the SMTP server does not support specified auth type.</p> <p>The following causes can be considered.</p> <ul style="list-style-type: none"> • Specified SMTP server is wrong. • Specified auth type is wrong. <p>(Message from the SMTP server)</p> <p>xxxxxxxxxxxxxxxxxxxxxx</p> <p>RL:\$1, SS-Agent:\$2</p>

Other error messages

If an error message other than the above is displayed, close the REMCS screen, open it again, and then reexecute the operation. If the same symptom still occurs, call the support center.

7.1.6 MMB log downloading

If a problem such as failure to send e-mail to the REMCS Center occurs, an MMB operation log may be required as troubleshooting material. If so, follow the instructions from the support center, go to the "System" menu of the MMB Web_UI menu and select "System Event Log" to download the log retained. For this operation, see Section 5.2.3, "[System Event Log] window" in the *PRIEMQUEST 580A/540A/520A/500/400 Series Reference Manual: Basic Operation/GUI/Commands* (C122-E003EN).

Submit the downloaded log file to a Fujitsu certified service engineer.

7.1.7 Notes on using the REMCS GUI

When using the REMCS GUI, note the following:

- The REMCS GUI appears in a separate window when the REMCS menu is selected from the MMB Web UI. If a security software product such as Symantec Client Firewall or Norton Internet Security with a firewall function is installed on the PC running the Web browser, cookie or reference source information may be blocked by default. In this event, a message indicating a screen transition error appears and the REMCS screen does not appear. The settings must be changed so that cookie and reference source information will not be blocked.

An example of changing the settings when Symantec Client Firewall is used is given below. For information on other software products, see the manuals and HELP of the respective products.

- 1 Start Symantec Client Firewall to display the initial screen.
 - 2 Select Privacy Control and click the Set button.
 - 3 The Privacy Control window appears. Click the Custom Level button.
 - 4 The Customize Privacy Setting window appears. Select No: Enable Cookie under Block Cookie and clear the Enable Browser Privacy check box, and click the OK button.
 - 5 The Privacy Control window is redisplayed. Click the OK button to complete the setting.
- If, after the REMCS GUI is displayed, no entry is made within the duration of the specified timeout value, the REMCS GUI session is disconnected. (The timeout value for this operation can be specified after selecting "Network"- "Network Protocols" in the Web-UI and setting the "Timeout" entry for "Web(HTTP/HTTPS)".)
 - Only one user can use the REMCS GUI at a time. If another user is already logged in, the following message appears.

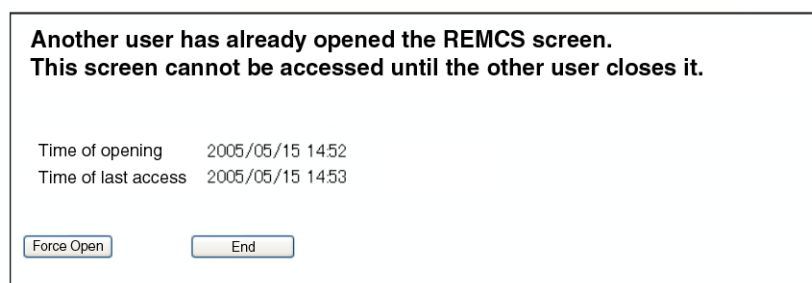


Figure 7.40 REMCS message screen

[Force open]: Logs in by forcibly logging out the currently logged in user.

[End]: Close the window.

- After using the MMB Web-UI to change the time zone, perform the following operation to update REMCS center information:

Set the periodic connection schedule.

The periodic connection schedule of REMCS is interpreted according to the currently set time zone.

CHAPTER 8 Onboard GbE (Broadcom Ethernet) Network Configuration Under Windows Environment

8.1 Outline (PRIMEQUEST 580A/540A/580/540/480/440)

The Teaming function (multi-path function) using Broadcom Ethernet supports the following on the PRIMEQUEST 580A/540A/580/540/480/440:

The Teaming function also uses the BASP (Broadcom Advanced Server Program) function within the BACS2 (Broadcom Advanced Control Suite2) utility.

(1) Smart Load Balance and Fail Over (+LiveLink)

This function disperses load among the load balance members. At the occurrence of member problems (all members), traffic is transferred to a standby member.

Upon the recovery of one or more load balance members, traffic is switched from the standby member to a load balance member. The LiveLink function is only available in this mode.

Remarks: The Livelink function monitors for link loss between all load balance members and the specified target and transfers traffic to normally operating load balance members.

(2) Generic Trunking (FEC/GEC)/802.3ad-Draft Static

This is a load balance function that uses PagP (Port Aggregation Protocol). A switch to be interfaced must have this function or an equivalent one. This function also actualizes fail-over among load balance members.

(3) SLB (Auto-Fallback Disable)

This function is basically the same as (1) "Smart Load Balance and Fail Over" but does not switch traffic from a standby member to a load balance member automatically. Moreover, this function cannot be used concurrently with LiveLink.

Remarks: The Link Aggregation (802.3ad) function is not supported.

Notes:

- The message "Broadcom 5704s chip is not supported" is output, but operation can continue without being affected.
- STP should be disabled when configuring SLB without using the LiveLink function.
Doing so enables the down time to be kept to a minimum when determining the spanning tree loop at the onset of a fail over.
- BASP (Broadcom Advanced Server Program: Teaming Software) does not support Microsoft Network Load Balancing (NLB).
- BASP (Broadcom Advanced Server Program: Teaming Software) operations require that the user be logged in with Administrator privileges.
- A team configuration name should be a character string from 1 to 39 characters in length.
- A team name must not begin with a space or contain any of the following characters:
& \ / : * ? < > | "
- A team name must be unique.
- When using the Generic Trunking function, you cannot specify a standby member.
- Click the [Fallback] button (on the Team Properties tab) when switching traffic back to a load balance member from a standby member by using SLB (Auto-Fallback Disable).
- The function cannot be used under a Dynamic Host Configuration Protocol environment.
- Up to eight members can be specified.
- All team members must be configured by using Broadcom Netextreme Fiber.

- **Broadcom Ethernet configuration (GSWB interface)**

Broadcom Ethernet ports of each IOU in the PRIMEQUEST 580A/540A/580/540/480/440 are connected to the IOU port of each GSWB as shown below.

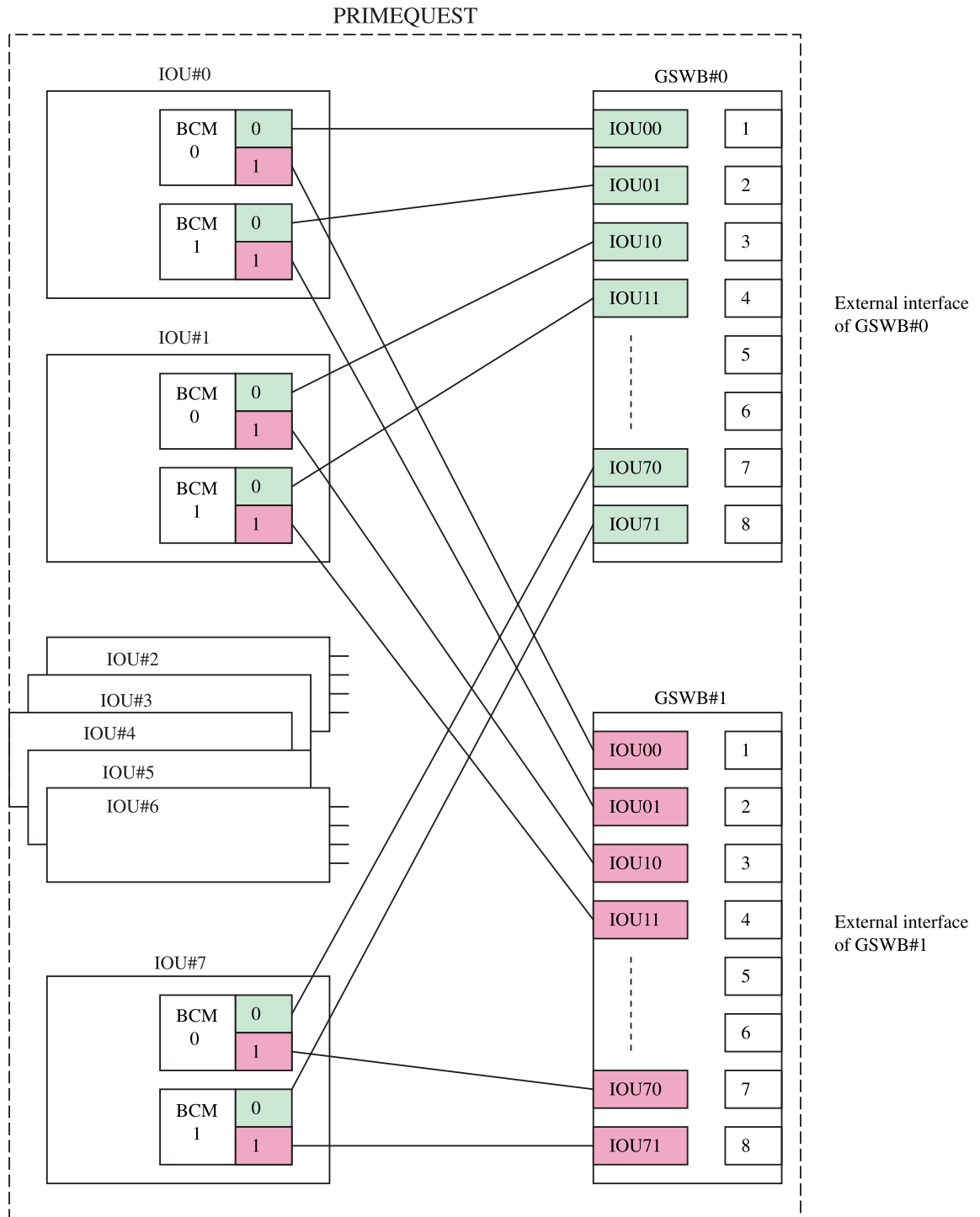


Figure 8.1 Broadcom Ethernet configuration (GSWB interface)

- Method of identifying a physical port on the PRIMEQUEST 580A/540A/580/540/480/440

- 1 Identify the physical position of a Broadcom Ethernet port to be controlled by BACS 2.

A Broadcom Ethernet port is displayed on Windows Server 2003 OS (Device Manager) or BACS 2 (Broadcom Advanced Control Suite 2) as follows:

"Broadcom NetXtreme Gigabit Fiber #<No>"

Next, identify the physical position of the Broadcom Ethernet port by referring to the MAC address information on Ethernet ports.

Confirm the MAC address of the Broadcom Ethernet port on the relevant IOU by using MMB Web UI.

Example: [System] → [IOU] → [IOU#x]

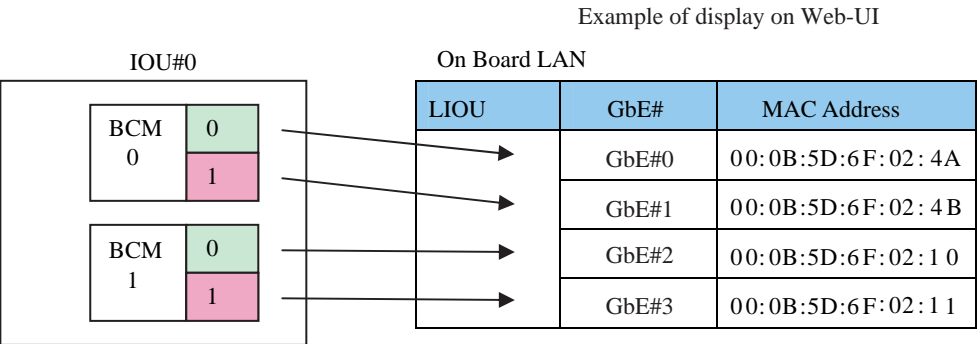


Figure 8.2 Physical positions of Ethernet ports

- 2 Confirm the MAC address of "Broadcom NetXtreme Gigabit Fiber #<No>" on BACS 2 and identify the physical position.

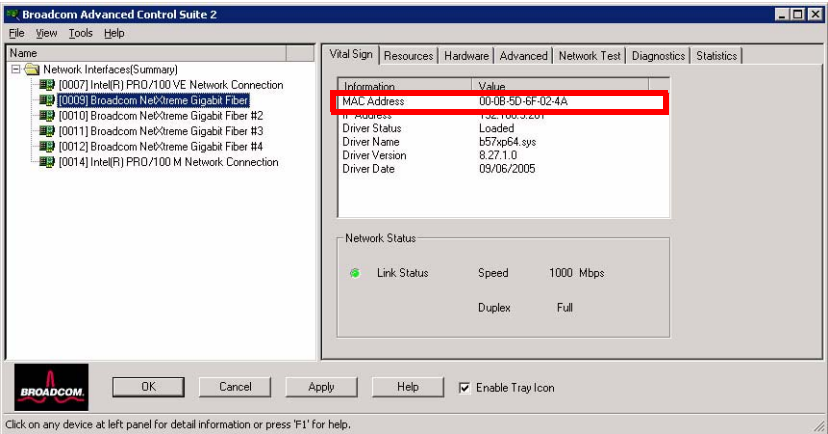


Figure 8.3 [Broadcom Advanced Control Suite 2] dialog window

- Notes on setting teams (multi-path setting) on the PRIMEQUEST 580A/540A/580/540/480/440

The Broadcom Ethernet ports of each IOU are grouped as GSWB#1 and GSWB#2. When configured, Generic Trunking (FEC/GEC) only supports the group member configuration.

Example: When partitions are built up with IOU#0 and IOU#1, the configuration can consist of the following groups:

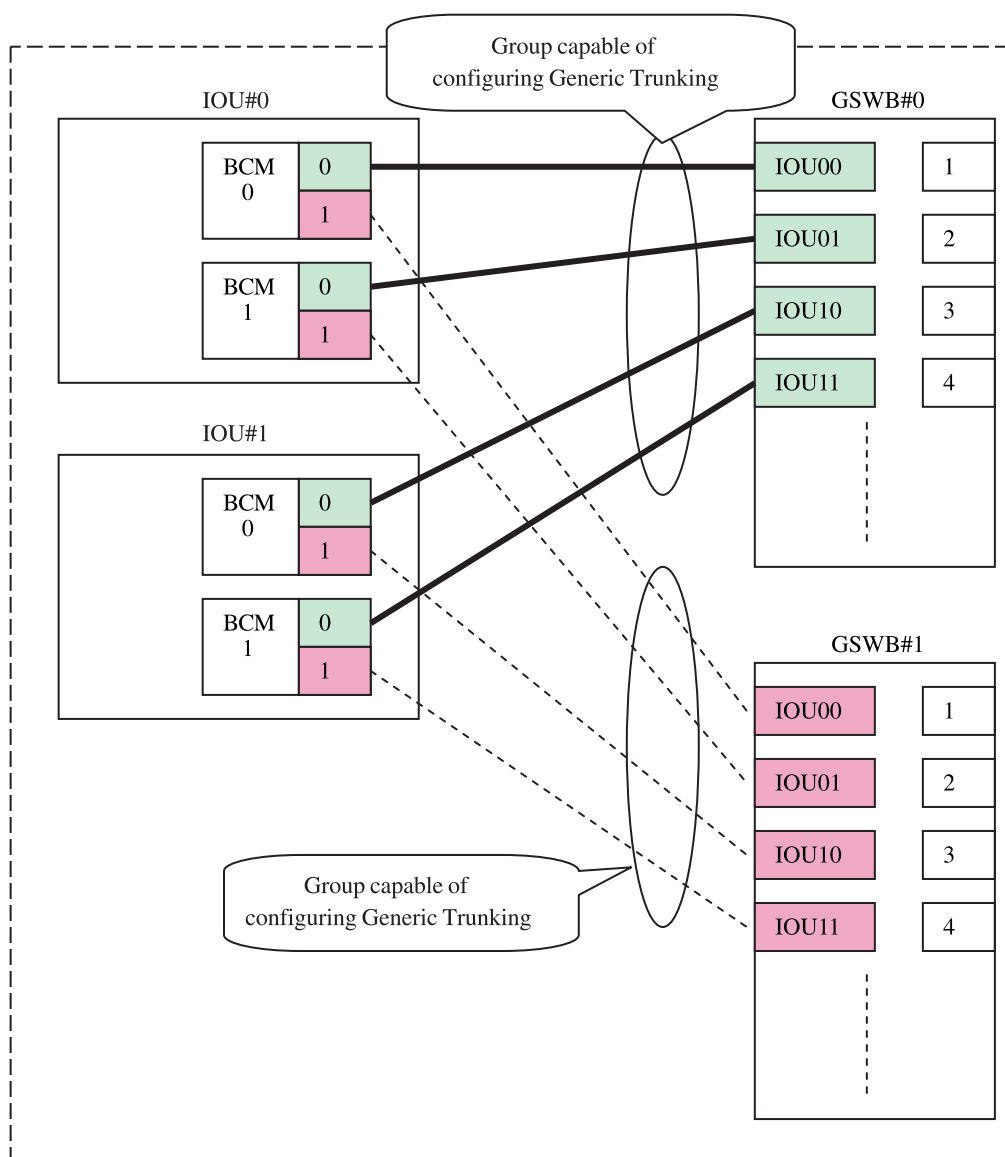
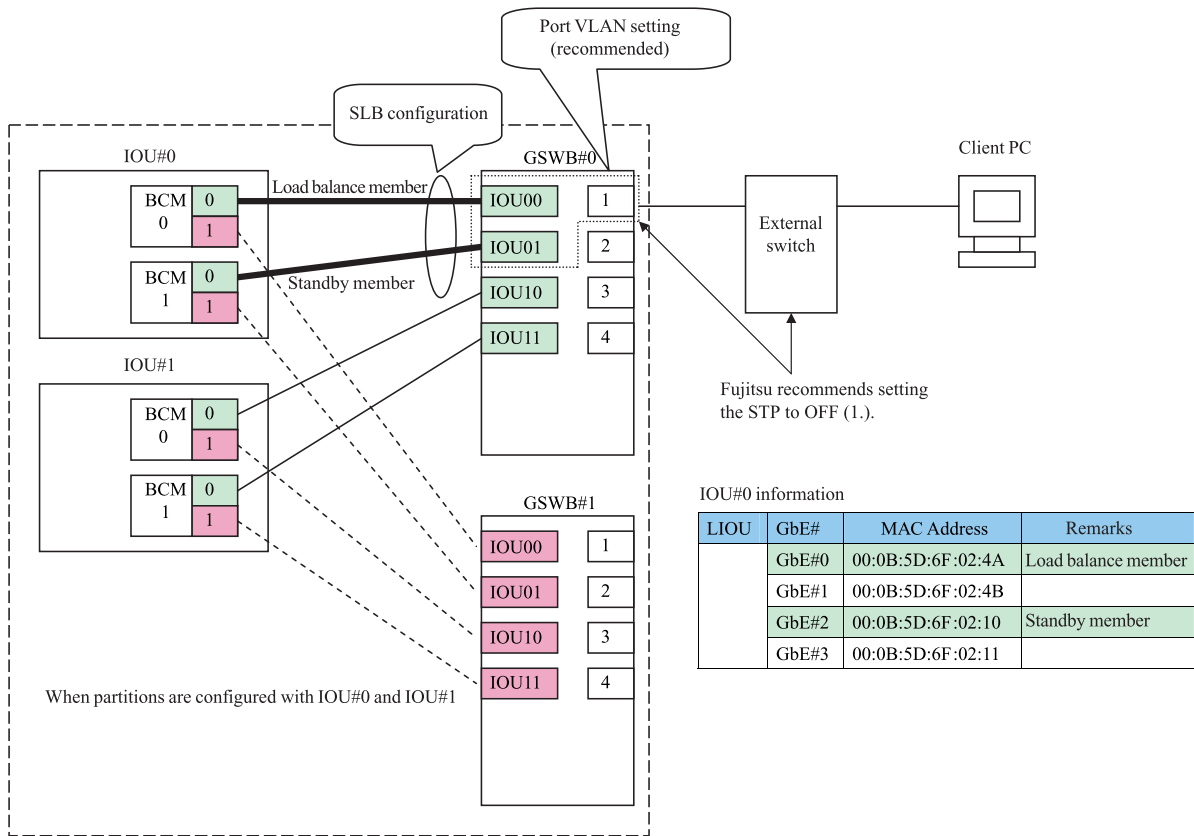


Figure 8.4 Notes on team setting (BACS setting)
(PRIMEQUEST 580A/540A/580/540/480/440)

- Example 1 of Smart Load Balance (SLB) configuration

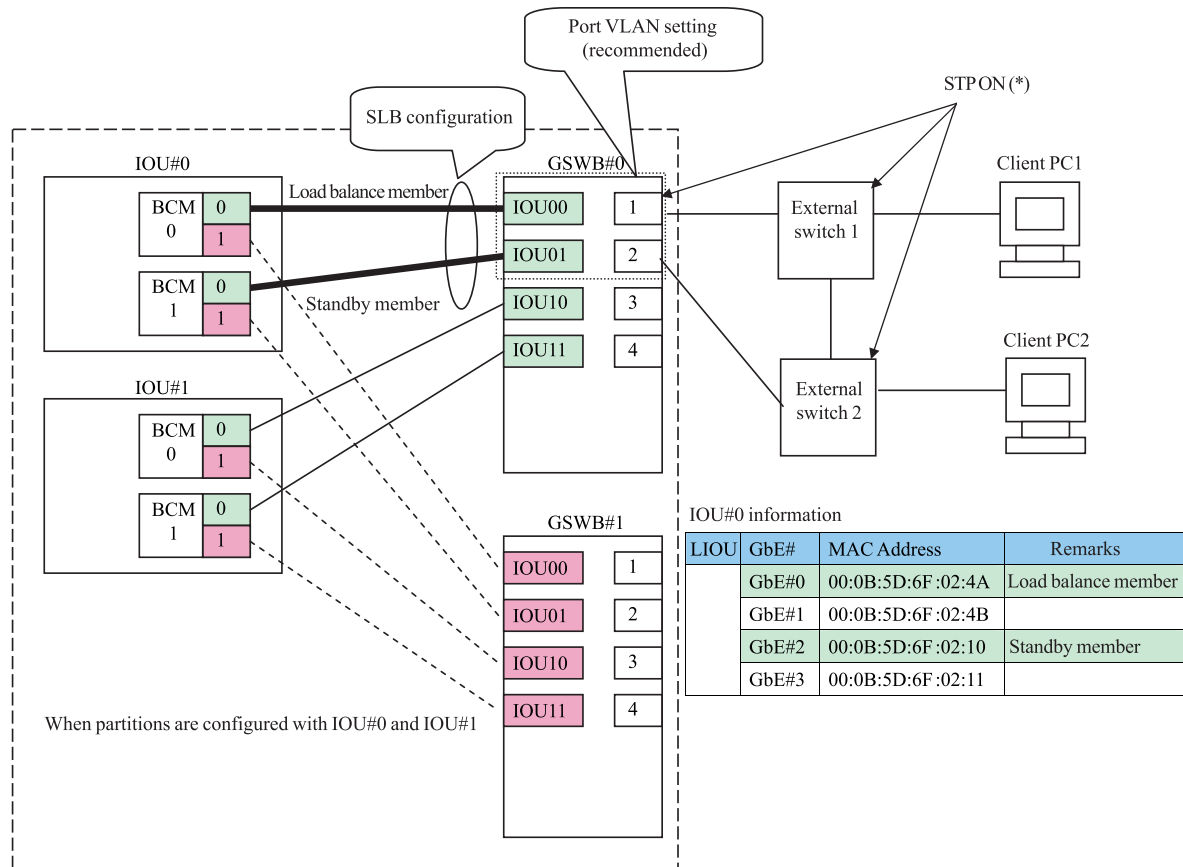


Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.5 Example 1 of Smart Load Balance (SLB) configuration

For how to set a port VLAN in a GSWB, see Section 4.12, "VLAN Menu," of the "PRIMEQUEST GSWB User's Manual" (C122-E028EN).

- Example 2 of Smart Load Balance (SLB) configuration

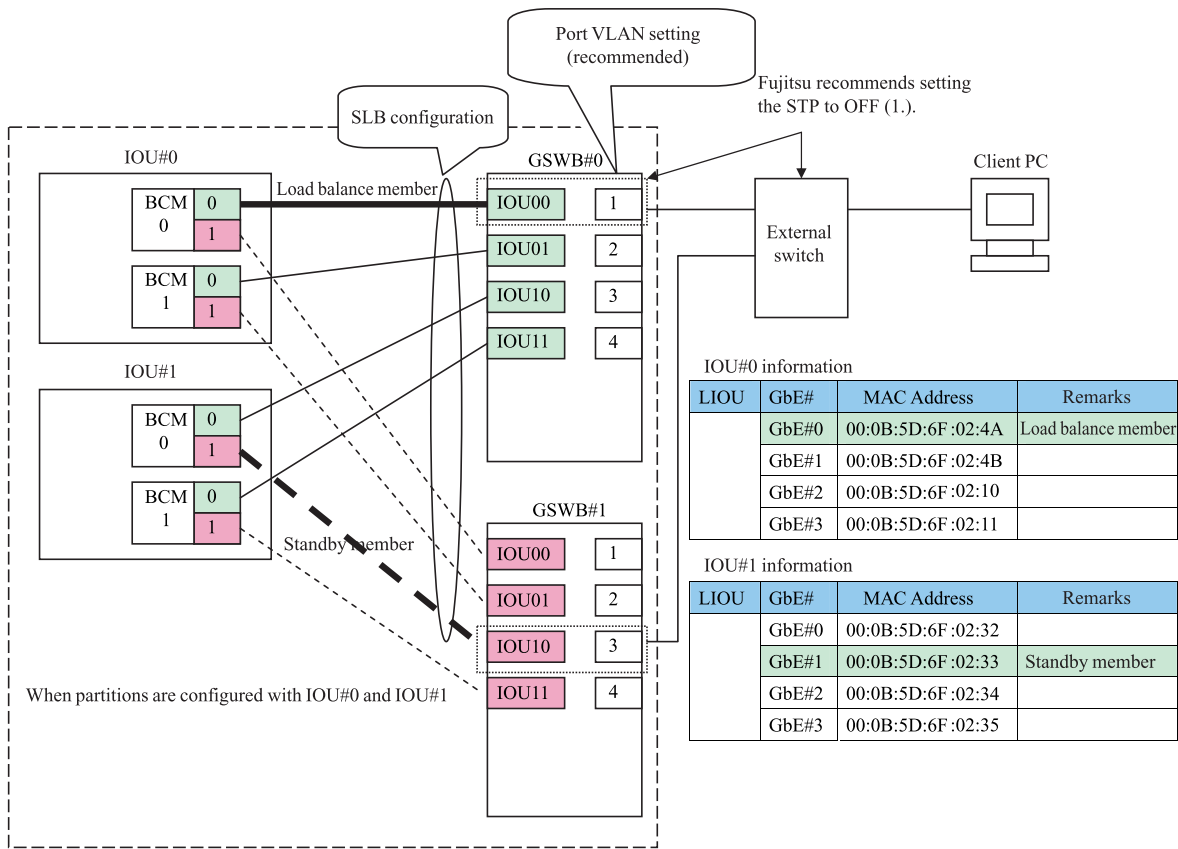


Note: As a network loop has been generated, set the STP to ON.

Figure 8.6 Example 2 of Smart Load Balance (SLB) configuration

For how to set a port VLAN in a GSGB, see Section 4.12, "VLAN Menu," of the "PRIMEQUEST GSGB User's Manual" (C122-E028EN).

- Example 3 of Smart Load Balance (SLB) configuration

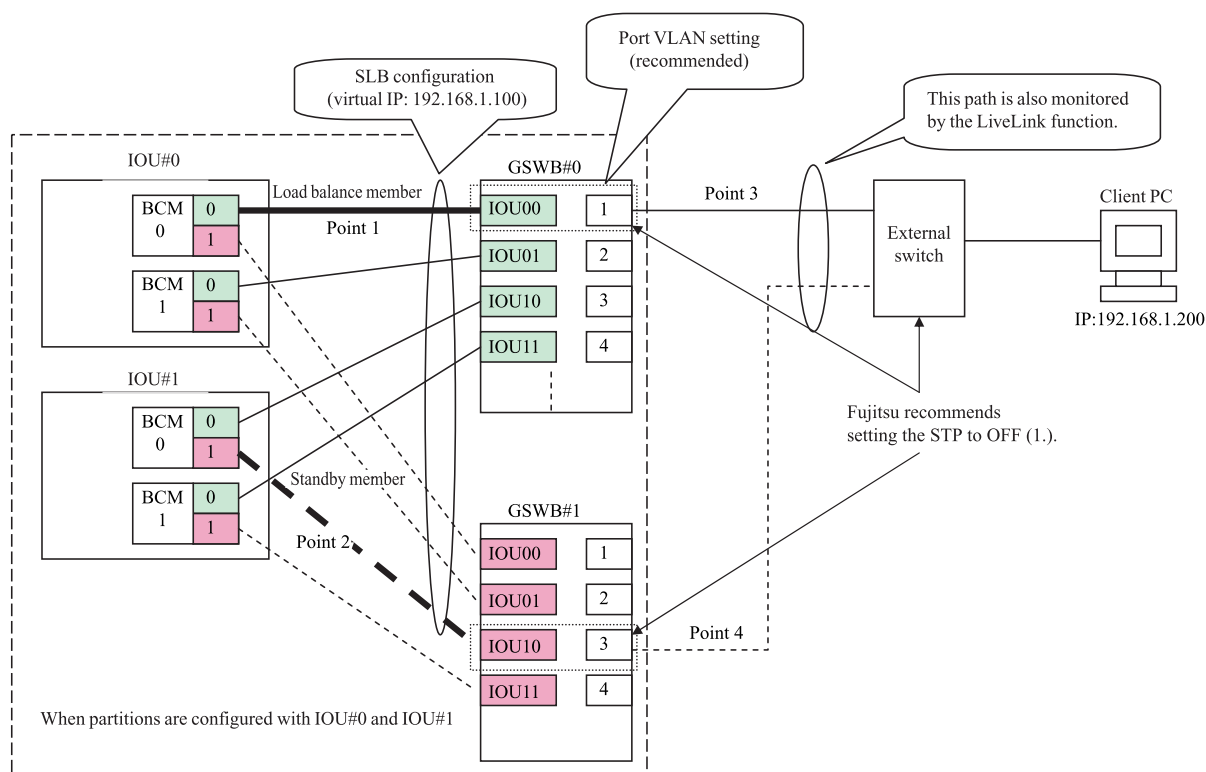


Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.7 Example 3 of Smart Load Balance (SLB) configuration

For how to set a port VLAN in a GSWB, see Section 4.12, "VLAN Menu," of the "PRIMEQUEST GSWB User's Manual" (C122-E028EN).

- Example 1 of Smart Load Balance (SLB + LiveLink) configuration

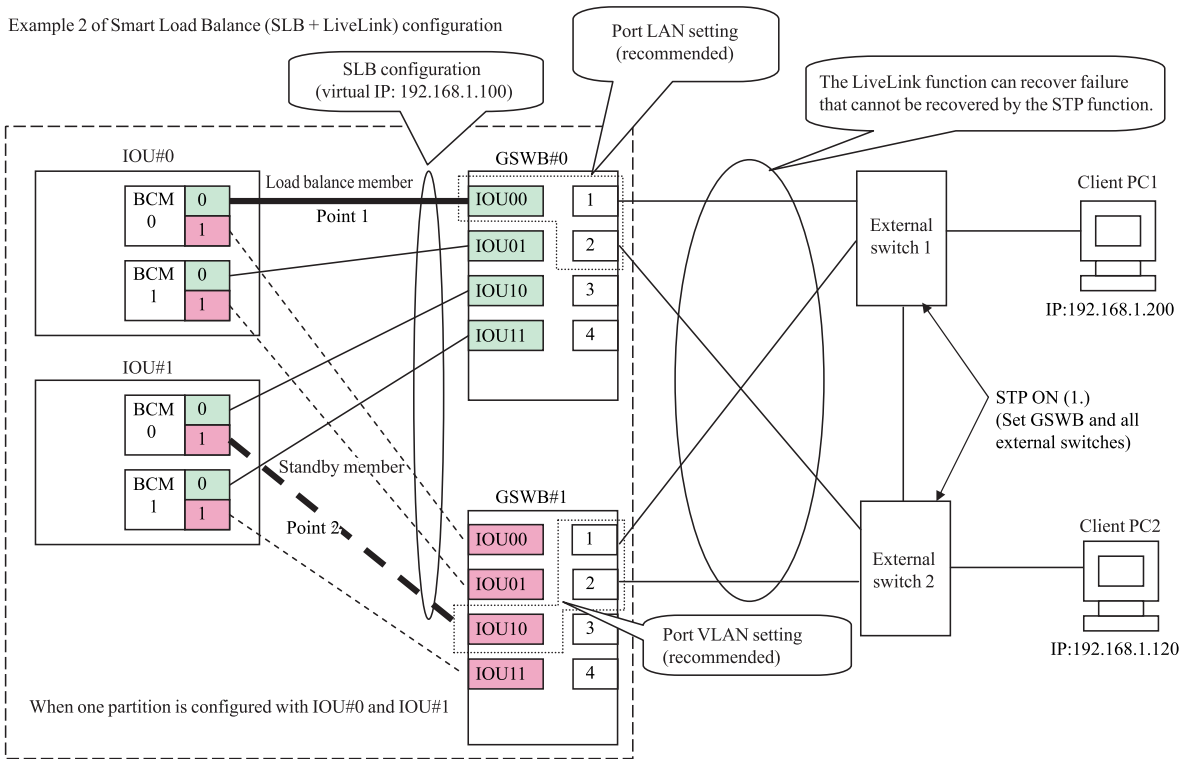


Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.8 Example 1 of Smart Load Balance (SLB + LiveLink) configuration

For how to set a port VLAN in a GSWB, see Section 4.12, "VLAN Menu," of the "PRIMEQUEST GSWB User's Manual" (C122-E028EN).

- Example 2 of Smart Load Balance (SLB + LiveLink) configuration



Note: As a network loop has been generated, set the STP to ON. GSWB and all external switches need to be set.

Figure 8.9 Example 2 of Smart Load Balance (SLB + LiveLink) configuration

For how to set a port VLAN in a GSWB, see the "*PRIMEQUEST GSWB User's Manual*" (C122-E028EN).

8.1.1 Broadcom LiveLink settings

The conventional SLB (Smart Local Balancing) function can only detect a link error between the Broadcom Ethernet chip and nearest Ethernet device, and perform recovery to the secondary side (by switching traffic). Conversely, the LiveLink function detects link errors over switches and performs traffic switching to a normal route.

(The function periodically checks communications between respective team members and respective targets, and switches to the secondary route if communication on the primary route fails.)

- Points where errors can be detected and recovered by the SLB function: Point 1 and point 2
- Points where errors can be detected and recovered by the SLB + LiveLink function: Point 1, point 2, point 3, and point 4 (See Configuration Example 1.)
- Notes on using LiveLink
 - LiveLink is only available for Smart Load Balance and Failover. [SLB (Auto-Fallback Disable) is not supported.])
 - LiveLink cannot be used on Tag VLAN.
 - The target must be on a subnet where a team member exists.
 - Up to four targets can be specified.
 - The time delay (switching time) between initial path error detection and actual switching is determined based on "Probe interval" and "Maximum retransmission number of probe."
$$\text{Switching time} = \text{"Probe interval"} \times \text{"Maximum retransmission number of probe"}$$
 - This function does not include the Auto-Fallback Disable function. Therefore, when the primary route is recovered from error status to normal status, traffic is automatically switched from the secondary route to the primary route.
 - The time delay during switch back from the secondary route to the primary route following recovery of a path from error status is calculated as follows: "Probe interval" x "Maximum retransmission number of probe."
 - If multiple targets are set, the system switches to the secondary route when all link loss is detected between the primary route and the target (for cases where at least 1 link between the secondary route and the target is normal.)

IOU#0 information

LIU	GbE#	MAC Address	Fixed IP address	Remarks
	GbE#0	00:0B:5D:6F:02:4A	192.168.1.10	Load balance member
	GbE#1	00:0B:5D:6F:02:4B		
	GbE#2	00:0B:5D:6F:02:10		
	GbE#3	00:0B:5D:6F:02:11		

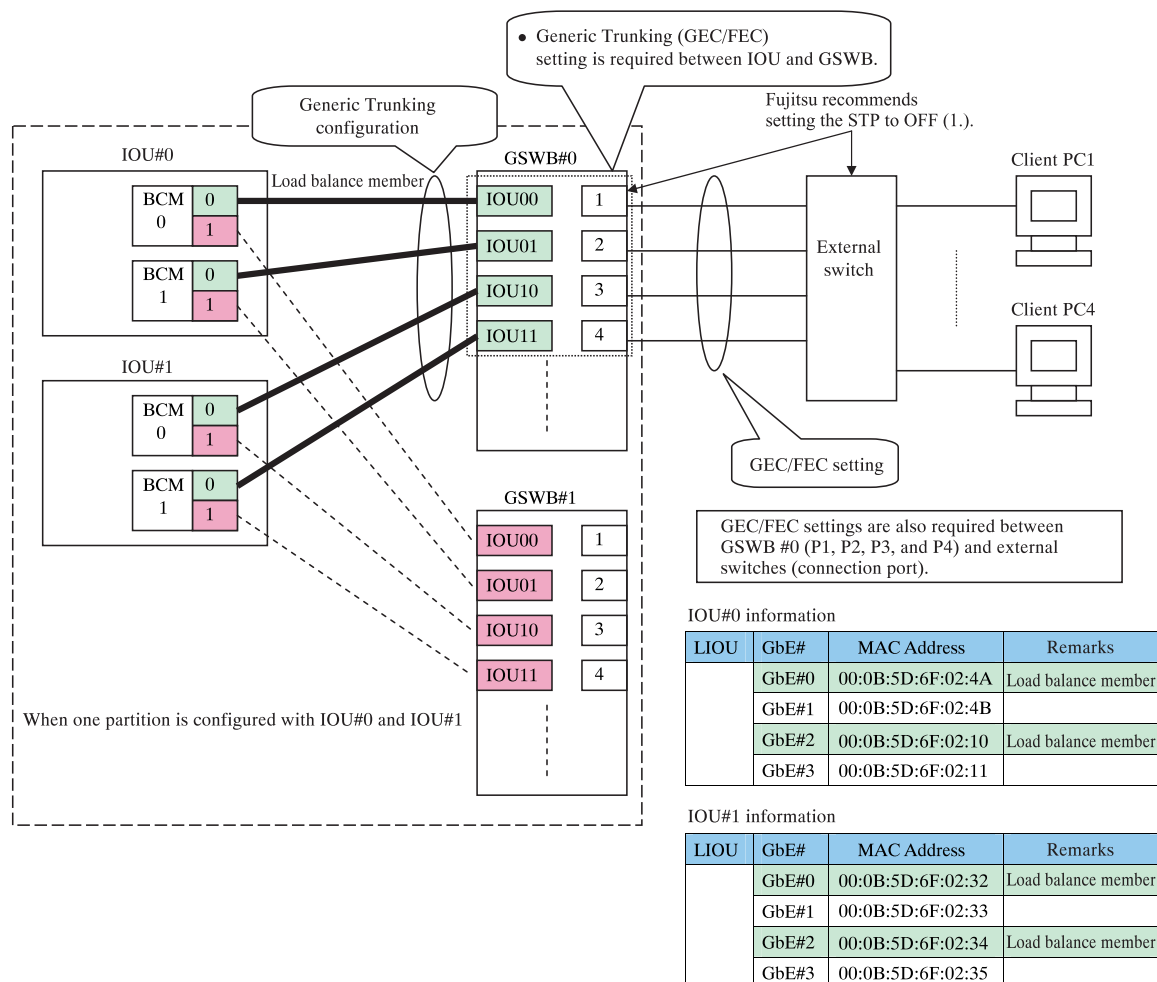
IOU#1 information

LIU	GbE#	MAC Address	Fixed IP address	Remarks
	GbE#0	00:0B:5D:6F:02:32		
	GbE#1	00:0B:5D:6F:02:33	192.168.1.11	Standby member
	GbE#2	00:0B:5D:6F:02:34		
	GbE#3	00:0B:5D:6F:02:35		

Figure 8.10 Broadcom LAN information of IO unit

Remarks: The function periodically checks the normality of paths between the fixed IP: 192.168.1.10 (192.168.1.11) and client PC of IP: 192.168.1.200. If the local path fails, this function switches between the load balance member and standby member on the Broadcom Ethernet chip.

- Example of Generic Trunking (GEC/FEC) configuration



Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.11 Example of Generic Trunking (GEC/FEC) configuration

For how to set a port VLAN in a GSWB, see Section 4.12, "VLAN Menu," of the *"PRIMEQUEST GSWB User's Manual"* (C122-E028EN).

For how to set GEC/FEC in a GSWB, see Section 4.14, "Channel Group Menu," of the *"PRIMEQUEST GSWB User's Manual"* (C122-E028EN).

For how to set Generic Trunking for IOU, see 5.2.11, "Port ranking function," of the *"PRIMEQUEST GSWB User's Manual"* (C122-E028EN)

8.2 Outline (PRIMEQUEST 520A/520/420)

The Teaming function (multi-path function) using Broadcom Ethernet supports the following on the PRIMEQUEST 520A/520/420:

The Teaming function also uses the BASP (Broadcom Advanced Server Program) function within the BACS2 (Broadcom Advanced Control Suite2) utility.

(1) Smart Load Balance and Fail Over (+LiveLink)

This function disperses load among load balance members. If all members are encountering trouble, traffic is transferred to a standby member.

Upon the recovery of one or more load balance members, traffic is switched from the standby member to a load balance member. The LiveLink function is only available in this mode.

Remarks: The Livelink function monitors for link loss between all load balance members and the specified target and transfers traffic to normally operating load balance members.

(2) Generic Trunking (FEC/GEC)/802.3ad-Draft Static

This is a load balance function that uses PagP (Port Aggregation Protocol). A switch to be interfaced must have this function or an equivalent one. This function also actualizes fail-over among load balance members.

(3) Link Aggregation (802.3ad)

This is a load balance function that uses LACP (Link Aggregation Control Protocol). A switch to be interfaced must have this function or an equivalent one. This function also actualizes fail-over among load balance members.

(4) SLB (Auto-Fallback Disable)

This function is basically the same as (1) "Smart Load Balance and Fail Over" but does not switch traffic from a standby member to a load balance member automatically. Moreover, this function cannot be used concurrently with LiveLink.

Remarks: The Link Aggregation (802.3ad) function is not supported.

Notes:

- The message "Broadcom 5704C chip is not supported" is output, but operation can continue without being affected.

- STP should be disabled when configuring SLB without using the LiveLink function.
Doing so enables the down time to be kept to a minimum when determining the spanning tree loop at the onset of a fail over.
- BASP (Broadcom Advanced Server Program: Teaming Software) does not support Microsoft Network Load Balancing (NLB).
- BASP (Broadcom Advanced Server Program: Teaming Software) operations require that the user be logged in with Administrator privileges.
- A team configuration name should be a character string from 1 to 39 characters in length.
- A team name must not begin with a space or contain any of the following characters:
& \ / : * ? < > | "
- A team name must be unique.
- When using the Generic Trunking function, you cannot specify a standby member.
- Click the [Fallback] button (on the Team Properties tab) when switching traffic back to a load balance member from a standby member by using SLB (Auto-Fallback Disable).
- The function cannot be used under a Dynamic Host Configuration Protocol environment.
- Up to eight members can be specified.
- All team members must be configured by using Broadcom NetXtreme Gigabit Ethernet.
- Method of identifying a physical port on the PRIMEQUEST 520A/520/420
 - 1 Identify the physical position of a Broadcom Ethernet port to be controlled by BACS 2.
A Broadcom Ethernet port is displayed on Windows Server 2003 OS (Device Manager) or BACS 2 (Broadcom Advanced Control Suite 2) as follows:
"Broadcom NetXtreme Gigabit Fiber #<No>"
Next, identify the physical position of the Broadcom Ethernet port by referring to the MAC address information on Ethernet ports.

Confirm the MAC address of the Broadcom Ethernet port on the relevant IOU by using Web UI.

Example: WEB-UI -[System] - [IOU] - [IOU]

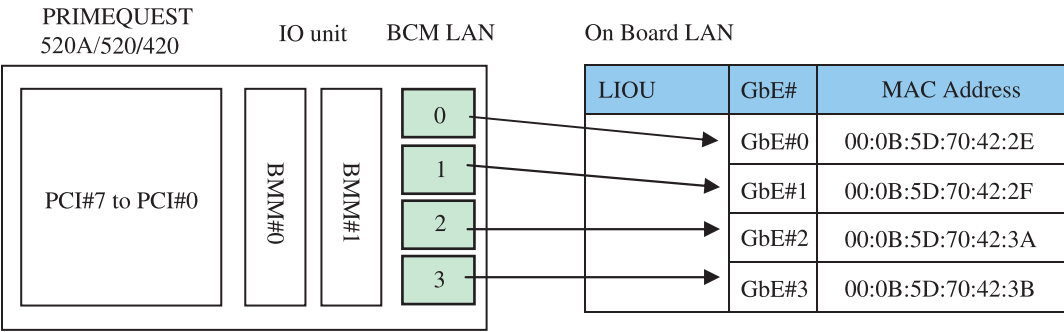


Figure 8.12 Physical positions of Ethernet ports (PRIMEQUEST 520A/520/420)

- 2 Confirm the MAC address of "Broadcom NetXtreme Gigabit Ethernet #<No>" on BACS 2 and identify the physical position.

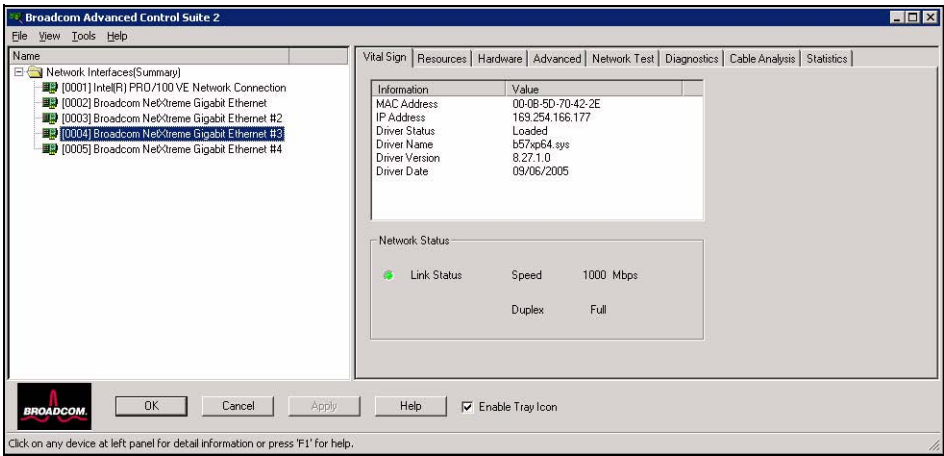
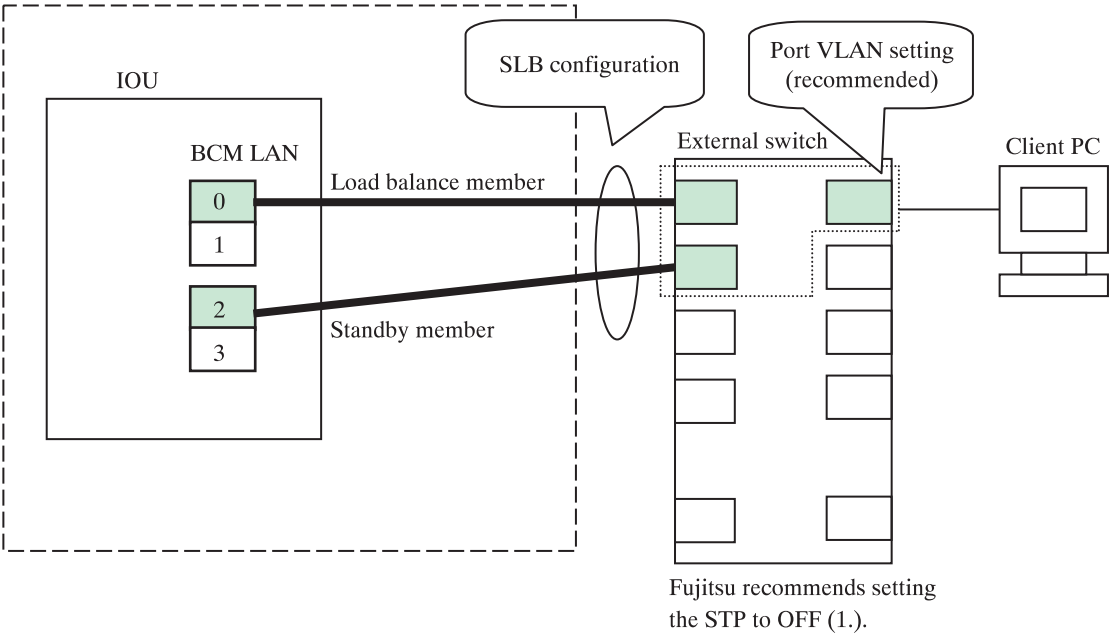


Figure 8.13 [Broadcom Advanced Control Suite 2] dialog box

- Example 1 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)



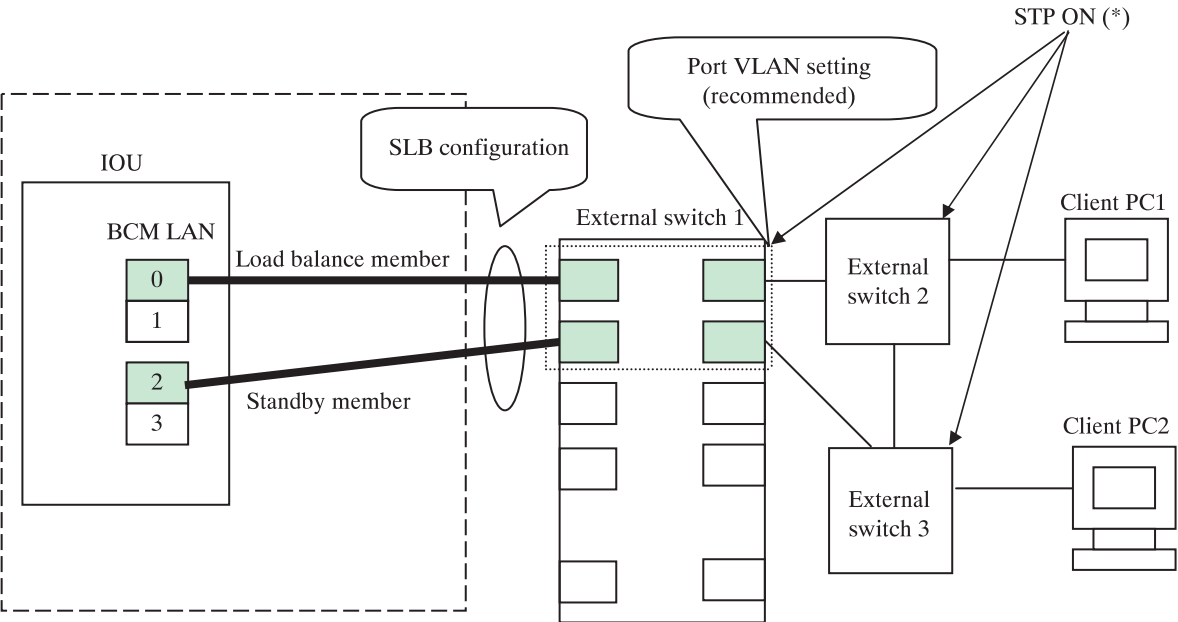
IO unit Broadcom LAN information

LIU	GbE#	MAC Address	Remarks
	GbE#0	00:0B:5D:70:42:2E	Load balance member
	GbE#1	00:0B:5D:70:42:2F	
	GbE#2	00:0B:5D:70:42:3A	Standby member
	GbE#3	00:0B:5D:70:42:3B	

Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.14 Example 1 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)

- Example 2 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)



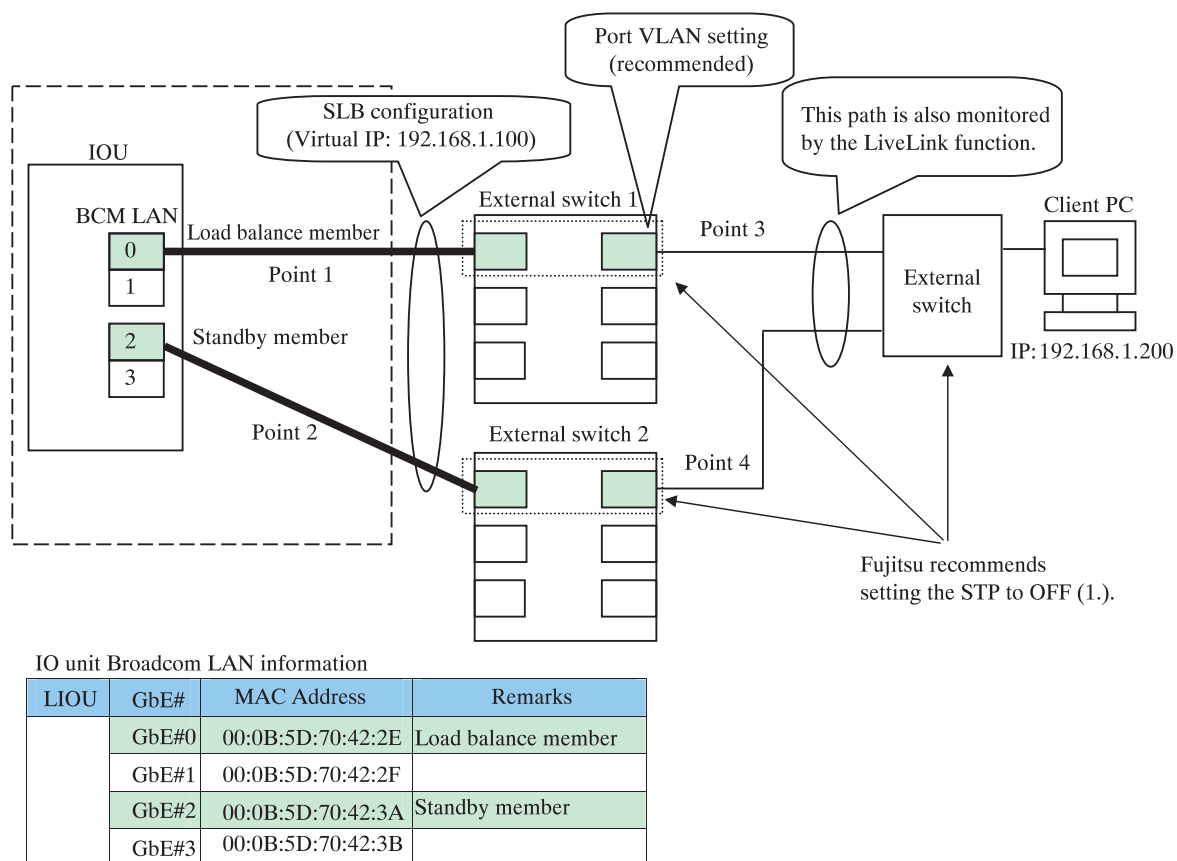
IO unit Broadcom LAN information

LIQU	GbE#	MAC Address	Remarks
	GbE#0	00:0B:5D:70:42:2E	Load balance member
	GbE#1	00:0B:5D:70:42:2F	
	GbE#2	00:0B:5D:70:42:3A	Standby member
	GbE#3	00:0B:5D:70:42:3B	

Note: As a network loop has been generated, set the STP to ON.

Figure 8.15 Example 2 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)

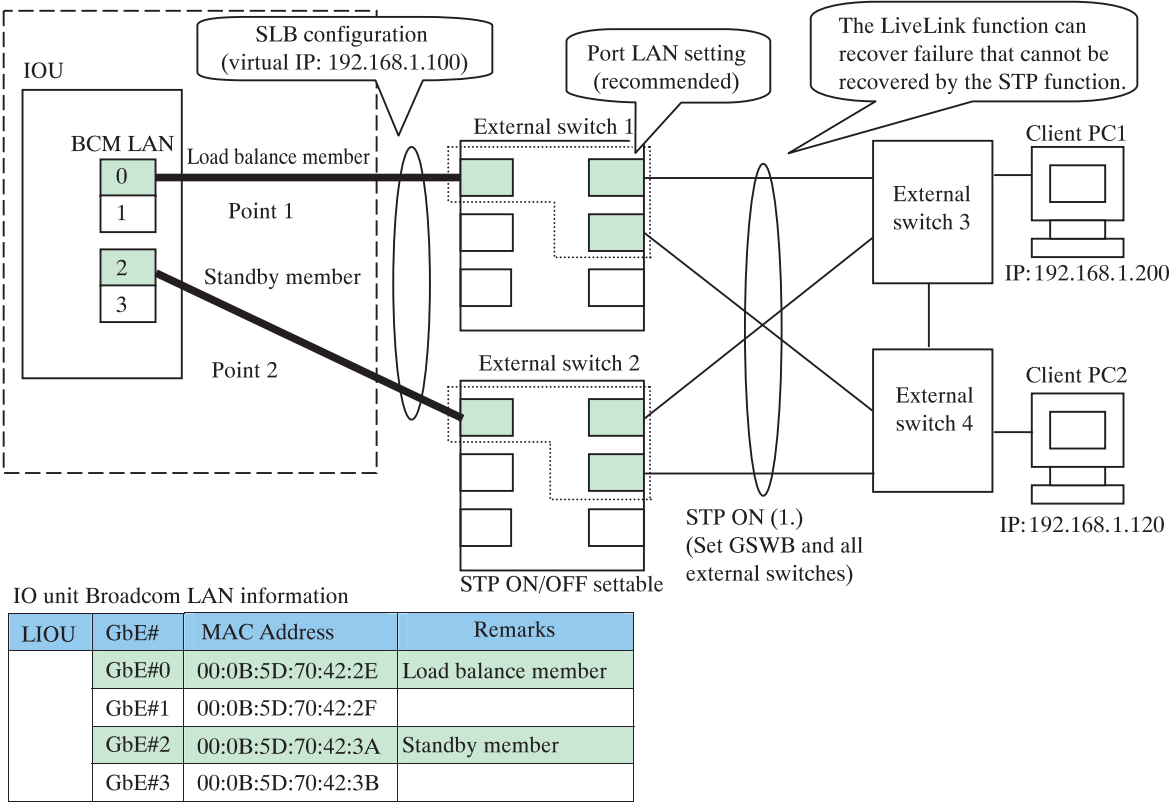
- Example 1 of Smart Load Balance (SLB + LiveLink) configuration (PRIMEQUEST 520A/520/420)



Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.16 Example 1 of Smart Load Balance (SLB) configuration (PRIMEQUEST 520A/520/420)

- Example 2 of Smart Load Balance (SLB + LiveLink) configuration (PRIMEQUEST 520A/520/420)



Note: As a network loop has been generated, set the STP to ON. GSWB and all external switches need to be set.

Figure 8.17 Example 2 of Smart Load Balance (SLB + LiveLink) configuration (PRIMEQUEST 520A/520/420)

8.2.1 Broadcom LiveLink settings

The conventional SLB (Smart Local Balancing) function can only detect a link error between the Broadcom Ethernet chip and nearest Ethernet device, and perform recovery to the secondary side (by switching traffic). Conversely, the LiveLink function detects link errors over switches and performs traffic switching to a normal route.

(The function periodically checks communications between respective team members and respective targets, and switches to the secondary route if the communication on the primary route fails.)

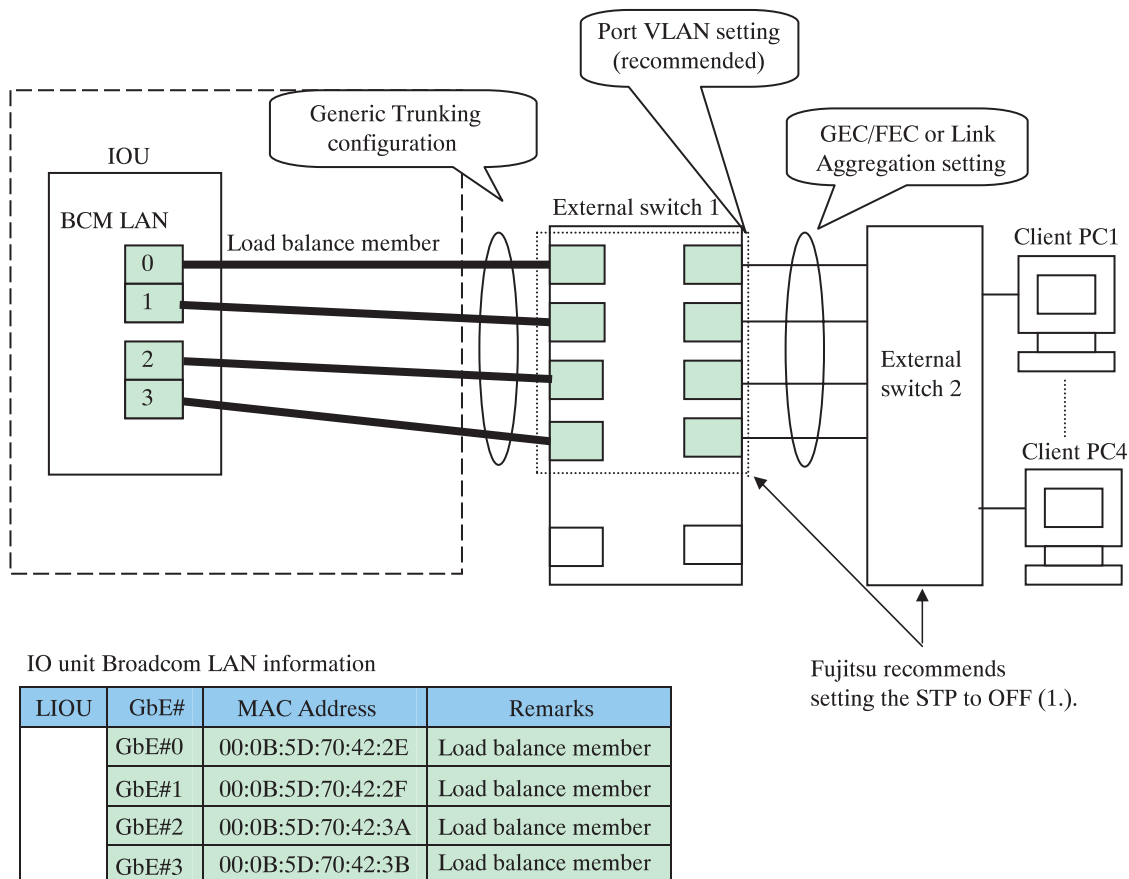
- Points where errors can be detected and recovered by the SLB function: Point 1 and point 2
- Points where errors can be detected and recovered by the SLB + LiveLink function: Point 1, point 2, point 3, and point 4 (See Configuration Example 1.)
- Notes on using LiveLink
 - LiveLink is only available for Smart Load Balance and Fail Over. [SLB (Auto-Fallback Disable) is not supported.]
 - LiveLink cannot be used on Tag VLAN.
 - The target must be on a subnet where a team member exists.
 - Up to four targets can be specified.
 - The time delay (switching time) between initial path error detection and actual switching is determined based on "Probe interval" and "Maximum retransmission number of probe."
Switching time = "Probe interval" x "Maximum retransmission number of probe"
 - This function does not include the Auto-Fallback Disable function. Therefore, when the primary route is recovered from error status to normal status, traffic is automatically switched from the secondary route to the primary route.
 - The time delay during switch back from the secondary route to the primary route following recovery of a path from error status is calculated as follows: "Probe interval" x "Maximum retransmission number of probe."
 - If multiple targets are set, the system switches to the secondary route when all link loss is detected between the primary route and the target (for cases where at least 1 link between the secondary route and the target is normal.)

LIQU	GbE#	MAC Address	Remarks	
	GbE#0	00:0B:5D:70:42:2E	192.168.1.10	Load balance member
	GbE#1	00:0B:5D:70:42:2F		
	GbE#2	00:0B:5D:70:42:3A	192.168.1.11	Standby member
	GbE#3	00:0B:5D:70:42:3B		

Figure 8.18 Broadcom LAN information of IO unit

Remarks: The function periodically checks the normality of paths between the fixed IP: 192.168.1.10 (192.168.1.11) and client PC of IP: 192.168.1.200. If the local path fails, this function switches between the load balance member and standby member on the Broadcom Ethernet chip.

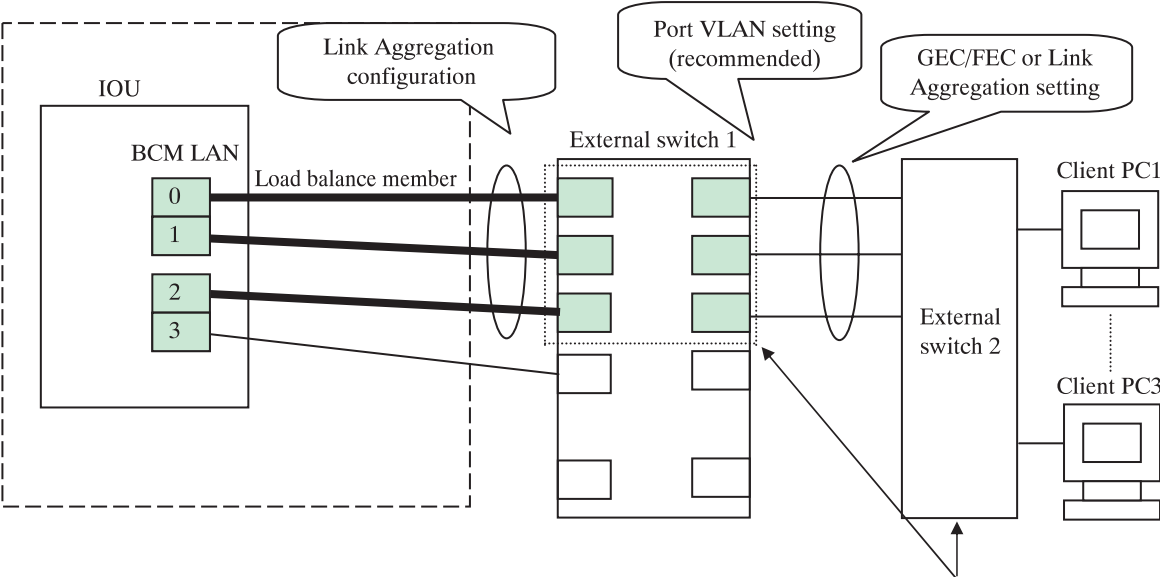
- Example of Generic Trunking (GEC/FEC) configuration (PRIMEQUEST 520A/520/420)



Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.19 Example of Generic Trunking (GEC/FEC) configuration (PRIMEQUEST 520A/520/420)

- Example of Link Aggregation (802.3ad) configuration (PRIMEQUEST 520A/520/420)



IO unit Broadcom LAN information

LIOW	GbE#	MAC Address	Remarks
	GbE#0	00:0B:5D:70:42:2E	Load balance member
	GbE#1	00:0B:5D:70:42:2F	Load balance member
	GbE#2	00:0B:5D:70:42:3A	Load balance member
	GbE#3	00:0B:5D:70:42:3B	

Note: As no network loop has been generated, Fujitsu recommends setting the STP to OFF.

Figure 8.20 Example of Link Aggregation (802.3ad) configuration (PRIMEQUEST 520A/520/420)

8.3 Smart Load Balance Setting Procedure

This section explains the procedure for setting Smart Load Balance.

- 1 From the [Start] menu, choose "Broadcom Advanced Control Suite 2."

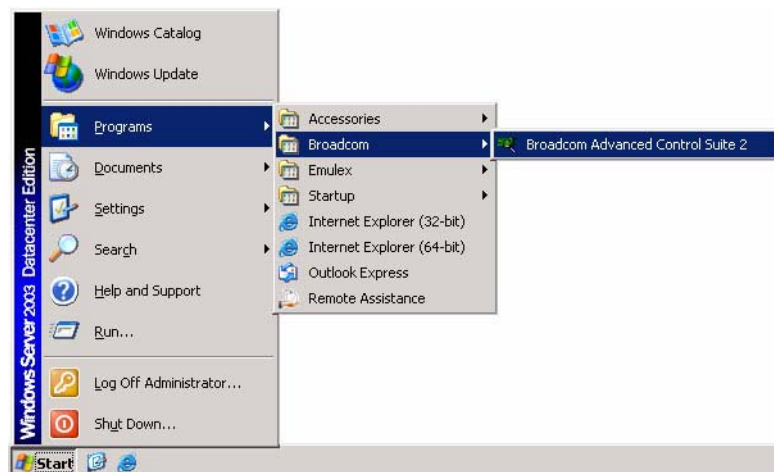


Figure 8.21 Starting Broadcom Advanced Control Suite 2

- 2 Select [Tools] → [Create Teams].

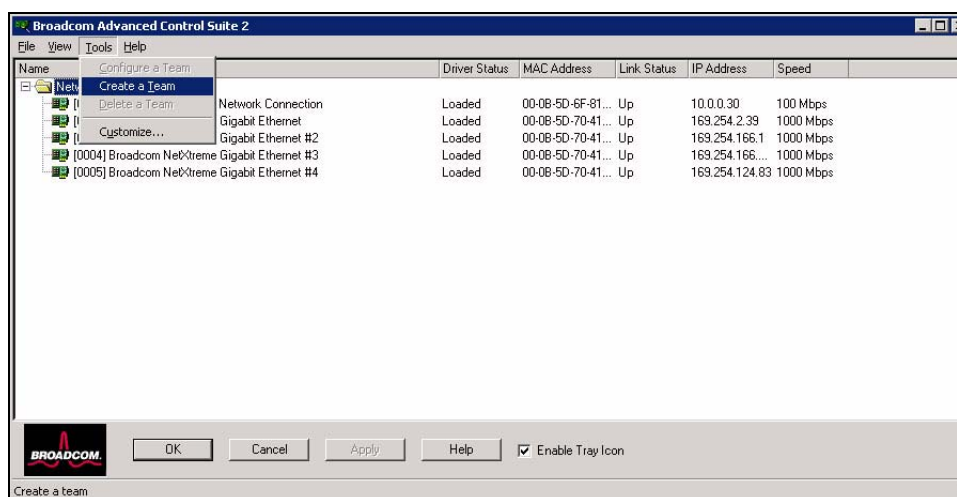


Figure 8.22 [Broadcom Advanced Control Suite 2] window

- 3 Enter a team identification name, select "Smart Load Balance and Failover," and then click [Next]. (The team name is arbitrary.)
If automatic fallback is not required, select "SLB (Auto-Fallback Disable)" and click [Next].
(The subsequent setting procedure is the same as for "Smart Load Balance and Failover.")

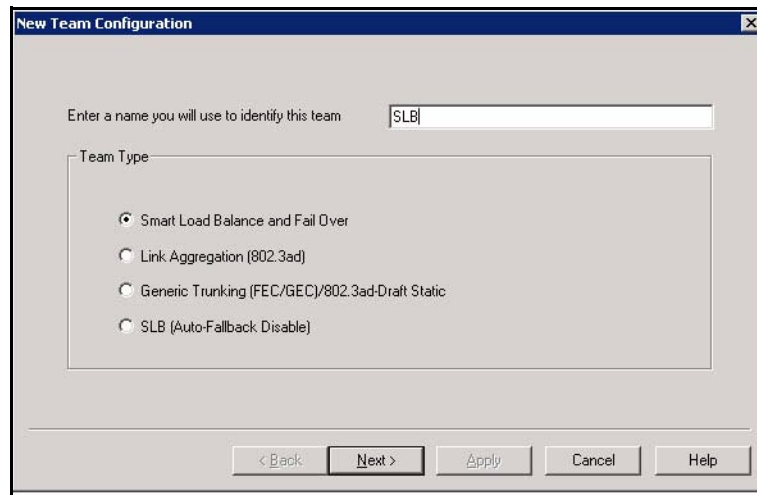


Figure 8.23 [Create Teams] dialog box

- 4 Select a load balance member from the list of available adapters and click the upper arrow button in the center of the screen. Next, select a standby member adapter from the list and click the lower arrow button in the center of the screen. Then click [Apply].

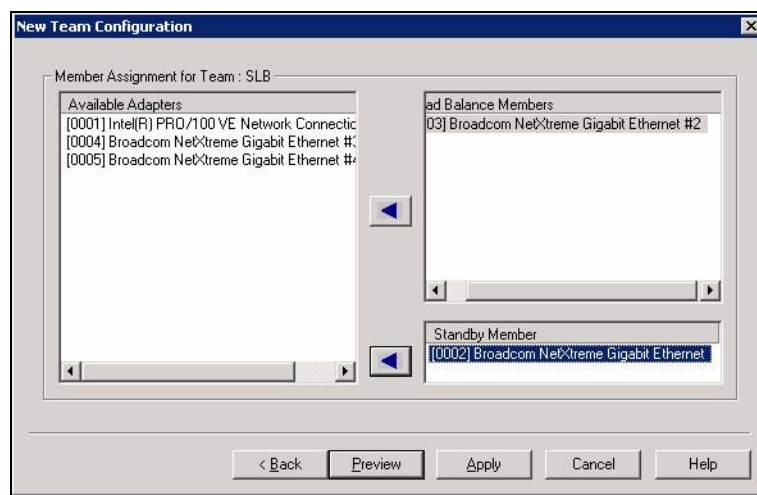


Figure 8.24 [Create Teams] dialog box

5 The following message dialog box appears. Click [Yes].

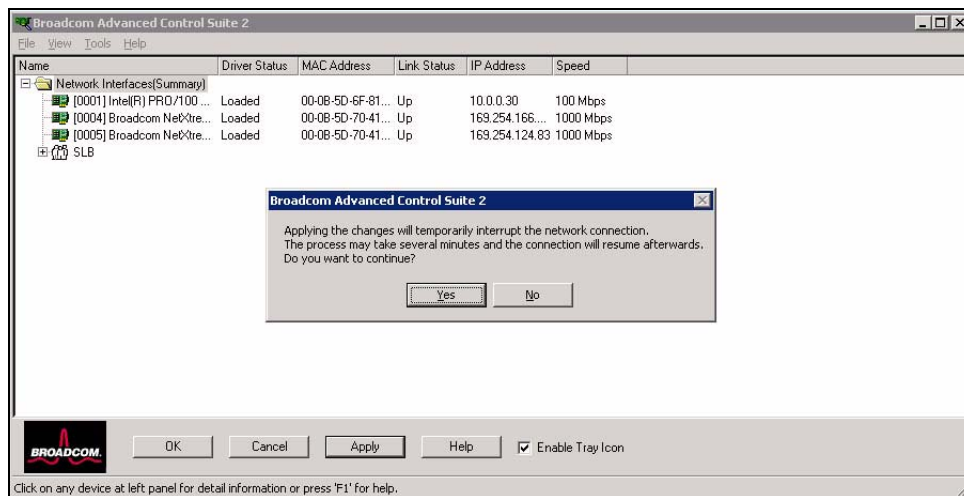


Figure 8.25 Message dialog box

6 When the team is created, a virtual adapter is also created on "Broadcom Advanced Control Suite 2."

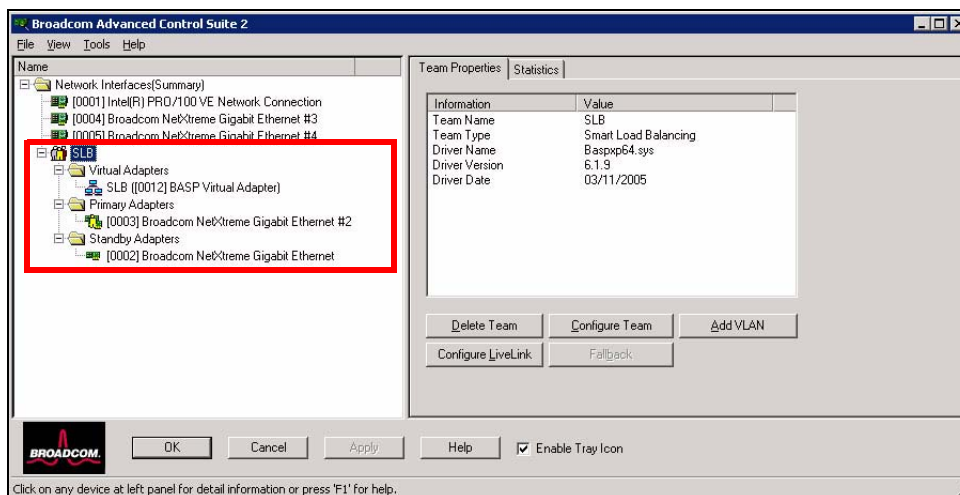


Figure 8.26 [Broadcom Advanced Control Suite 2] window

- 7 Set an IP address for the created virtual adapter on "Network connections" of Windows. (Device name "BAS Virtual Adapter" is assigned to the adapter.)

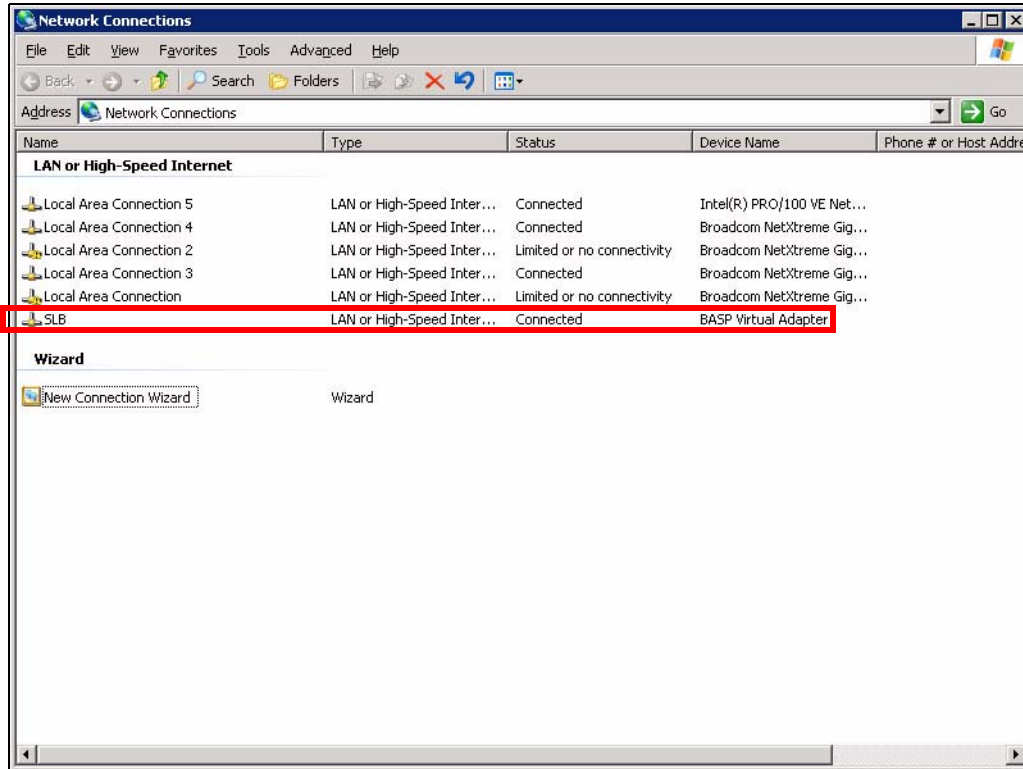


Figure 8.27 [Network connections] window

8.4 Smart Load Balance LiveLink Setting Procedure

This section explains the procedure for setting Smart Load Balance LiveLink.

- 1 From the [Start] menu, choose "Broadcom Advanced Control Suite 2."

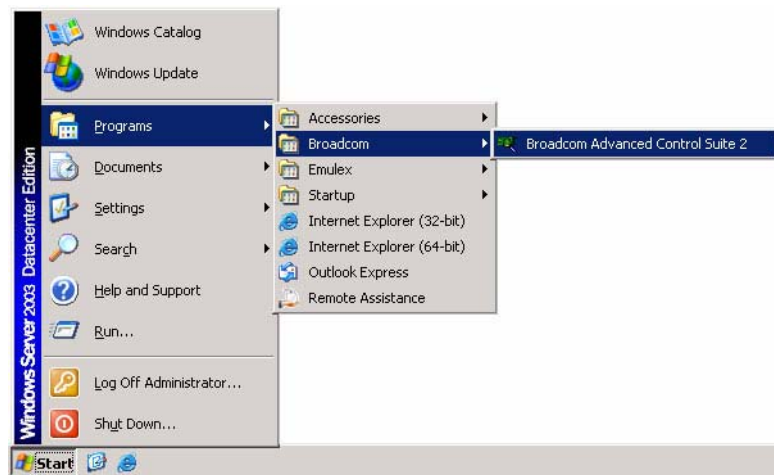


Figure 8.28 Starting Broadcom Advanced Control Suite 2

- 2 Select [Tools] → [Create Teams].

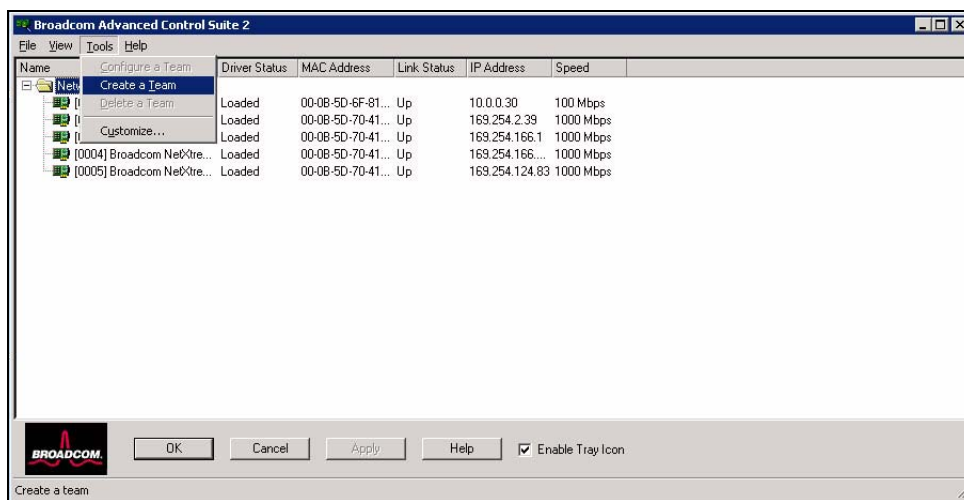


Figure 8.29 [Broadcom Advanced Control Suite 2] window

- 3 Enter a team identification name, select "Smart Load Balance and Failover," and then click [Next]. (The team name is arbitrary.)

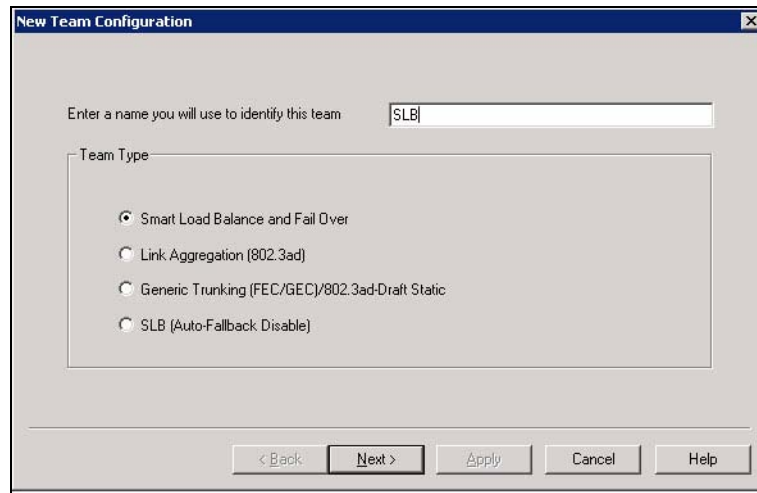


Figure 8.30 [Create Teams] dialog box

- 4 Select a load balance member from the list of available adapters and click the upper arrow button in the center of the screen. Next, select a standby member adapter from the list and click the lower arrow button in the center of the screen. Then click [Apply].

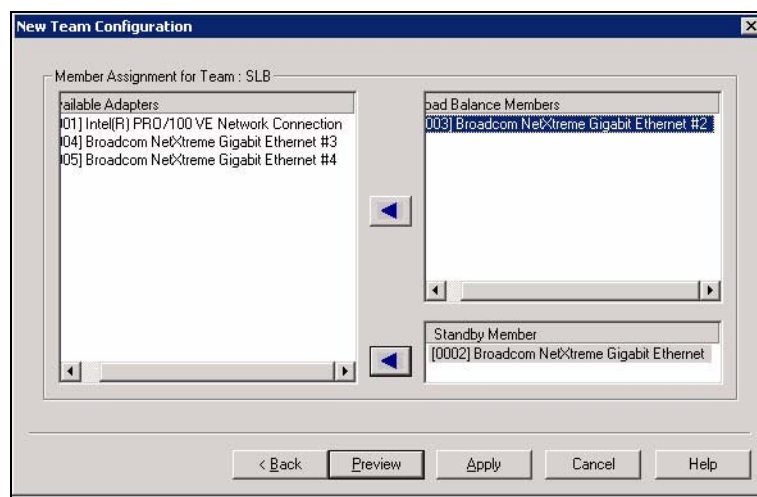


Figure 8.31 [Create Teams] dialog box

5 The following message dialog box appears. Click [Yes].

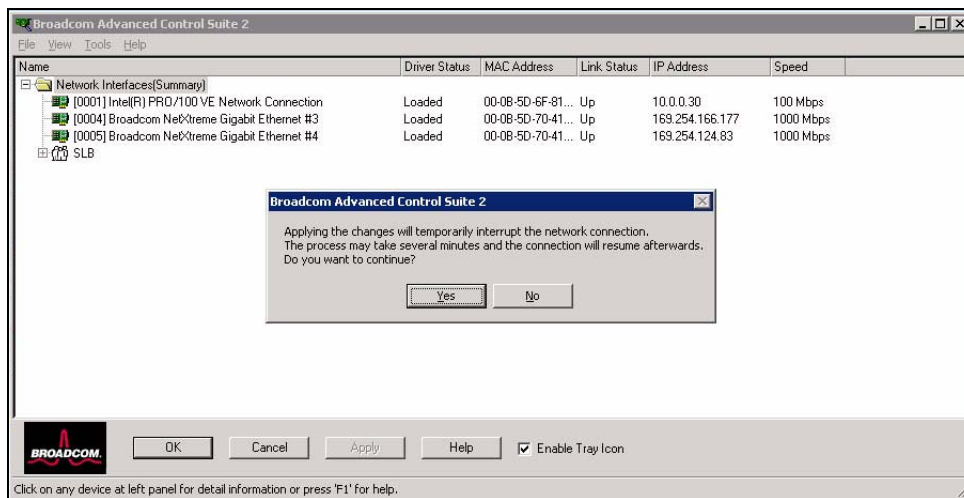


Figure 8.32 Message dialog box

6 When the team is created, a virtual adapter is also created on "Broadcom Advanced Control Suite 2."

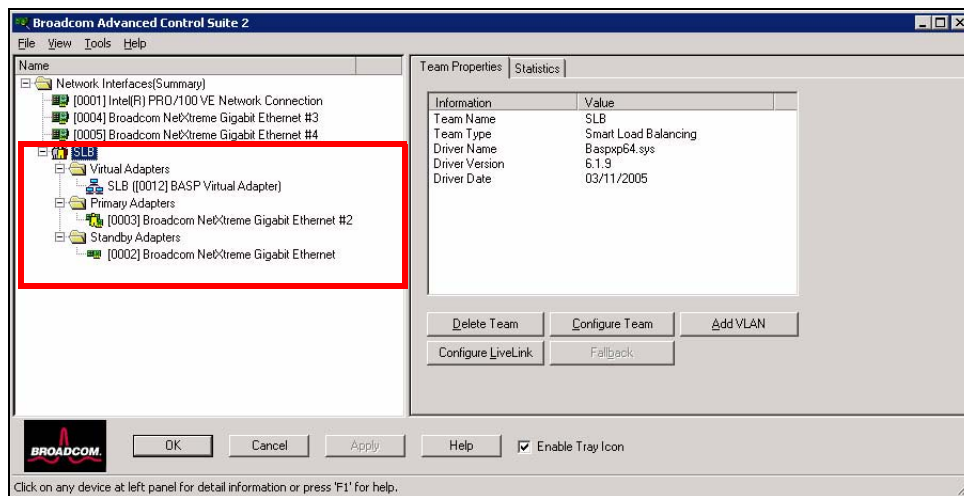


Figure 8.33 [Broadcom Advanced Control Suite 2] window

- 7 Click team name "SLB." The "LiveLink" setting menu appears. Click "LiveLink setting."

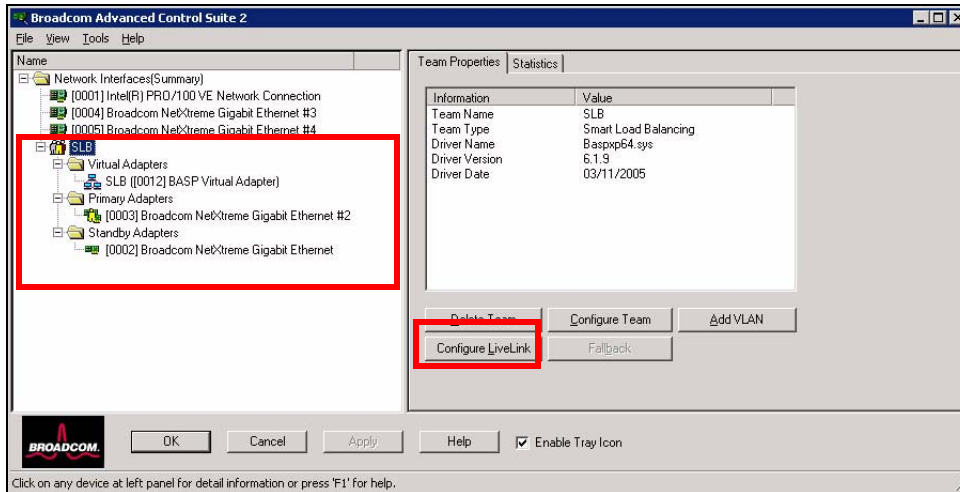


Figure 8.34 [Broadcom Advanced Control Suite 2] window

- 8 Select "Enable LiveLink."

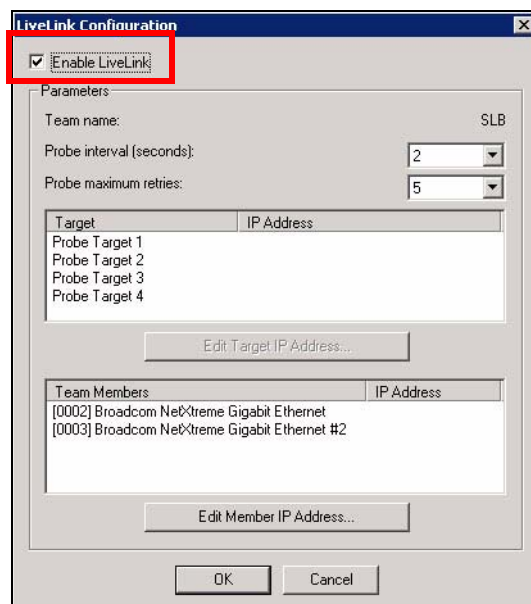


Figure 8.35 [LiveLink setting] dialog box

- 9 Set an IP address for a probe whose link error you want to detect.
Click "Edit selected IP address." (Up to four probes)

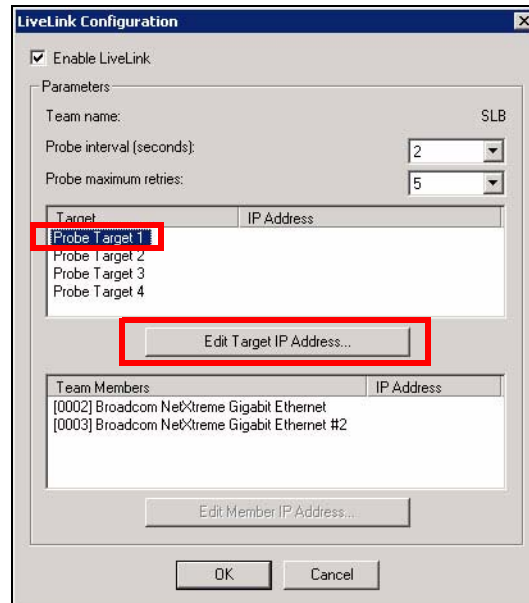


Figure 8.36 [LiveLink setting] dialog box

- 10 Set the IP address of a probe whose link error you want to detect, and then click [OK].

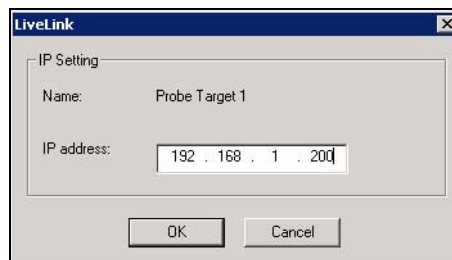


Figure 8.37 [LiveLink] dialog box

- 11 Set the IP address of the team member. Click "Edit member IP address."
(The member monitors the path of the selected probe.)

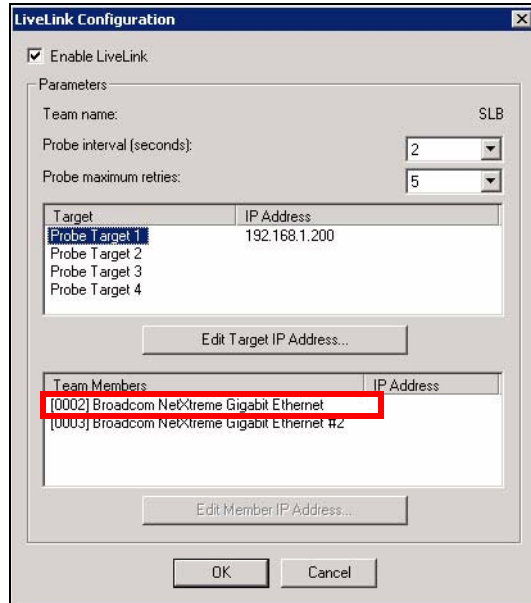


Figure 8.38 [LiveLink setting] dialog box

- 12 Set an IP address for every team member, and then click [OK].

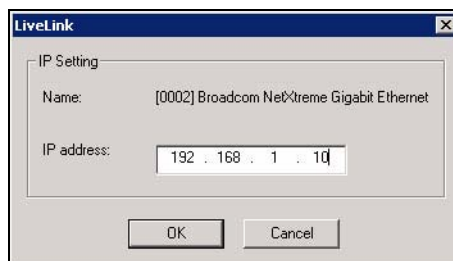


Figure 8.39 [LiveLink] dialog box

13 After the setting is complete, the following is displayed:

- Monitoring links between Target= 192.168.1.200 and Member = 192.168.1.10
Monitoring links between Target= 192.168.1.200 and Member = 192.168.1.11
- Switching time = "Probe interval" (2) x "Maximum retransmission number of probe" (5) = 10 seconds (12 seconds maximum)

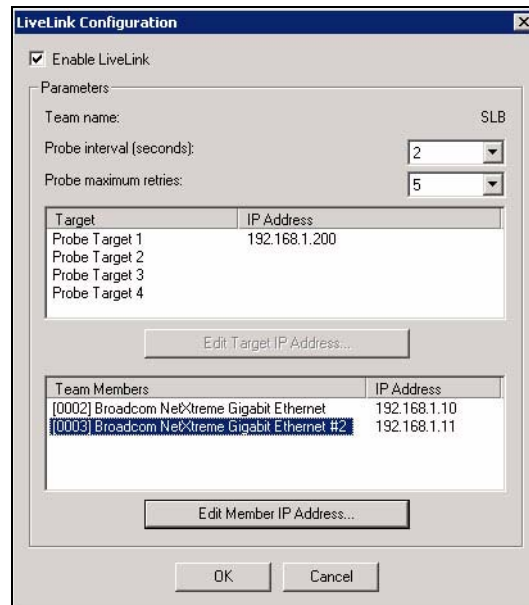


Figure 8.40 [LiveLink setting] dialog box

14 When the following window reappears, click [Apply].

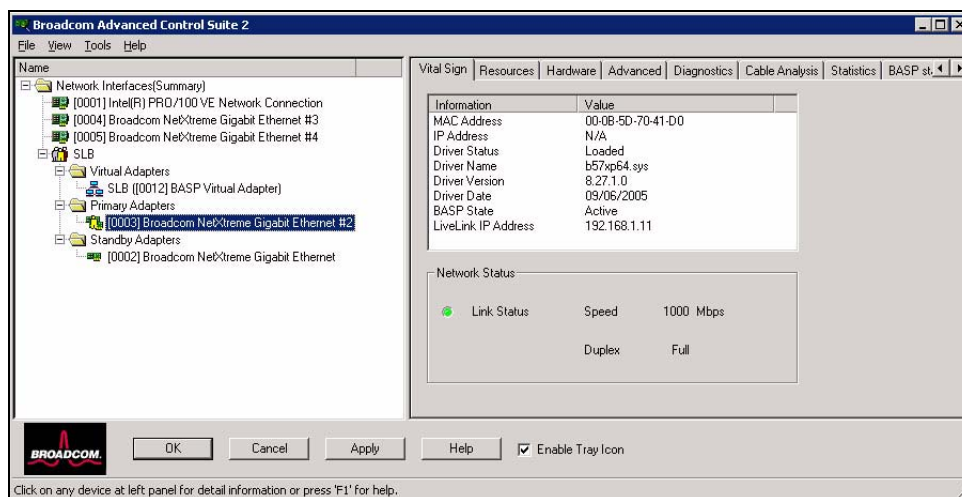


Figure 8.41 [Broadcom Advanced Control Suite 2] window

15 The following message dialog box appears. Click [Yes].

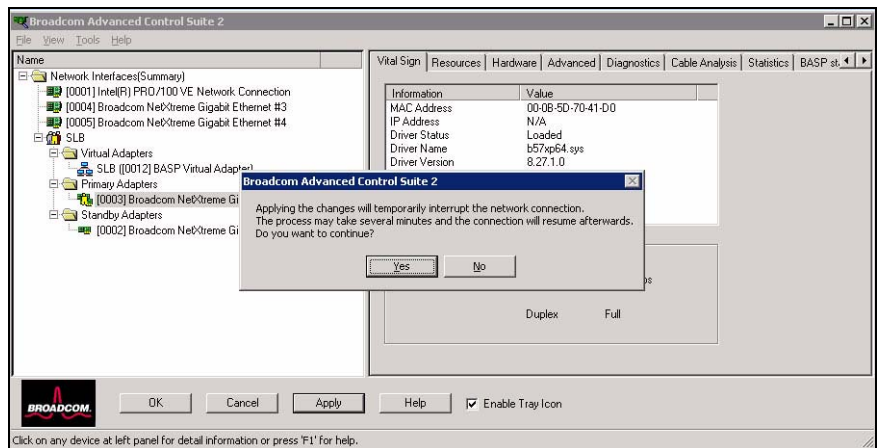


Figure 8.42 [Broadcom Advanced Control Suite 2] dialog box

16 After the LiveLink setting is complete, the following BACS dialog box is displayed:

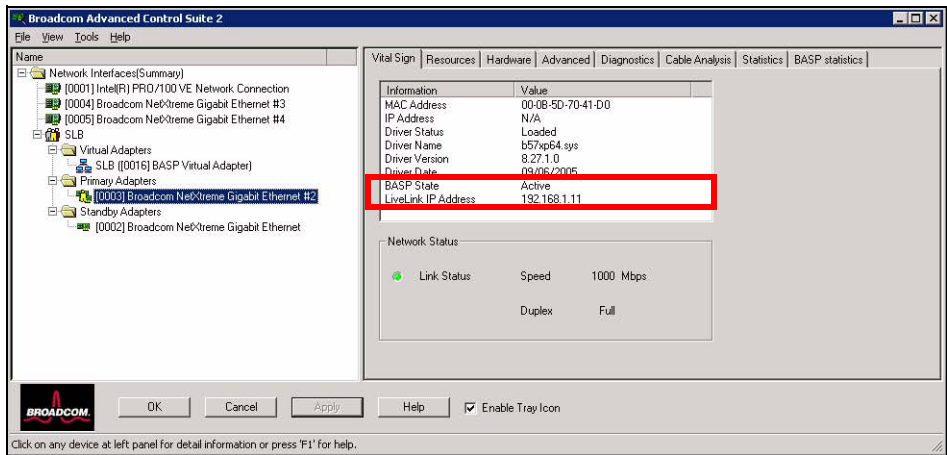


Figure 8.43 [Broadcom Advanced Control Suite 2] window

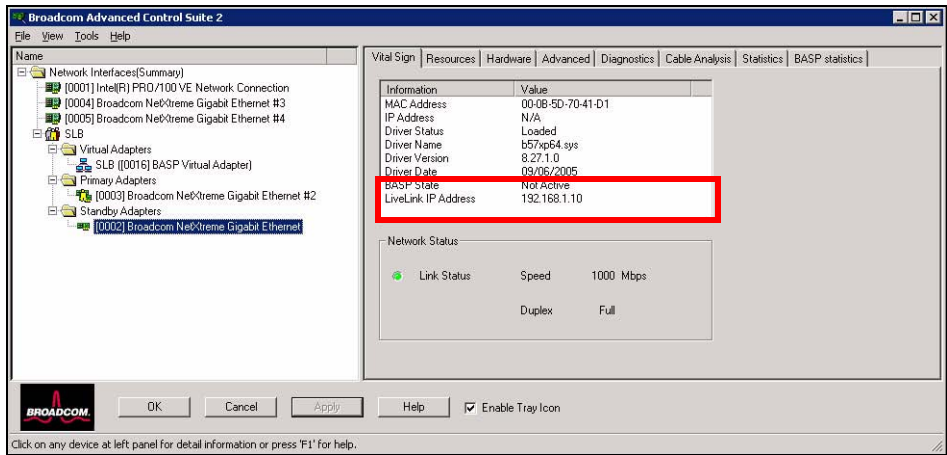


Figure 8.44 [Broadcom Advanced Control Suite 2] window

- 17 Set an IP address for the created virtual adapter on "Network connections" of Windows. (Device name "BAS Virtual Adapter" is assigned to the adapter.)

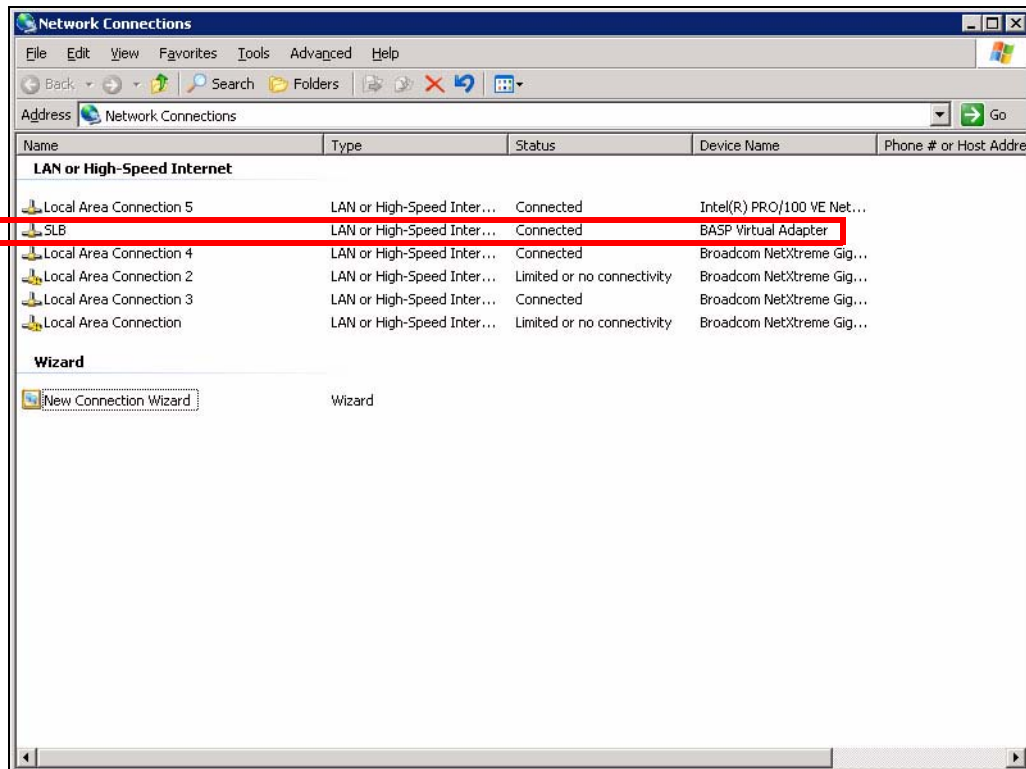


Figure 8.45 [Network connections] window

8.5 Generic Trunking (FEC/GEC) Setting Procedure

This section explains the procedure for setting generic trunking (FEC/GEC).

Generic trunking indicates Generic Trunking (FEC/GEC)/802.3ad-Draft Static.

- 1 From the [Start] menu, choose "Broadcom Advanced Control Suite 2."

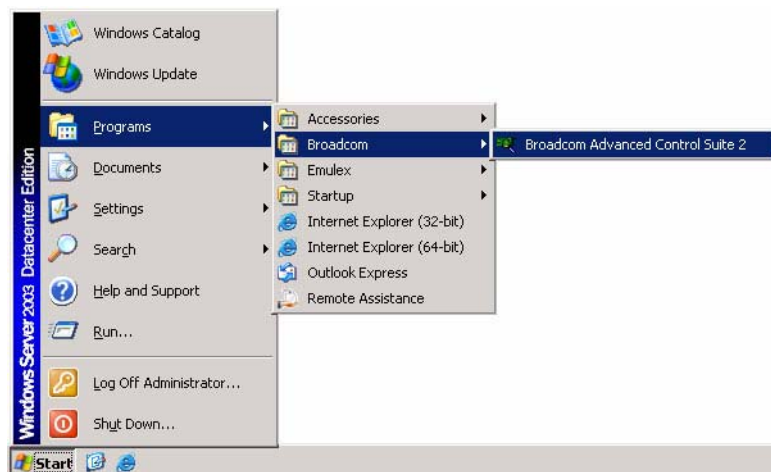


Figure 8.46 Starting Broadcom Advanced Control Suite 2

- 2 Select [Tools] → [Create Teams].

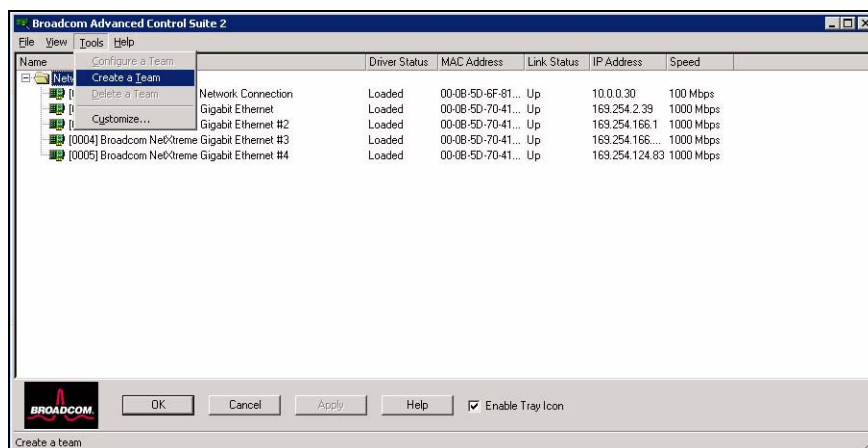


Figure 8.47 [Broadcom Advanced Control Suite 2] window

- 3 Enter a team identification name, select "Generic Trunking (FEC/GEC)/802.3ad-Draft Static," and then click [Next].

Remarks: The team name is arbitrary.

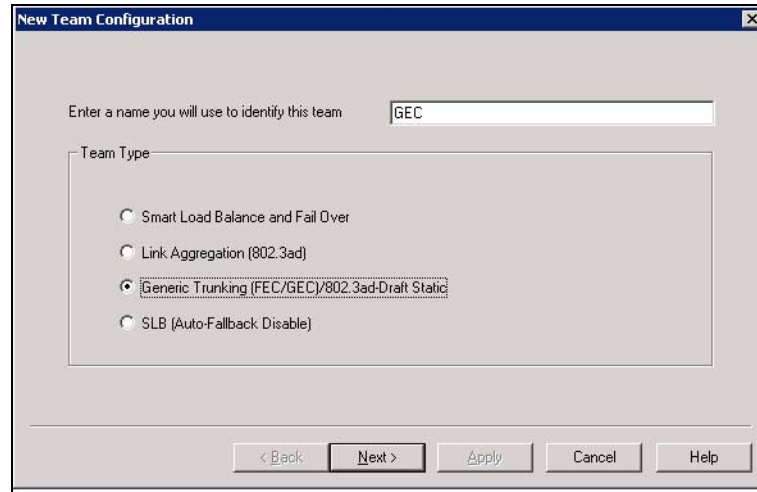


Figure 8.48 [Create Teams] dialog box

- 4 Select a load balance member from the list of available adapters and click the upper arrow button in the center of the screen.

Remarks: You cannot select a standby member.

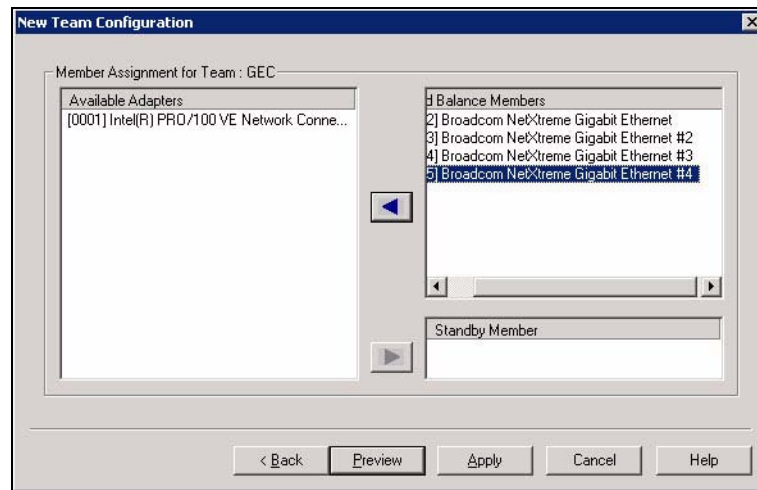


Figure 8.49 [Create Teams] dialog box

5 The following message dialog box appears. Click [Yes].

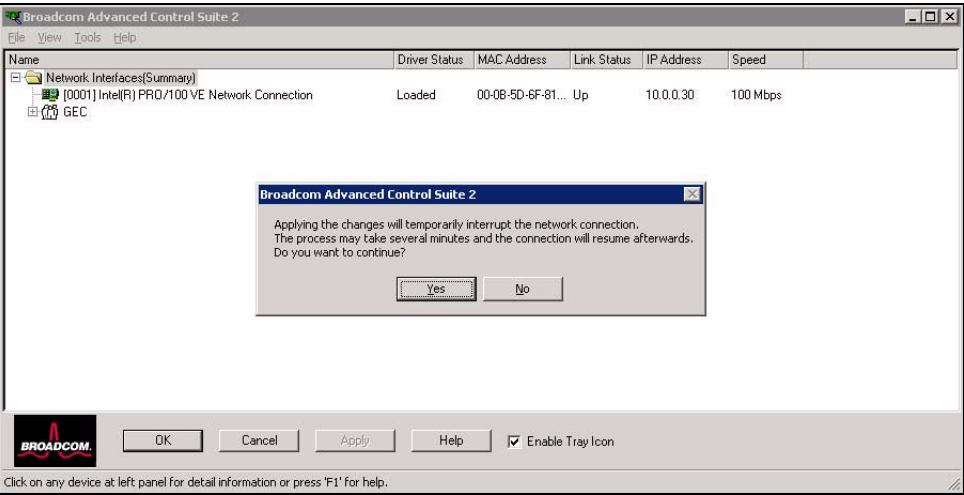


Figure 8.50 [Broadcom Advanced Control Suite 2] dialog box

6 When the team is created, a virtual adapter is also created on "Broadcom Advanced Control Suite 2."

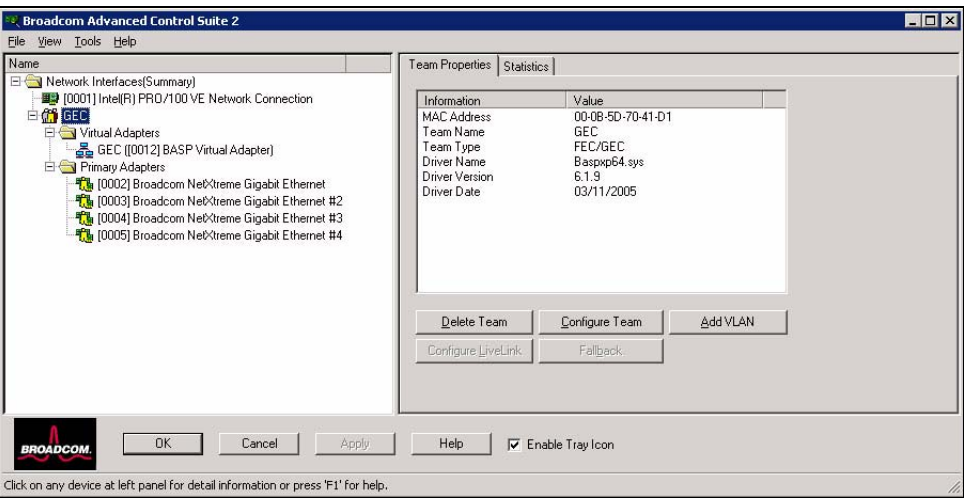


Figure 8.51 [Broadcom Advanced Control Suite 2] window

- 7 Set an IP address for the created virtual adapter on "Network connections" of Windows. (Device name "BAS Virtual Adapter" is assigned to the adapter.)

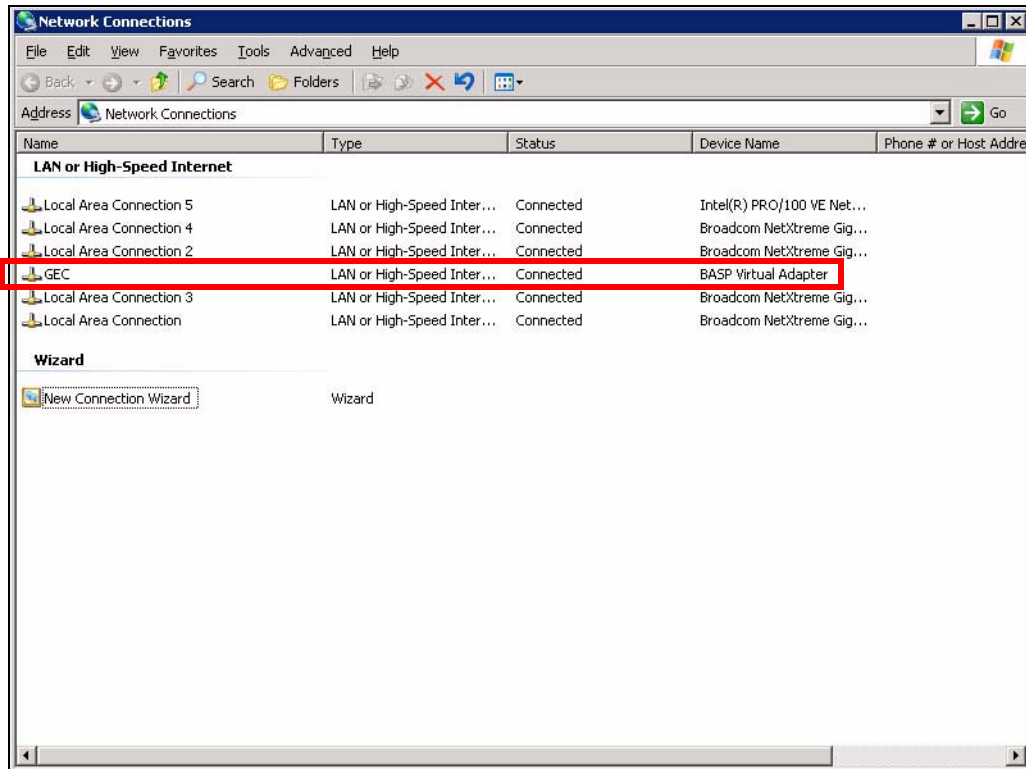


Figure 8.52 [Network connections] window

8.6 Link Aggregation (802.3ad) Setting Procedure

This section explains the procedure for setting Link Aggregation (802.3ad).

- 1 From the [Start] menu, choose "Broadcom Advanced Control Suite 2."

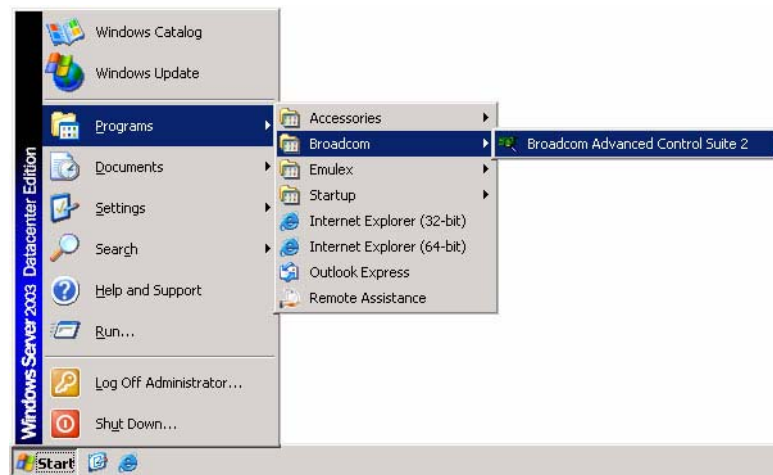


Figure 8.53 Starting Broadcom Advanced Control Suite 2

- 2 Select [Tools] → [Create Teams].

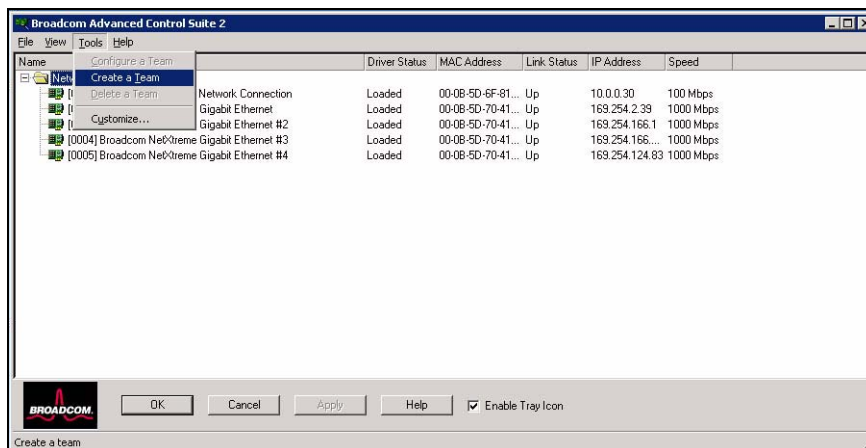


Figure 8.54 [Broadcom Advanced Control Suite 2] dialog box

- 3 Enter a team identification name, select "Link Aggregation (802.3ad)," and then click [Next].

Remarks: The team name is arbitrary.

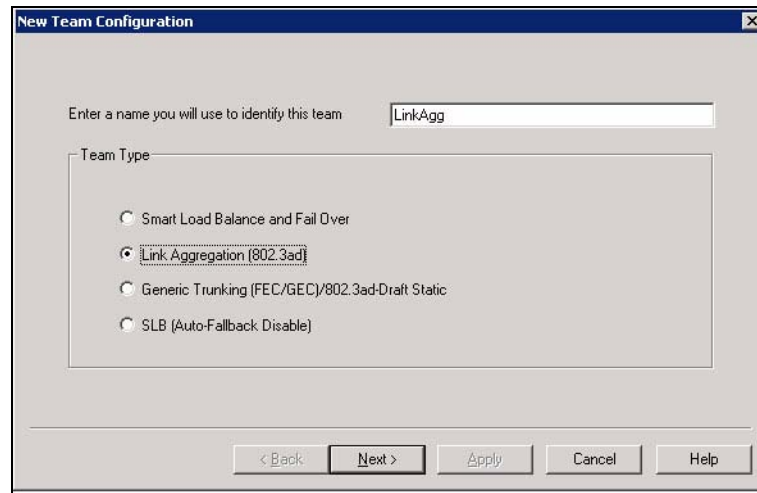


Figure 8.55 [Create Teams] dialog box

- 4 Select a load balance member from the list of available adapters and click the upper arrow button in the center of the screen.

Remarks: You cannot select a standby member.

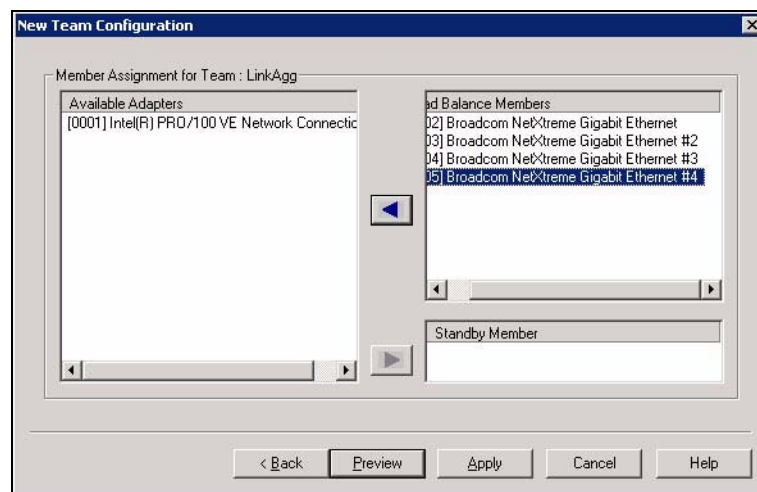


Figure 8.56 [Create Teams] dialog box

- 5 The following message dialog box appears. Click [Yes].

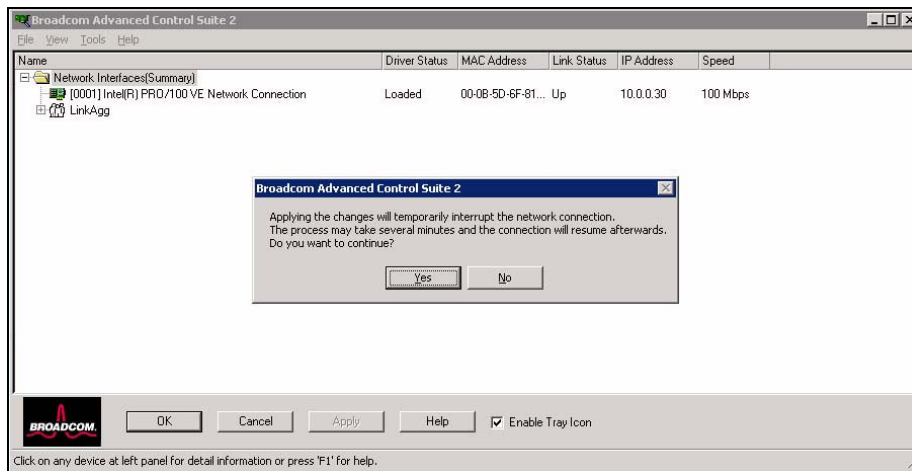


Figure 8.57 Message dialog box

- 6 When the team is created, a virtual adapter is also created on "Broadcom Advanced Control Suite 2."

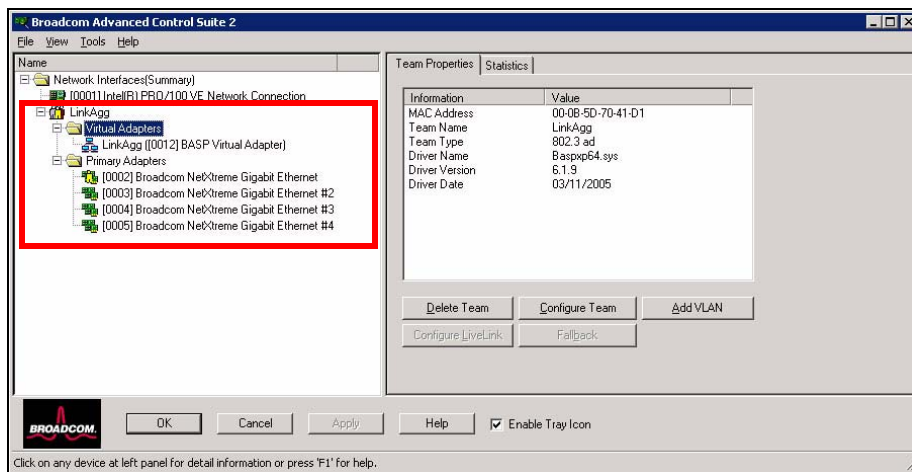


Figure 8.58 [Broadcom Advanced Control Suite 2] window (Display of virtual adapters)

- 7 Set an IP address for the created virtual adapter on "Network connections" of Windows. (Device name "BAS Virtual Adapter" is assigned to the adapter.)

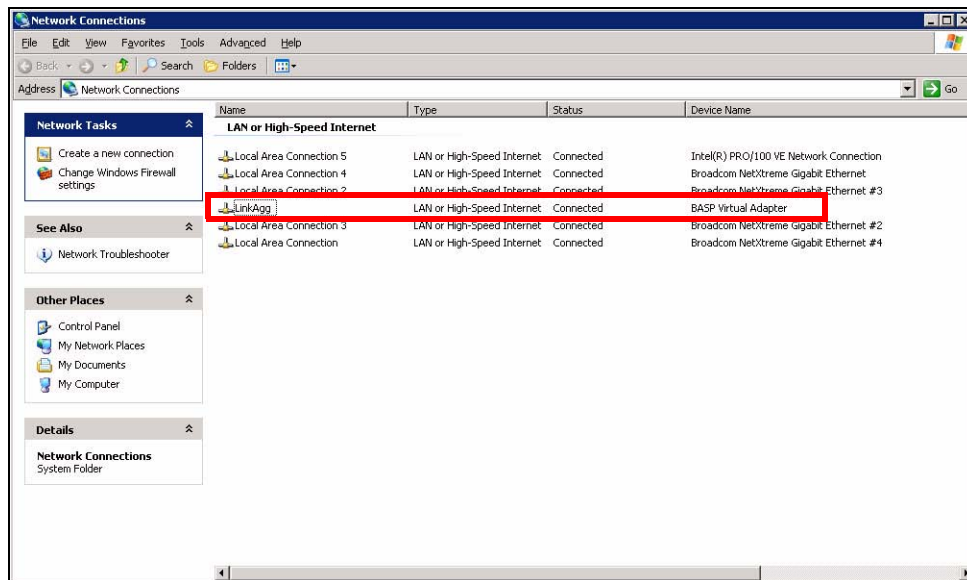


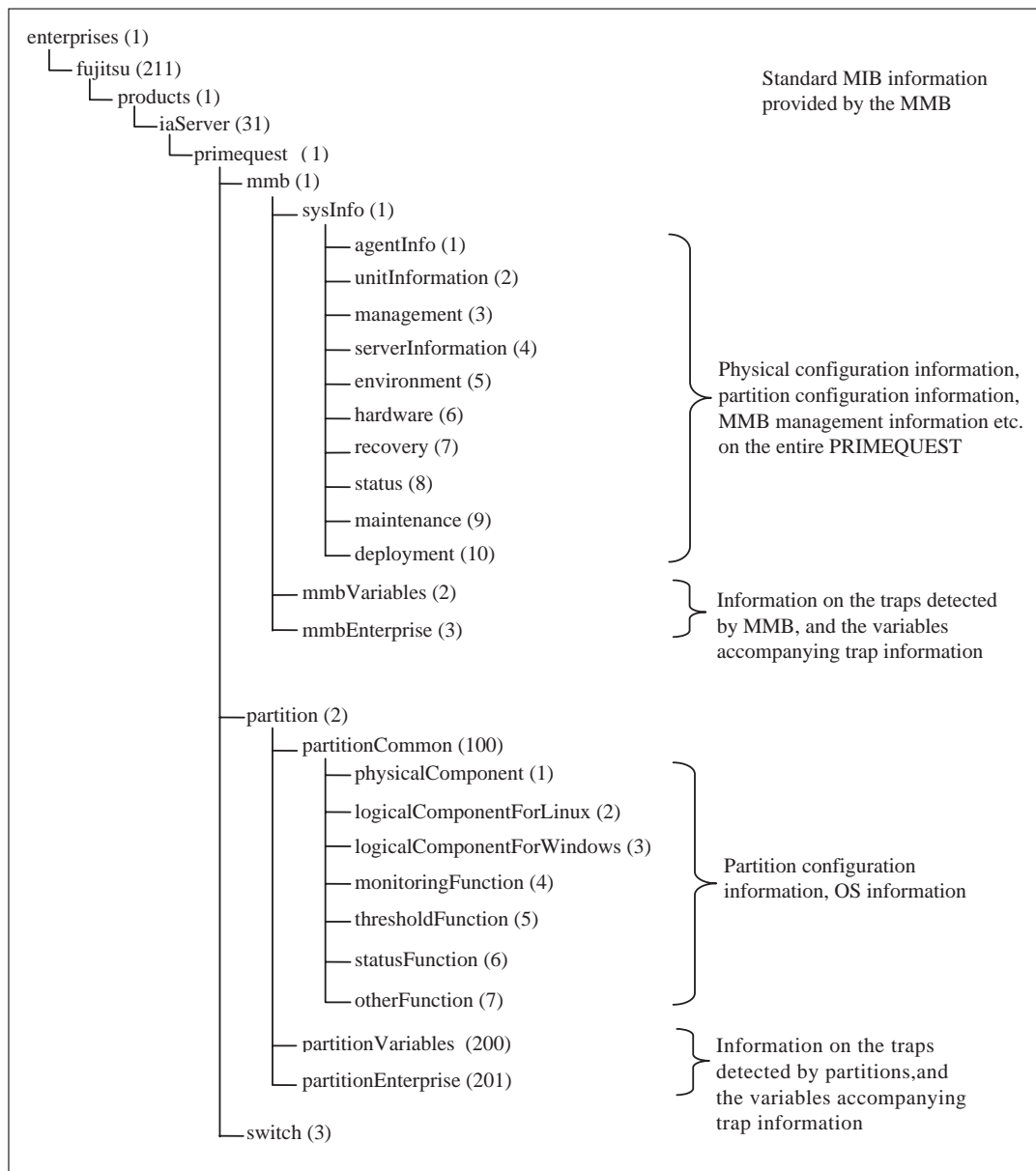
Figure 8.59 [Network connections] window

CHAPTER 9 MIB Tree Provided by PRIMEQUEST

The Management Information Base (MIB) tree provided in the PRIMEQUEST is shown below. The MIB information under "mmb(1)" is provided by the MMB agent and can be obtained from SNMPD on the Management Board (MMB). Standard MIB information can also be obtained from the MMB.

The MIB information under "partition(2)" is provided by PSA and can be obtained from MMB SNMPD via the proxy but can also be obtained directly from SNMPD on the partition.

That MIB information that is obtained via the proxy can be obtained for each partition by requesting an OID and replacing the partitionCommon(100) value with the partition ID.



- * iso(1),org(3), dod(6), internet(1), and private(4) are omitted before enterprises (1) in the above MIB tree.
- * Detailed MIB information defined at the above MIB tree branches is omitted.
- * In the above MIB tree, the MIB information provided by the MMB agent includes Logical System Board (LSB) information and Logical IO Unit (LIOU) information. Some versions of control manager software that uses SNMP obtain this information and display it as part of hardware configuration information. LSB and LIOU are the basic units of SB and IO Unit allocation to partitions.
- * For detailed information, see the MIB file (provided with the 'PRIMEQUEST Manuals' (C122-E013-C2)).

CHAPTER 10 Status Confirmation from LED

PRIMEQUEST has a function for indicating the power-on or off state of each component, whether an error exists, and the physical location of such an error by using LEDs. More detailed state information on each component can be confirmed by using the MMB Web-UI.

When the resident power supply unit is turned on to supply power to components, the Alarm LEDs for all the components go on. This is not indicative of a fault or error. When the components are verified as being normal, the Alarm LEDs go off.

Each component is equipped with the following LEDs:

- Power-LED (Green)
Indicates the power state within the component or indicates that hot swapping of the component is being performed. Also, when this LED is off, hot swapping (hot removal) of the component can be performed.
- Alarm-LED (Orange)
Indicates whether an error has occurred in a component.
- Location-LED (Blue)
Indicates the mounting location of the component. This LED includes a display function for assisting hot swapping work. This function can be set on or off by the user.

Remarks: For information on the physical location of each component, see [CHAPTER 2, "Physical Locations of Components."](#)

10.1 LED Display on the Operator Panel

PRIMEQUEST has an LED display function on the operator panel which displays the power status and whether an error has occurred.

Here, the operator panel of the PRIMEQUEST 580A/540A/580/540/480/440 is described as an example.

- The operator panel has a Power-LED (green) and Alarm-LED (orange), which indicate the power status of the cabinet and whether an error has occurred.
- The operator panel has a MMB-Ready-LED (green), from which the MMB status can be checked from the outside of the cabinet.
- The operator panel has a Location-LED (blue), from which the device to be operated can be identified.

Detailed information that cannot be represented by only the LEDs can be checked through the management LAN by using a terminal connected outside the cabinet.

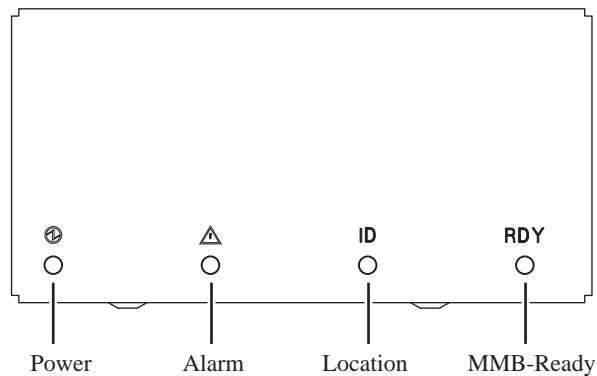


Figure 10.1 LEDs on the operator panel

10.2 LED Display of Each Board or Component

PRIMEQUEST has a function for indicating the power-on or off state of each board or component, whether an error exists, and the physical location of such an error by using LEDs. More detailed state information on each component can be confirmed by using the MMB Web-UI.

This section explains the following items:

- [LED display for each board or component](#) → (10.2.1)
- [List of LED displays for different boards and components](#) → (10.2.3)
- [LED display at power-on](#) → (10.2.4)
- [Display function of HDD LEDs](#) → (10.2.5)

10.2.1 LED display for each board or component

Each board or component has the following display functions:

Here, the indicators on the PRIMEQUEST 580A/540A/580/540/480/440 are described as an example.

- Each of the main boards has a Power-LED (green), which indicates the power status, and an Alarm-LED (orange), which indicates failure.
- When the Power-LED is turned off, the component can be deleted (regardless of the states of the other LEDs).
- Multiple components in the system that are of the same type have their own Location-LEDs (blue). The terminal operator can identify the physical location of a component by specifying its location-LED to blink or go on.
- Each of components that can be hot-inserted or hot-removed has a Location-LED (blue), which can be freely operated by the user. The user can also set the Location-LED to go on when a component can be hot-inserted or hot-removed. This facilitates the identification of components to be hot-inserted or hot-removed.

10.2.1.1 LED display of the MMB

Besides the Power-LED (green), Alarm-LED (orange), and Location-LED (blue), the MMB has a Ready-LED (green), which indicates that the MMB is being operated, and the Active-LED (green), which indicates that the MMB is the Active one of duplicated MMBs. Since the Ready-LED is synchronized with MMB-Ready on the operator panel, the MMB status can also be checked from the operator panel.

Also, the MMB has LEDs for a LAN. The Speed LED is placed to the left of the LAN connector and the Link/Act LED is placed to the right of it.

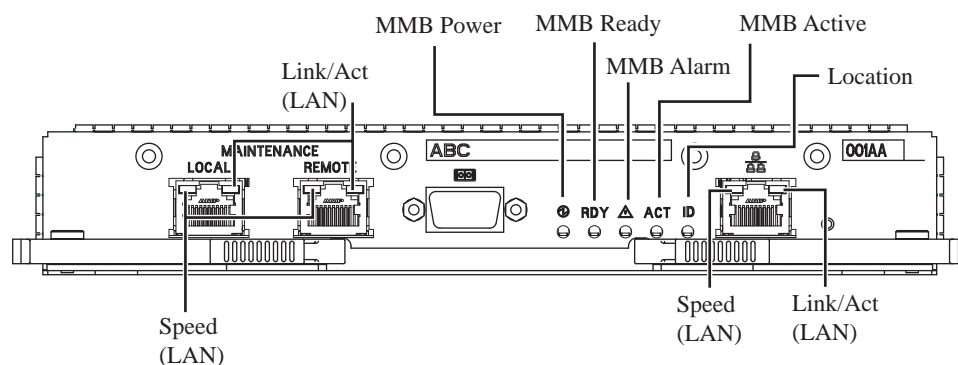


Figure 10.2 LEDs of the MMB

10.2.1.2 LED display of a GTHB

Besides the Power-LED (green), Alarm-LED (orange), and Location-LED (blue), a GTHB has LEDs for a LAN. The Speed LED is placed to the left of the LAN connector and the Link/Act LED is placed to the right of it.

Remarks: The GTHB can be mounted only in PRIMEQUEST 580A/540A/580/540 servers.

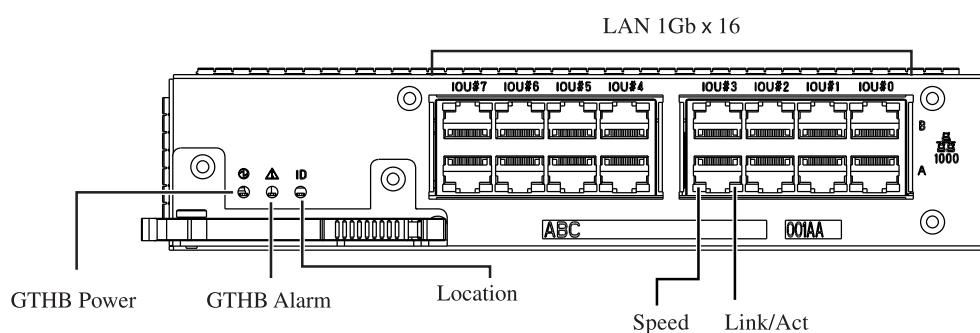


Figure 10.3 LED display of the GTHB

10.2.2 Other boards

Each of the boards other than the OPL, MMB, or GSWB has a Power-LED (green), Alarm-LED (orange), and Location-LED (blue). The following shows two examples in which LEDs are arranged vertically or horizontally:

The examples show the LED arrangements on the PRIMEQUEST 580A/540A/580/540/480/440.

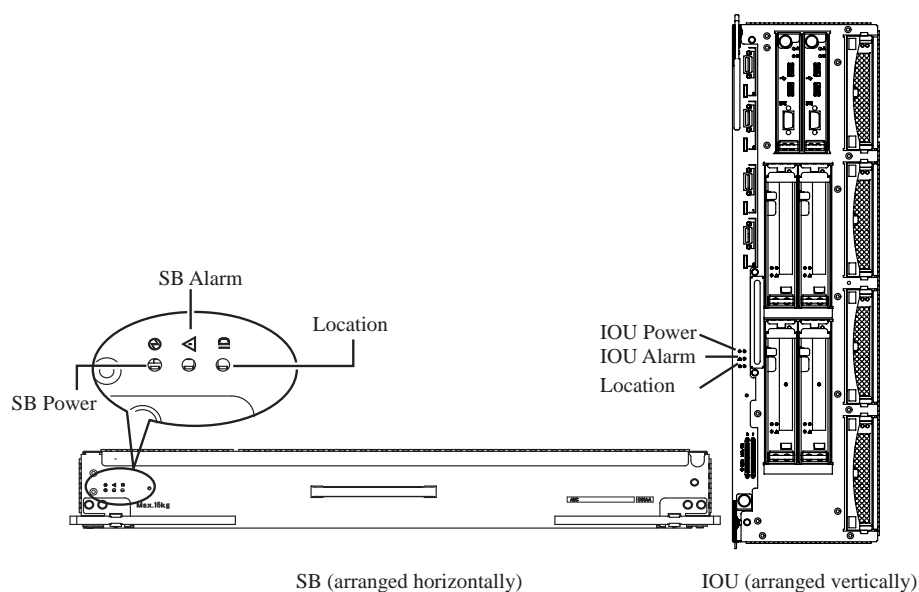


Figure 10.4 LEDs of other boards

10.2.3 List of LED displays for different boards and components

List of LED displays (PRIMEQUEST 580A/540A/580/540/480/440)

The following table shows LED states of different boards and their meaning:

Remarks: For details on LED display on the GSWB, refer to the *PRIMEQUEST GSWB User's Manual* (C122-E028EN).

Table 10.1 LED list (PRIMEQUEST 580A/540A/580/540/480/440)

Board, component	LED	Color	Number	State	Meaning
OPL (operator panel)	Power	green	1	On	Equipment power-ON (Op-panel 48V supplied)
	Alarm	orange	1	On	An error in the cabinet
	MMB Ready	green	1	On	MMB in the standby state (initialization complete)
				Blinking	MMB initialization in progress
	Location	blue	1	On/ blinking	Cabinet identification
SB (system board)	SB Power	green	1	On	48V supplied in the SB
				Blinking	Hot swapping being performed
	SB Alarm	orange	1	On	An error in the SB
	Location	blue	1	On/ blinking	A component identified
MMB (Management Board)	MMB Power	green	1	On	12V supplied to the MMB
	MMB Alarm	orange	1	On	An error in the MMB
	Location	blue	1	On/ blinking	A component identified
	MMB Active	green	1	On	Indicating the Active-MMB
	MMB Ready	green	1	On	MMB has been started.
				Blinking	MMB initialization in progress
	LAN 100BASE-TX Link/Act	green	1/LAN port	Off	Network disconnected
				On	Network connected
				Blinking	Data being transferred
	MMB LAN Speed	green	1/LAN port	Off	Operation being performed at 10 Mbps
				green On	Operation being performed at 100 Mbps

Board, component	LED	Color	Number	State	Meaning
IO Unit					
IOB	IOU Power	green	1	On	48V supplied into the IO Unit
				Blinking	Hot swapping being performed
	IOU Alarm	orange	1	On	An error in the IO Unit, BMM, or PERS
	Location	blue	1	On/ blinking	A component identified
BMM	Home BMM	green	1/BMM	On	BMM on which the home ICH mounted
	Location	blue	1	On/ blinking	A component identified
HDD	HDD Access	green	1/HDD	Blinking	In operation
	HDD Alarm	orange	1/HDD	On	An error in the HDD. Hot removal possible
PCI card cassette	Power	green	1/Cassette	On	Power-ON (PHP)
				Blinking	Hot swapping being performed
	Alarm	orange	1/cassette	On	An error in the PCI slot
				Blinking	A PCI slot identified
XAI	Power	green	1	On	48V supplied to the XAI
				Blinking	Hot swapping being performed
	Alarm	orange	1	On	An error in the XAI
	Location	blue	1	On/ blinking	A component identified
XDI	Power	green	1	On	48V supplied to the XDI
				Blinking	Hot swapping being performed
	Alarm	orange	1	On	An error in the XDI
	Location	blue	1	On/ blinking	A component identified
CPCB	Alarm	orange	1	On	An error in the CPCB
FAN TRAY	Alarm	orange	1/TRAY	On	An error in the FAN TRAY (FAN error)
PSU	Power Good	green	1/ PSU	On	Supplied power is sufficient
	Power Alarm	orange	1/ PSU	On	Supplied power is insufficient
	Predictive Alarm (FAN speed Alarm)	orange	1/ PSU	On	Fan rotation speed has decreased

Board, component	LED	Color	Number	State	Meaning
KVM	Power	green	1	On	48V supplied to the KVM
				Blinking	Hot swapping being performed
	Alarm	orange	1	On	An error in the KVM
	Location	blue	1	On/ blinking	A component identified
GTHB (only for the PRIMEQUEST 580A/540A/580/ 540)	GTHB Power	green	1	On	2.5 V supplied to the GTHB
				Blinking	Hot swapping being performed
	GTHB Alarm	orange	1	On	An error in the GTHB
	Location	blue	1	On/ blinking	A component identified
LAN 100BASE-T	GTHB LAN Link/ Act	green	1/LAN port	Off	Network disconnected
				On	Network connected
				Blinking	Data being transferred
	GTHB LAN Speed	green	1/LAN port	Off	Network disconnected
				On	Operation being performed at 1000 Mbps

Board, component	LED	Color	Number	State	Meaning
PCI_Box	Power	green	1	On	3.3V supplied to the PCI_Box
				Blinking	Hot swapping being performed
	Alarm	orange	1	On	An error in the PCI_Box
	Location	blue	1	On	A component identified
				Blinking	A component identified
	PCIU-Location	blue	4	On/ blinking	A component identified
PCIU	Power	green	1/Unit	On	3.3V supplied to the PCIU
				Blinking	Hot swapping being performed
	Alarm	orange	1/Unit	On	An error in the PCIU
PEXU	Power	green	1/Unit	On	3.3 V supplied to the PEXU
				Blinking	Hot swapping being performed
	Alarm	orange	1/Unit	On	An error in the PEXU
PCI card cassette	Power	green	1/cassette	On	Power-ON (PCI Hot Plug)
				Blinking	Hot swapping being performed
	Alarm	orange	1/cassette	On	An error in the PCI slot
				Blinking	A PCI slot identified
FAN TRAY	Alarm	orange	1/TRAY	On	An error in the FAN TRAY (FAN error)
FAN (individual)	Alarm	orange	1/FAN	On	FAN rotation speed has decreased
IO-PSU	Power Good	green	1/ IO-PSU	On	Supplied power is sufficient
	Power Alarm	orange	1/ IO-PSU	On	Supplied power is insufficient
	Predictive Alarm	orange	1/ IO-PSU	On	IO-PSU life expired

List of LED displays (PRIMEQUEST 520A/520/420)

The following table shows LED states of different boards and their meaning:

Table 10.2 LED list (PRIMEQUEST 520A/520/420)

Board, component	LED	Color	Number	State	Meaning
OPL (operator panel)	Power	green	1	On	Equipment power-ON (Op-panel 48V supplied)
	Alarm	orange	1	On	An error in the cabinet
	MMB Ready	green	1	On	MMB in the standby state (initialization complete)
				Blinking	MMB initialization in progress
	Location	blue	1	On/ blinking	Cabinet identification
SB (system board)	SB Power	green	1	On	48V supplied in the SB
				Blinking	Hot swapping being performed
	SB Alarm	orange	1	On	An error in the SB
	Location	blue	1	On/ blinking	A component identified
MMB (Management Board)	MMB Power	green	1	On	12V supplied to the MMB
	MMB Alarm	orange	1	On	An error in the MMB
	Location	blue	1	On/ blinking	A component identified
	MMB Active	green	1	On	Indicating the Active-MMB
	MMB Ready	green	1	On	MMB has been started.
				Blinking	MMB initialization in progress
	LAN 100BASE-TX Link/Act	green	1/LAN port	Off	Network disconnected
				On	Network connected
				Blinking	Data being transferred
	MMB LAN Speed	green	1/LAN port	Off	Operation being performed at 10 Mbps
				green On	Operation being performed at 100 Mbps

Board, component	LED	Color	Number	State	Meaning	
IO Unit	IOB	IOU Power	green	1	On	48V supplied into the IO Unit
					Blinking	Hot swapping being performed
		IOU Alarm	orange	1	On	An error in the IO Unit, BMM, or PERS
		Location	blue	1	On/ blinking	A component identified
	LAN 1000BASE-T	Link/Act	green	1/LAN port	green Blinking	Data being transferred
		Speed	green/ orange	1/LAN port	Off	Operation being performed at 10 Mbps
					orange On	Operation being performed at 100 Mbps
					green Blinking	Operation being performed at 1000 Mbps
	BMM	Home BMM	green	1/BMM	On	BMM on which the home ICH mounted
		Location	blue	1	On/ blinking	A component identified
	PCI card cassette	Power	green	1/Cassette	On	Power-ON (PCI Hot Plug)
					Blinking	Hot swapping being performed
		Alarm	orange	1/cassette	On	An error in the PCI slot
					Blinking	A PCI slot identified
	I O X	IOXB	Power	green	1	On
Off						Hot swapping being performed
Alarm			orange	1	On	An error in the IOX
					On/ blinking	A component identified
BMM		Home BMM	green	1	On	BMM on which the home ICH mounted
		Location	blue	1	On/ blinking	A component identified
HDD	HDD Access	green	1/HDD	Blinking	In operation	
				On	Power-ON	
	HDD Alarm	orange	1/HDD	On	An error in the HDD. Hot removal possible	
FAN TRAY	Alarm	orange	1/TRAY	On	An error in the FAN TRAY (FAN error)	

Board, component	LED	Color	Number	State	Meaning
PSU	Power Good	green	1/ PSU	On	Supplied power is sufficient
	Power Alarm	orange	1/ PSU	On	Supplied power is insufficient
	Predictive Alarm (FAN speed Alarm)	orange	1/ PSU	On	Fan rotation speed has decreased

Board, component	LED	Color	Number	State	Meaning
PCI_Box	Power	green	1	On	3.3V supplied to the PCI_Box
				Blinking	Hot swapping being performed
	Alarm	orange	1	On	An error in the PCI_Box
	Location	blue	1	On/ blinking	A component identified
	PCIU- Location	blue	4	On/ blinking	A component identified
PCIU	Power	green	1/Unit	On	3.3V supplied to the PCIU
				Blinking	Hot swapping being performed
	Alarm	orange	1/Unit	On	An error in the PCIU
PEXU	Power	green	1/Unit	On	3.3V supplied to the PEXU
				Blinking	Hot swapping being performed
	Alarm	orange	1/Unit	On	An error in the PEXU
PCI card cassette	Power	green	1/cassette	On	Power-ON (PCI Hot Plug)
				Blinking	Hot swapping being performed
	Alarm	orange	1/cassette	On	An error in the PCI slot
				Blinking	A PCI slot identified
FAN TRAY	Alarm	orange	1/TRAY	On	An error in the FAN TRAY (FAN error)
FAN (individual)	Alarm	orange	1/FAN	On	FAN rotation speed has decreased
IO-PSU	Power Good	green	1/ IO-PSU	On	Supplied power is sufficient
	Power Alarm	orange	1/ IO-PSU	On	Supplied power is insufficient
	Predictive Alarm	orange	1/ IO-PSU	On	IO-PSU life expired

10.2.4 LED display at power-on

The following table lists LED display during the period from power-on to the start of the MMB and LED display cases where a problem occurs at the start time:

Table 10.3 LED Display of the operator panel (cabinet) and MMB

State	Operator panel			MMB				
				Common to Active-MMB and Standby-MMB			Active -MMB	Standby -MMB
	Power (green)	MMB-Ready (green)	Alarm (orange)	Power (green)	Ready (green)	Alarm (orange)	Active (green)	Active (green)
All plugs disengaged	Off	Off	Off	Off	Off	Off	Off	Off
Power failure (*1)	Off	Off	Off	Off	Off	Off	Off	Off
Power supply started	Off	Off	On	On	Off	On	Off	Off
MMB being initialized	Off	Blinking	Off	On	Blinking	Off	Off	Off
Hangup during MMB initialization (*2)	Off	Undefined	Off	On	Undefined	On	Off	Off
Error detected during MMB initialization	Off	Blinking	On	On	Blinking	On	Off	Off
Standby state (MMB initialization completed normally)	Off	On	Off	On	On	Off	On	Off
Power-ON (48V supplied)	On	On	Off	On	On	Off	On	Off
Power-ON being performed (POST/PAL/SAL/EFI processing)	On	On	Off	On	On	Off	On	Off
Hangup or error detected in POST/PAL/SAL/EFI/	On	On	On	On	On	Off	On	Off
POST/PAL/SAL/EFI completed normally	On	On	Off	On	On	Off	On	Off
Environment/monitoring error	On	On	On	On	On	Off	On	Off
FATAL	On	On	On	On	On	Off	On	Off
OS hung	On	On	Off	On	On	Off	On	Off

*1 The MMB starts normally if at least one normal PSU is present.

*2 The MMB-Ready LED of the operator Panel is synchronized with the Ready LED of the Active-MMB.

10.2.5 Display function of HDD LEDs

The LED display of an HDD is as follows:

Table 10.4 LED display of an HDD
(PRIMEQUEST 580A/540A/580/540/480/440)

	Access(green)	Check(orange)
Power-OFF (not mounted)	Off	Off
Power-OFF (mounted)	Off	On
Power-ON (no disk access)	Off	Off
Power-ON (disk being accessed)	On	Off
Power-ON (error location identified)	Off	On

Table 10.5 LED display of an HDD (PRIMEQUEST 520A/520/420)

	Access (green)	Check (orange)
Power-OFF (not mounted)	Off	Off
Power-OFF (mounted)	Off	On
Power-ON (no disk access)	On	Off
Power-ON (disk being accessed)	On	Off
Power-ON (error location identified)	On	On

10.2.6 Link-Act-LED display function of network interface

This section explains Link-Act-LED display function of network interface.

Table 10.6 Link-Act-LED display of network interface

	Partition stopped		OS operating					
			Network interface operating		Network interface stopped			
			Linux/Windows		Linux		Windows	
	(1)LED	(2)LED	(1)LED	(2)LED	(1)LED	(2)LED	(1)LED	(2)LED
GSWB (GSWB-ON)	On	On	On	On	On	On	On	On
GTHB	Off	Off	On	On	On	On	Off (*)	Off (*)
LAN card (electrical)	Off	Off	On	On	Off	Off	Off	Off
LAN card (optical)	Off	Off	On	On	On (*)	On (*)	Off (*)	Off (*)

*: When the network is stopped (ifdown for Linux, or network disabled for Windows), the display may differ depending on the OS and device driver versions.

Remarks: The number in the parenthesis corresponds to the LEDs in the [Figure 10.5](#).

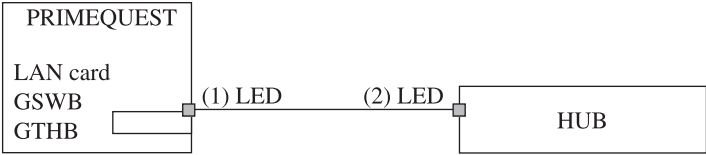


Figure 10.5 Example of network interface connection

Appendix A Alternative Key Combinations for Some Special Keys on Serial Terminals

On a serial terminal, you can use alternative key combinations for some special keys, as indicated in [Table A.1](#).

Table A.1 Special keys and their alternatives

Special key	Alternative key combination
HOME	ESC + h (press the [ESC] key and the [h] key in sequence)
END	ESC + k
INSERT	ESC + +
DELETE	ESC + -
PAGEUP	ESC + ?
PAGEDOWN	ESC + /
F1	ESC + 1
F2	ESC + 2
F3	ESC + 3
F4	ESC + 4
F5	ESC + 5
F6	ESC + 6
F7	ESC + 7
F8	ESC + 8
F9	ESC + 9
F10	ESC + 0

Glossary

ACS (AC Section)

AC power input section

ASIC (Application Specific Integrated Circuit)

Integrated circuit (IC) designed and manufactured for specific applications

API (Application Program Interface)

A set of instructions and functions used for developing operating systems and middleware

BIOS (Basic Input Output System)

Part of the operating system (OS) function. The BIOS is the system that controls input/output to devices. For the PRIMEQUEST-series machine, BIOS is a general term for PAL, SAL, and EFI.

BMC (Baseboard Management Controller)

The BMC is a system management controller that continuously monitors the system for serious hardware errors and notifies the OS of such errors.

BMM (BMC Module)

Board on which legacy I/O ports such as BMC, VGA, USB, and COM ports are mounted

BP (Backplane)

The backplane is connected to SBs, IO Units, and other devices. Together with the XAI and XDI, it constitutes the memory and I/O interconnect (crossbar).

Business LAN

LAN used to configure a user business system

CLI (Command Line Interface)

This interface with UNIX or DOS allows the user to enter commands and optional arguments to communicate with the OS.

CoA

Abbreviation for Certificate of Authenticity. This is a visual identifier that helps identify genuine Microsoft software and components.

COM Port (Communication Port)

RS-232C serial port for PC/AT compatible machines. A COM port is also called an "RS-232C port." Most PC/AT compatible machines each have two COM ports, which are often used to connect a modem, terminal adapter, or scanner. Most of these ports use D-Sub 25-pin or D-Sub 9-pin connectors.

CPCB (Clock and PCI_Box Control Board)

Board equipped with a system clock oscillator and a PCI_Box control interface

Crossbar

This concept covers the address crossbar and data crossbar that transfer data and control the data transfer between SBs and IO Units. Memory and I/O interconnect has the same meaning as crossbar.

DDR2 (Double Data Rate 2)

Standards for the next generation of memory that operates at higher speeds and consumes less power than conventional DDR memory

DIMM (Dual Inline Memory Module)

This compact memory module has pins on both sides and is mainly used in notebook PCs.

DP

Abbreviation for Dynamic Partitioning. This is a function for dynamically adding, deleting, or replacing CPU or memory resources as well as PCI cards and onboard I/O units in a partition while the operating system is running in the partition.

DVD-ROM (Digital Versatile Disc-Read-Only Memory)

Digital format for high-volume storage of data on optical disks

ECC (Error Checking Correction)

Error correction code or a method of using the error correction code to check for and correct errors

EFI (Extensible Firmware Interface)

Specifications for an interface between an OS and firmware. Instead of the BIOS, EFI is used for hardware control.

FC (Fibre Channel)

One of the serial interface standards. The Fibre Channel standard uses fiber cables as the transmission medium.

Firmware

Built-in software for basic hardware control

FWH (Firmware Hub)

LSI device from Intel Corporation. FWH is flash memory that stores SAL (BIOS). The PRIMEQUEST-series machine uses two types of FWH: one type is mounted on an SB and the other is mounted in an IO Unit.

GAC (Global Address Controller)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

GbE (Gigabit Ethernet)

Ethernet standards for high-speed communication of up to 1 Gbps

GDS

Abbreviation for PRIMECLUSTER GDS

GDX (Global Data Xbar)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

GLS

Abbreviation for PRIMECLUSTER GLS

GSWB (Gigabit Switch Board)

Board with a switching hub function and a connector that receives Gigabit Ethernet interface output from an IO Unit via the BP and outputs it to a destination outside the cabinet

HBA

Abbreviation for a host bus adapter

HDD (Hard Disk Drive)

Device that reads a hard disk. HDD may also be an abbreviation for the hard disk itself.

Hot Plug

Method of replacing components while power is on

HTTP (Hypertext Transfer Protocol)

Protocol used by Web servers and clients for data transmission

I2C (Inter Integrated Circuit)

Protocol used for high-speed communication between integrated circuits (ICs)

IA (Intel Architecture)

Generic term for the basic design (architecture) of Intel's microprocessors

IFT (Instruction Fetch)

Mechanism for reading instructions stored in memory

IHV (Independent Hardware Vendor)

This hardware provider has no special relationship with a particular hardware or OS maker.

IO Unit

I/O control unit that contains PCI card slot, HDD, SCSI controller, GbE controller, and other I/O interfaces

IP Address (Internet Protocol Address)

Identification number assigned to each computer connected to an IP network, such as the Internet and intranets

IPMI (Intelligent Platform Management Interface)

Standardized interface specifications established so that SNMP and server management software can monitor server hardware independently of specific hardware systems and OSs

ISV (Independent Software Vendor)

This application software provider has no special relationship with a particular hardware or OS maker.

KVM (KVM interface unit)

Unit used to select the USB interface for keyboard and mouse, or the VGA interface, for external output from a partition

LAN (Local Area Network)

Using optical fiber, for example, this network allows data to be transferred among computers and printers connected in a facility.

LDAP (Lightweight Directory Access Protocol)

Protocol used to access directory databases in a TCP/IP network, such as the Internet and intranets

LDX (Local Data Xbar)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

LED

Abbreviation for a light emitting diode

MAC address (Media Access Control Address)

Unique address assigned to each network interface device, switch, or router mounted on a network interface card (NIC) or motherboard

Management LAN

This LAN connects the MMB to partitions and to LANs outside the cabinet so that the PRIMEQUEST system can be managed.

MIB (Management Information Base)

Information released by a network device managed by SNMP in order to post the device status to an external destination

Middleware

Software that runs under an OS and provides application software with more advanced and detailed functions than the OS. It is positioned between the OS and application software in terms of its characteristics.

MMB (Management Board)

This server management board is a system control unit whose tasks include control and monitoring of cabinet hardware, partition management, and system initialization.

NIC (Network Interface Controller)

Hardware that supports network functions

NTP (Network Time Protocol)

Standard time information protocol used on the Internet. Highly precise time information with consideration of line speeds and load changes in paths can be obtained with this protocol.

PAL (Physical Abstract Layer)

Firmware that provides platform initialization and operating system boot functions

Partition

System equipped with the functions of a processing unit. Each partition contains software resources such as an OS and applications as well as hardware resources such as SBs and IO Units.

PCI_Box

Device used for PCI slot expansion

PCI Hot Plug

Technology that enables PCI cards to be mounted and removed while the system is operating

PCI (Peripheral Component Interconnect)

Bus architecture established by PCI SIG for connecting PC components

PCIU (PCI Unit)

PCI-X card slot expansion unit that is mounted in a PCI_Box

PEXU

PCI Express card slot expansion unit that is mounted in a PCI_Box

Platform

OS type or environment that is the basis for operation of application software

POST (Power-On Self Test)

Hardware test that is automatically run when the computer is powered on

Private LAN

LAN used for internal control, under which firmware programs installed on hardware components communicate with one another. MMB firmware, GSWB firmware, and BMC firmware installed on IO Units can use a private LAN for communication with one another. OSs and applications cannot use a private LAN.

PSA (PRIMEQUEST Server Agent)

Software that performs hardware error monitoring and configuration management over PRIMEQUEST partitions

PSU (Power Supply Unit)

Component that converts AC voltage to DC voltage as a DC power supply

PXE

PXE (Preboot eXecution Environment) Network boot standard based on BIOS technology that enables remote operation of management tasks such as system start and OS installation/update

RAID (Redundant Array of Independent Disks)

Technology that increases reliability and processing speeds by using multiple hard disks as a single disk

REMCS (Remote Customer Support System)

Fujitsu's remote customer support service

Reserved SB

Standby SB reserved for possible failures

RHEL (Red Hat Enterprise Linux)

Linux distribution released by Red Hat, Inc.

SAF-TE

Abbreviation for a SCSI accessed fault-tolerant enclosure

SAL (System Abstraction Layer)

Firmware that supports processor initialization and error recovery functions

SAN (Storage Area Network)

Dedicated network for connections between a server and storage devices

SAS

Abbreviation for Serial Attached SCSI. This is one of the interfaces included in the SCSI standards. Serial Attached SCSI is an interface for connecting devices such as hard disks to a computer. With this interface, data is transferred in serial communication.

SB (System Board)

Board on which a CPU and memory are mounted

SCSI (Small Computer System Interface)

Standards for connections between PCs and peripherals. SCSI was established by the American Standards Association.

SDRAM (Synchronous DRAM)

Memory standard for access speeds that are higher than those of DRAM

SEL (System Event Log)

Information on the processing parameters, processing, and processing results logged during hardware and software operations

SERDES (Serializer Deserializer)

Parallel-to-serial converter (from low speeds to high speeds)

SIRMS (Software Product Information Collection for Remote Maintenance Support)

Software that collects configuration information on software installed in PRIMEQUEST partitions

S.M.A.R.T. (Self-Monitoring Analysis Reporting Technology)

Function that enables a hard disk to monitor its own conditions and notify the BIOS of any error detected

SMP (Symmetric Multiple Processor)

Parallel processing system in which all processors work together through common memory resources

SNMP (Simple Network Management Protocol)

TCP/IP-compliant protocol for managing devices in a network

SSL (Secure Sockets Layer)

Protocol under which information is encrypted for transmission. SSL was developed by Netscape Communications Corp.

System Mirror Mode

Mechanism for duplicating memory, system interconnects, and internal hardware components of chipsets so that operation can continue with another component in the event that one of duplicated components fails.

Systemwalker

One of Fujitsu's middleware products. Systemwalker is integrated operation management software.

Telnet

Protocol or standard method for remote control of computers connected to a TCP/IP network, such as the Internet and intranets

UPS (Uninterruptible Power Supply)

Power supply unit that stores power and protects against possible damage and loss of computer data from a momentary voltage drop or unexpected power failure

USB (Universal Serial Bus)

One of the standards on connecting peripheral devices such as keyboards and mice

VLAN (Virtual LAN)

Function that logically groups the ports of one switching hub so each group works as an independent LAN

Web UI (Web User Interface)

Interface that uses a Web browser for displaying information to users and for user operations

XAI (Xbar Address Interconnect Board)

Board that transfers address information and controls the information transfer between SBs and IO Unit boards

XDI (Xbar Data Interconnect Board)

Board that transfers data and controls the data transfer between SBs and IO Unit boards

Index

A

adapter name, changing 6-16
Add a Port dialog box. 4-83, 4-84,
4-100, 4-101, 4-123, 4-144
Advanced tab 4-75
agreement item screen for information
transmission, message 7-51
alert message v
automatic-setting result screen,
message 7-47

B

backup 1-38
Linux 1-38
PRIMECLUSTER GDS being
used 1-46
PRIMECLUSTER GDS not
being used. 1-39
Windows 1-59
BACS setting 8-5
Broadcom Advanced Control
Suite 2 8-25, 8-29, 8-38, 8-42
Broadcom Advanced Control Suite 2 dialog
box 8-4, 8-25, 8-36, 8-40, 8-42
Broadcom Advanced Control Suite 2
window 8-27, 8-29, 8-31, 8-32,
8-35, 8-36, 8-38, 8-40, 8-44
Broadcom Advanced Control Suite
dialog box. 8-16
Broadcom Ethernet 8-1
Broadcom Ethernet configuration. 8-3
Broadcom LAN information 8-12, 8-22
Broadcom LiveLink setting 8-11, 8-21
bus number 5-7, 5-12

C

communication error message. 7-55
component 2-1
Computer Management
window 4-71, 4-110
confirmation message dialog
box 4-131, 4-152
confirmation message window 4-89
confirmation window 4-106

connection check result screen,
message 7-53
connection check screen,
message 7-52
connection-destination center change
screen, message 7-54
contents of manual i
CPCB 2-10
Create Teams dialog
box. 8-26, 8-30, 8-39, 8-43
customer information screen,
message 7-50, 7-51

D

Deleted previous version of PSA
window 4-105, 4-149
Detected previous version of PSA
window 4-88, 4-128
device file 1-49
Device Manager window 6-13, 6-14
DSNAP 1-26
dump environment 1-31

E

environment detail setting screen 7-42
environment detail setting screen,
message 7-54
environment setting (Internet - mail only)
screen, message 7-47
environment setting (P-P) screen,
message 7-48
environmental requirement for using
product. vi
Ethernet port, physical position 8-4, 8-16

F

FE operation initial screen 7-40
firewall 4-14, 4-31, 4-58, 4-83, 4-100,
4-122, 4-143
fjsnap 1-25
format partition 1-50

G

Generic Trunking (FEC/GEC)/802.3ad-Draft
Static 8-1

Generic Trunking (GEC/FEC)

- configuration 8-13, 8-23
- GLS hot plug support 3-23
- GSWB 2-5
- GTHB 2-6
- GTHB LED display 10-5
- GTHB location 2-6

H

- hard disk 1-3
- Hardware Added screen 6-18, 6-19
- hardware configuration information
 - transmission screen, message 7-53
- Hardware Removed screen 6-17, 6-18
- HBA (FA card) and ETERNUS,
 - swapping. 3-48
- HBA (FC card) and ETERNUS,
 - addition 3-46
- HBA (FC card) and ETERNUS,
 - removal 3-47
- HBA removal
 - (multi-path configuration) 3-52
- HBA swapping
 - (multi-path configuration) 3-54
- hot plug 3-1
- hot swapping 1-2

I

- information check list 1-30
- initial setting screen, message 7-46
- installation
 - PSA (Linux: Red Hat) 4-22
 - PSA (Linux: SUSE) 4-39
 - PSA
 - (Windows Server 2003) 4-67, 4-90
 - PSA
 - (Windows Server 2008) 4-107, 4-133
 - SIRMS 4-30
- installation completion
 - window 4-78, 4-138
- installation preparation window 4-77,
 - 4-86, 4-87, 4-94, 4-103, 4-104, 4-116,
 - 4-126, 4-128, 4-137, 4-147, 4-149
- installation window 4-94, 4-116, 4-137
- InstallShield Wizard Complete
 - window 4-117
- interface name, assigning 3-41
- IO Unit 2-7, 2-15
- IOU window 6-9

- IOU#x window 6-2
- IOU/IOX information window 6-5
- IOX 2-16

K

- kernel memory dump 1-32
- key combination A-1
- kudzu (8) window, optional item 3-24
- Kudzu start up 6-17
- kudzu, handling 3-40
- KVM interface unit 2-11

L

- LED 10-1
- Link Aggregation (802.3ad)
 - configuration 8-24
- Link-Act-LED display 10-16
- Linux
 - backup 1-38
 - setting device name 1-60
- Linux single-user mode, startup 6-19
- LiveLink dialog box 8-33, 8-34
- LiveLink setting dialog box 8-32, 8-33,
 - 8-34, 8-35
- Local Area Connection Properties
 - dialog box 6-12
- Local Area Network Connection Properties
 - dialog box 4-75, 4-114

M

- maintenance completion
 - window 4-89, 4-106
- maintenance data, collecting 1-25, 1-26
- maintenance dialog box 4-131, 4-152
- Maintenance PCI Card 1-1
- management LAN 4-3, 4-24, 4-40,
 - 4-69, 4-92, 4-109, 4-135
- management LAN duplication 4-47
- management LAN reconfiguration 6-1
- manual installation (Linux: Red Hat) 4-1
- memory dump 1-31
- memory dump setting 1-33
- memory dump setting, verifying 1-34
- Message dialog box 8-27, 8-31, 8-44
- MIB tree 9-1
- minimum memory dump 1-32
- MMB 2-4, 2-14
- MMB log downloading 7-57

N

network adapter list 4-72, 4-112
network configuration 8-1
network configuration, outline 8-1, 8-14
Network connections
 window 8-28, 8-37, 8-41, 8-45
network interface connection 10-16
network interface list 6-11
New Team Wizard window 4-72, 4-111

O

old setting, confirming 6-16
Onboard GbE 8-1
operator panel 10-2
OP-panel 2-2, 2-12
organization of manual i

P

paging file 1-31, 1-35
partition, rebooting 4-13, 4-30, 4-57
path addition by HBA addition 3-51
PCI slot 5-15
PCI slot bus number 5-7
periodic-connection scheduling screen,
 message 7-49
physical location 2-1, 2-12, 5-7, 5-15
Physical Location and Bus
 Number 5-1
physical mounting location 5-7, 5-12
PRIMEQUEST server agent update
 window 4-103
product handling vii
PSA
 manual installation
 (Linux: Red Hat) 4-22
 manual installation
 (Linux: SUSE) 4-39
 manual installation
 (Windows) 4-67, 4-90, 4-107, 4-133
 operation 4-3, 4-11, 4-24, 4-27,
 4-40, 4-56
 uninstallation 4-21, 4-38, 4-66,
 4-89, 4-106, 4-131, 4-152
 update installation 4-20, 4-37, 4-65,
 4-86, 4-103, 4-126, 4-147

R

reconfiguring partition 1-50
Red Hat 6-2
reference manual ii
registration result screen, message 7-51
REMCS center 7-1
REMCS function 1-23
REMCS GUI 7-58
REMCS initial screen 7-26
REMCS message 7-46
REMCS service 1-22, 7-1
rescue mode 1-48
restoration
 Linux 1-47
 PRIMECLUSTER GDS being
 used 1-58
 PRIMECLUSTER GDS not being
 used 1-47
 Windows 1-59
restore file system 1-51
restoring setting 6-16

S

SB 2-3, 2-13
secLevel setting 4-16, 4-33, 4-60
Select Features dialog box 4-129, 4-150
Select Features window 4-78, 4-95,
 4-115, 4-117, 4-136, 4-138
selection completed
 window 4-73, 4-113
SELinux 4-3, 4-12, 4-24, 4-29, 4-40, 4-57
serial terminal A-1
setting information backup screen,
 message 7-52
setting information restoration screen,
 message 7-46
setup completion window 4-95
setup window 4-77
SIRMS
 installation 4-30
 uninstallation 4-21, 4-38
 update installation 4-21, 4-38
SLB (Auto-Fallback Disable) 8-1
Smart Load Balance (SLB + LiveLink)
 configuration 8-9, 8-10, 8-20
Smart Load Balance (SLB)
 configuration 8-6, 8-7, 8-8, 8-17,
 8-18, 8-19

Smart Load Balance and Fail Over
 (+LiveLink) 8-1
Smart Load Balance LiveLink setting
 procedure 8-29
Smart Load Balance setting
 procedure 8-25
software configuration information
 transmission screen, message 7-53
special key A-1
stop/restart center connection screen,
 message 7-53
SUSE 9. 6-7
System Control Panel Applet
 dialog box 1-37

T

Team #x Properties dialog box 6-13
team mode list 4-73, 4-112
team number 0 properties
 window 4-74, 4-113
Team Settings dialog box 6-14
Teaming tab 4-71, 4-111
text convention iv
trap destination 4-13, 4-15, 4-30,
 4-32, 4-58, 4-59, 4-81, 4-98, 4-120, 4-141

U

uninstall complete
 dialog box 4-132, 4-153
uninstallation
 PSA 4-21, 4-38, 4-66, 4-89,
 4-106, 4-131, 4-152
 SIRMS 4-21, 4-38

update completion
 window 4-87, 4-104, 4-127, 4-148
update installation
 PSA 4-20, 4-37, 4-65, 4-86,
 4-103, 4-126, 4-147
 SIRMS 4-21, 4-38
update installation completion
 dialog box 4-130, 4-151
Update installation
 dialog box 4-129, 4-150
Update Installation window 4-147
update installation window 4-86, 4-126

W

Watchdog monitoring
 setting 4-85, 4-102, 4-124, 4-145
Welcome to Kudzu screen 6-17
Windows backup 1-59
Windows Firewall Settings
 dialog box 4-122, 4-143
Windows restoration 1-59
Windows Security dialog box 4-125,
 4-127, 4-130, 4-146, 4-151
Windows Server 2003 6-11

X

XAI 2-8
XDI 2-9

Y

YaST screen 6-8
YaST window 4-50

Reader's Comment Form

We would appreciate your comments and suggestions for improving this publication.

Date: _____
Your Name: _____
Company: _____
Address: _____
City/State/Zip: _____
Phone/Email address: _____

Publication No.: C122-E074-03EN
Publication Name: PRIMEQUEST
500A/500/400 Series
REFERENCE MANUAL:
TOOLS/OPERATION
INFORMATION

Your Comments:

Page	Line	Comments

Reply requested: ☐ Yes ☐ No

Please evaluate the overall quality of this manual by checking (✓)the appropriate boxes

	Good	Fair	Poor		Good	Fair	Poor		Good	Fair	Poor
Organization:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Use of examples:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Legibility:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Accuracy:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Index coverage:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Binding:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clarity:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cross				Figures and tables:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overall rating of				referencing:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	General appearance:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
this publication:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								
Technical level:	<input type="checkbox"/>	Too detailed		<input type="checkbox"/>	Appropriate		<input type="checkbox"/>	Not enough detail			

All comments and suggestions become the property of Fujitsu Limited.

For Users in U.S.A., Canada, and Mexico

Fold and fasten as shown on back
No postage necessary if mailed in U.S.A.

Fujitsu Computer Systems
Attention: Engineering Ops M/S 249
1250 East Arques Avenue
Sunnyvale, CA 94085-5401
FAX: (408) 746-6676

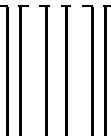
For Users in Other Countries

Fax this form to the number below or send this form to the address below.

Fujitsu Learning Media Limited
FAX: 81-3-3730-3702
37-10 Nishi-Kamata 7-chome
Oota-Ku
Tokyo 144-0051
JAPAN

FUJITSU LIMITED

FOLD AND TAPE

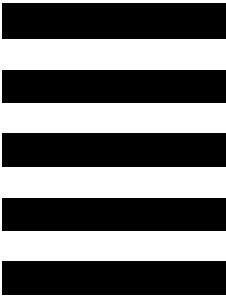


NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO 741 SUNNYVALE CA


POSTAGE WILL BE PAID BY ADDRESSEE



FUJITSU COMPUTER SYSTEMS
ATTENTION ENGINEERING OPS M/S 249
1250 EAST ARQUES AVENUE
SUNNYVALE CA 94085-5401



FOLD AND TAPE


FUJITSU