


FUJITSU Software

PRIMECLUSTER

Global Link Services

A decorative horizontal band with a red-to-dark-red gradient, featuring abstract, glowing white and red lines that swirl and intersect, creating a sense of motion and technology.

Configuration and Administration

Guide 4.5

Redundant Line Control Function

Oracle Solaris

J2S2-1676-02ENZ0(00)
February 2019

Preface

Purpose

This document describes the functions, installation, and operation procedure of Redundant Line Control Function that is a function of Global Link Services (hereinafter GLS).

Who should use this document

This document is intended for system administrators who are familiar with GLS operations and cluster control. Anyone who installs, configures, and maintains GLS to increase the availability of the system should read this documentation. A basic knowledge of PRIMECLUSTER is assumed.

Abstract

The document consists of the following chapters, appendices, and glossary:

[Chapter 1 Overview](#)

This chapter explains the redundant line control function of GLS.

[Chapter 2 Feature description](#)

This chapter outlines the functions and features of GLS.

[Chapter 3 Environment configuration](#)

This chapter discusses how to set up and configure GLS.

[Chapter 4 Operation](#)

This chapter explains how to operate the redundant line control function.

[Chapter 5 GLS operation on cluster systems](#)

This chapter explains how to operate the redundant line control on a cluster system.

[Chapter 6 Maintenance](#)

This chapter focuses on a general approach to troubleshooting. It presents a troubleshooting strategy and identifies commands that are available in Resource Coordinator for finding and correcting problems. Further, it discusses how to collect troubleshooting information.

[Chapter 7 Command reference](#)

This chapter outlines GLS commands.

[Appendix A Messages and corrective actions](#)

This appendix outlines messages and corrective actions to be taken to eliminate errors.

[Appendix B Examples of configuring system environments](#)

This appendix explains how to configure the system environment with the redundant line control function.

[Appendix C Operations in Solaris Zones Environment](#)

This appendix describes the operation of GLS on Solaris Zones.

[Appendix D Operation in Oracle VM Environments](#)

This appendix describes the operation of GLS in Oracle VM environments.

[Appendix E Cloning Environments](#)

This appendix describes how to build system by cloning the redundant line control function.

[Appendix F Changes from previous versions](#)

This appendix discusses changes to the GLS specification. It also suggests some operational guidelines.

[Appendix G Notice of supplemental information](#)

This appendix provides supplemental information regarding GLS.

Related Documentation

Please refer to the following manuals if necessary:

- PRIMECLUSTER Global Link Services Configuration and Administration Guide: Redundant Line Control Function for Virtual NIC Mode
- PRIMECLUSTER Concepts Guide
- PRIMECLUSTER Installation and Administration Guide
- FJQSS (Information Collection Tool) User's Guide
- Enhanced Support Facility User's Guide For Dynamic Reconfiguration
- Enhanced Support Facility User's Guide Dynamic Reconfiguration I/O device
- Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide
- Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual
- Fujitsu M10-1/SPARC M10-1 Service Manual
- Fujitsu M10-4/Fujitsu M10-4S/SPARC M10-4/SPARC M10-4S Service Manual
- Fujitsu SPARC M12-1 Service Manual
- Fujitsu SPARC M12-2/2S Service Manual
- PCI Expansion Unit for Fujitsu M10/SPARC M10 Systems Service Manual
- PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
- SPARC Enterprise M4000/M5000/M8000/M9000 Servers Dynamic Reconfiguration (DR) User's Guide
- SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide
- SPARC Enterprise M4000/M5000 Servers Service Manual
- SPARC Enterprise M8000/M9000 Servers Service Manual
- OSIV VTAM-G TISP Handbook
- Oracle VM Server for SPARC Guide

Notational conventions

Manual page section numbers

In manuals, helps, and messages of PRIMECLUSTER, a section number in a manual page is shown in parentheses after a command name or a file name. Example: cp(1)

For Oracle Solaris 11.4 or later, replace the section numbers as follows:

- "(1M)" to "(8)"
- "(4)" to "(5)"
- "(5)" to "(7)"
- "(7)" to "(4)"

Symbols

Material of particular interest is preceded by the following symbols in this manual:



.....
Text that requires special attention
.....

Note

Information that users should be cautious of

Information

Information that users can refer to

See

Manuals users find workable

Abbreviated name

- Oracle Solaris might be described as Solaris or Solaris Operating System.
- Oracle Solaris 10 is abbreviated as Solaris 10.
- Oracle Solaris 11 is abbreviated as Solaris 11.
- Oracle VM Server for SPARC is abbreviated as Oracle VM.
- Oracle Solaris Zones are abbreviated as Solaris Zones.

Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Trademark

- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Oracle is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
- Ethernet is a trademark of Fuji Xerox Corporation.
- Other product names that appear in this manual are product names, trademarks, or registered trademarks of respective companies.
- Fujitsu SPARC M12 is sold as SPARC M12 by Fujitsu in Japan. Fujitsu SPARC M12 and SPARC M12 are identical products.
- Fujitsu M10 is sold as SPARC M10 by Fujitsu in Japan. Fujitsu M10 and SPARC M10 are identical products.

Date of publication and edition

| |
|--|
| April 2017, First edition February 2019, Second edition |
|--|

High Risk Activity

This Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. You shall not use this Product without securing the sufficient safety required for the High Safety Required Use. If you wish to use this Product for High Safety Required Use, please consult with our sales representatives before such use.

Requests

- No part of this document may be reproduced or copied without permission of FUJITSU LIMITED.
- The contents of this document may be revised without prior notice.

All Rights Reserved, Copyright (C) FUJITSU LIMITED 2017-2019.

Contents

| | |
|---|----|
| Chapter 1 Overview..... | 1 |
| 1.1 What is redundant line control?..... | 1 |
| 1.1.1 Functional comparison..... | 4 |
| 1.1.2 Criteria for selecting redundant line control methods..... | 7 |
| 1.2 Redundant line control effects..... | 7 |
| 1.3 System Configuration..... | 8 |
| Chapter 2 Feature description..... | 12 |
| 2.1 Overview of Functions..... | 12 |
| 2.1.1 Fast switching mode..... | 12 |
| 2.1.1.1 Fault monitoring function..... | 13 |
| 2.1.1.2 Switching function..... | 14 |
| 2.1.1.3 Connectable remote host..... | 15 |
| 2.1.1.4 Available application..... | 15 |
| 2.1.1.5 Notes..... | 16 |
| 2.1.2 NIC switching mode..... | 16 |
| 2.1.2.1 Fault monitoring function..... | 17 |
| 2.1.2.2 Switching function..... | 19 |
| 2.1.2.3 Connectable remote host..... | 20 |
| 2.1.2.4 Available application..... | 20 |
| 2.1.2.5 Notes..... | 21 |
| 2.1.3 GS/SURE linkage mode..... | 21 |
| 2.1.3.1 Fault monitoring function..... | 24 |
| 2.1.3.2 Switching function..... | 25 |
| 2.1.3.3 Connectable remote host..... | 25 |
| 2.1.3.4 Available applications..... | 25 |
| 2.1.3.5 Notes..... | 25 |
| 2.2 Option Functions..... | 26 |
| 2.2.1 Configuring multiple virtual interfaces..... | 26 |
| 2.2.2 Cluster fail-over when entire transfer routes fails..... | 27 |
| 2.2.3 Sharing physical interface..... | 28 |
| 2.2.3.1 Using Fast switching mode..... | 28 |
| 2.2.3.2 Using NIC switching mode..... | 29 |
| 2.2.3.3 Using GS/SURE linkage mode..... | 29 |
| 2.2.3.4 Notices..... | 30 |
| 2.2.4 Configuring multiple logical virtual interfaces..... | 30 |
| 2.2.5 Configuring single physical interface..... | 30 |
| 2.2.6 HUB monitoring function..... | 31 |
| 2.2.6.1 Not using HUB-to-HUB monitoring feature..... | 32 |
| 2.2.6.2 Using HUB-to-HUB monitoring feature..... | 33 |
| 2.2.6.3 Multiple HUB monitoring of single physical interface..... | 35 |
| 2.2.6.4 Transfer path monitoring on individual virtual interface..... | 36 |
| 2.2.7 Monitoring communicating host..... | 39 |
| 2.2.8 Standby patrol function..... | 40 |
| 2.2.9 Automatic fail-back function..... | 41 |
| 2.2.10 Dynamically adding/deleting/switching physical interface..... | 44 |
| 2.2.11 User command execution function..... | 45 |
| 2.3 Other functions..... | 51 |
| 2.3.1 Message output when a line failure occurs..... | 51 |
| 2.3.2 DR (Dynamic Reconfiguration) function..... | 51 |
| 2.3.2.1 DR (Dynamic Reconfiguration) linkage function..... | 52 |
| 2.3.2.2 DR function of XSCF..... | 54 |
| 2.3.3 PCI Hot Plug (PHP) linkage..... | 56 |
| 2.3.4 Interface status monitoring feature..... | 56 |
| 2.3.5 Multiplexing transfer route with Tagged VLAN interfaces..... | 56 |

| | |
|---|-----|
| 2.3.5.1 Redundant Line Control function using Tagged VLAN interface..... | 57 |
| 2.3.6 Self-checking function..... | 60 |
| 2.4 Notes..... | 62 |
| 2.4.1 General..... | 62 |
| 2.4.2 Duplicated operation by Fast switching mode..... | 64 |
| 2.4.3 Duplicated operation via NIC switching mode..... | 64 |
| 2.4.4 Duplicated operation via GS/SURE linkage mode..... | 64 |
| Chapter 3 Environment configuration..... | 66 |
| 3.1 Setup..... | 66 |
| 3.1.1 Selecting mode..... | 66 |
| 3.1.2 Selecting appropriate contents..... | 67 |
| 3.1.2.1 Fast switching mode..... | 67 |
| 3.1.2.2 NIC switching mode..... | 68 |
| 3.1.2.3 GS/SURE linkage mode..... | 70 |
| 3.1.2.4 Configuration of individual mode..... | 72 |
| 3.1.2.5 Upper limit of configuration..... | 74 |
| 3.2 System Setup..... | 75 |
| 3.2.1 Checking system resources..... | 75 |
| 3.2.2 Network configuration..... | 75 |
| 3.2.2.1 Setup common to modes..... | 75 |
| 3.2.2.2 System setup in Fast switching mode..... | 79 |
| 3.2.2.3 System setup in NIC switching mode..... | 79 |
| 3.2.2.4 System setup in GS/SURE linkage mode..... | 80 |
| 3.2.3 syslog setup..... | 81 |
| 3.3 Additional system setup..... | 82 |
| 3.3.1 Fast switching mode..... | 82 |
| 3.3.2 NIC switching mode..... | 83 |
| 3.3.3 GS/SURE linkage mode..... | 84 |
| 3.3.4 Setting parameter for individual mode..... | 84 |
| 3.4 Changing system setup..... | 84 |
| 3.4.1 Fast switching mode..... | 85 |
| 3.4.2 NIC switching mode..... | 86 |
| 3.4.3 GS/SURE linkage mode..... | 87 |
| 3.4.4 Note on changing configuration information..... | 88 |
| 3.5 Deleting configuration information..... | 88 |
| 3.5.1 Fast switching mode..... | 88 |
| 3.5.2 NIC switching mode..... | 89 |
| 3.5.3 GS/SURE linkage mode..... | 90 |
| 3.5.4 Note on deleting configuration information..... | 91 |
| 3.6 Setting Option Function..... | 91 |
| 3.6.1 Configuring multiple virtual interfaces..... | 91 |
| 3.6.2 Switching cluster when all the transfer paths fails..... | 91 |
| 3.6.3 Sharing physical interface..... | 91 |
| 3.6.4 Multiple logical virtual interface definition..... | 91 |
| 3.6.5 Single physical interface definition..... | 91 |
| 3.6.6 HUB monitoring function..... | 91 |
| 3.6.6.1 Creating monitoring information..... | 92 |
| 3.6.6.2 Enabling HUB monitoring function..... | 92 |
| 3.6.6.3 Transfer route error detection time for NIC switching mode..... | 94 |
| 3.6.7 Monitoring the remote host..... | 99 |
| 3.6.7.1 Transfer route error detection time in GS/SURE linkage mode..... | 99 |
| 3.6.7.2 Transfer route recovery detection time in GS/SURE linkage mode..... | 101 |
| 3.6.8 Standby patrol function..... | 102 |
| 3.6.8.1 Setting what to be monitored..... | 102 |
| 3.6.8.2 Setting monitoring interval..... | 102 |
| 3.6.8.3 Setting error monitoring interval..... | 102 |

| | |
|---|------------|
| 3.6.9 Setting dynamic addition/deletion/switching function of physical interfaces..... | 103 |
| 3.6.9.1 Dynamic addition of physical interfaces..... | 103 |
| 3.6.9.2 Dynamic deletion of physical interfaces..... | 103 |
| 3.6.9.3 Dynamic switching of physical interfaces..... | 103 |
| 3.6.10 Setting User command execution function..... | 103 |
| 3.6.10.1 Settings for NIC switching mode..... | 104 |
| 3.6.10.2 Settings for GS/SURE linkage mode..... | 112 |
| 3.6.10.3 Settings of the service for Redundant Line Control function..... | 112 |
| 3.7 Configuring other functions..... | 115 |
| 3.7.1 Outputting message when transfer paths fails..... | 115 |
| 3.7.2 Setting Dynamic Reconfiguration (DR)..... | 115 |
| 3.7.2.1 Configure environment..... | 115 |
| 3.7.2.2 When using DR linkage function of ESF..... | 115 |
| 3.7.3 Transfer route multiplexing with Tagged VLAN interface..... | 116 |
| 3.7.3.1 Operating VLAN interface on Fast switching mode..... | 116 |
| 3.7.3.2 Operating VLAN interface on NIC switching mode..... | 117 |
| Chapter 4 Operation..... | 120 |
| 4.1 Starting and Stopping Redundant Line Control function..... | 120 |
| 4.1.1 Starting Redundant Line Control function..... | 120 |
| 4.1.2 Stopping Redundant Line Control function..... | 120 |
| 4.2 Activating and Inactivating Virtual Interfaces..... | 120 |
| 4.2.1 Activating virtual interfaces..... | 121 |
| 4.2.2 Inactivating virtual interfaces..... | 121 |
| 4.3 Displaying Operation Status..... | 121 |
| 4.4 Displaying Monitoring Status..... | 121 |
| 4.5 Dynamic operation (Replacement / Expansion)..... | 121 |
| 4.5.1 Executing DR command of ESF..... | 122 |
| 4.5.2 Replacing the system board using the DR of XSCF..... | 122 |
| 4.5.2.1 Replacing the system board using the DR of XSCF (SPARC M12-2S/ M10-4S)..... | 122 |
| 4.5.2.2 Replacing the system board using the DR of XSCF (SPARC Enterprise M4000/M5000/M8000/M9000)..... | 127 |
| 4.5.3 Replacement/Expansion PHP (PCI Hot Plug)..... | 132 |
| 4.5.3.1 Replacement of PCI card on redundant system..... | 132 |
| 4.5.3.2 Extension of PCI cards with new redundant system..... | 137 |
| 4.5.3.3 Extension of PCI cards to redundant system..... | 139 |
| 4.6 Recovery Procedure from Line Failure..... | 142 |
| 4.6.1 Recovery procedure from line failure in Fast switching mode..... | 142 |
| 4.6.2 Recovery procedure from line failure in NIC switching mode..... | 142 |
| 4.6.3 Recovery procedure from line failure in GS/SURE linkage mode..... | 143 |
| 4.6.4 How to recover when an error occurred in a transfer route at the execution of DR..... | 143 |
| 4.6.5 How to recover when an error occurred in a transfer route at the execution of PHP..... | 143 |
| 4.7 Backing up and Restoring Configuration Files..... | 143 |
| 4.7.1 Backing up Configuration Files..... | 144 |
| 4.7.2 Restoring Configuration Files..... | 144 |
| Chapter 5 GLS operation on cluster systems..... | 145 |
| 5.1 Outline of Cluster System Support..... | 145 |
| 5.1.1 Active Standby..... | 147 |
| 5.1.1.1 Starting..... | 147 |
| 5.1.1.1.1 Fast switching mode..... | 147 |
| 5.1.1.1.2 NIC switching mode..... | 147 |
| 5.1.1.1.3 GS/SURE linkage mode..... | 150 |
| 5.1.1.2 Switching..... | 151 |
| 5.1.1.2.1 Fast switching mode..... | 151 |
| 5.1.1.2.2 NIC switching mode..... | 152 |
| 5.1.1.2.3 GS/SURE linkage mode..... | 156 |
| 5.1.1.3 Fail-back..... | 157 |
| 5.1.1.4 Stopping..... | 158 |

| | |
|---|------------|
| 5.1.1.4.1 Fast switching mode..... | 158 |
| 5.1.1.4.2 NIC switching mode..... | 158 |
| 5.1.1.4.3 GS/SURE linkage mode..... | 161 |
| 5.1.2 Mutual standby..... | 162 |
| 5.1.2.1 Starting..... | 162 |
| 5.1.2.2 Switching..... | 162 |
| 5.1.2.2.1 Fast switching mode..... | 162 |
| 5.1.2.2.2 NIC switching mode..... | 163 |
| 5.1.2.3 Fail-back..... | 164 |
| 5.1.2.4 Stopping..... | 164 |
| 5.1.3 Cascade..... | 164 |
| 5.1.3.1 Startup..... | 164 |
| 5.1.3.1.1 Fast switching mode..... | 164 |
| 5.1.3.1.2 NIC switching mode..... | 165 |
| 5.1.3.2 Switching..... | 168 |
| 5.1.3.2.1 Fast switching mode..... | 168 |
| 5.1.3.2.2 NIC switching mode..... | 169 |
| 5.1.3.3 Fail-back..... | 173 |
| 5.1.3.4 Stopping..... | 173 |
| 5.1.3.4.1 Fast switching mode..... | 173 |
| 5.1.3.4.2 NIC switching mode..... | 174 |
| 5.1.4 Monitoring resource status of standby node..... | 177 |
| 5.1.4.1 Preface..... | 177 |
| 5.1.4.2 Configuration..... | 177 |
| 5.1.4.3 Recovering from a resource failure in Standby node..... | 178 |
| 5.1.5 Tagged VLAN interface multiplexing on NIC switching mode (Standby)..... | 178 |
| 5.1.5.1 Standby..... | 178 |
| 5.1.5.1.1 Fast switching mode..... | 178 |
| 5.1.5.1.2 NIC switching mode..... | 178 |
| 5.1.5.2 Mutual Standby..... | 179 |
| 5.1.5.2.1 Fast switching mode..... | 179 |
| 5.1.5.2.2 NIC switching mode..... | 179 |
| 5.1.5.3 Cascade..... | 180 |
| 5.1.5.3.1 Fast switching mode..... | 180 |
| 5.1.5.3.2 NIC switching mode..... | 180 |
| 5.2 Adding configuration for Cluster System..... | 181 |
| 5.2.1 Creating configuration information..... | 182 |
| 5.2.2 Creating Takeover virtual interface..... | 183 |
| 5.2.3 Configuring cluster system..... | 183 |
| 5.2.4 Starting a userApplication..... | 183 |
| 5.3 Modifying configuration for Cluster System..... | 183 |
| 5.4 Deleting configuration for Cluster System..... | 183 |
| 5.4.1 Deleting configuration for a cluster environment..... | 184 |
| 5.4.2 Deleting Takeover virtual interface..... | 184 |
| 5.4.3 Deletion of a Configuration information..... | 184 |
| 5.5 Backup/Restore Cluster configuration settings..... | 185 |
| Chapter 6 Maintenance..... | 186 |
| 6.1 Redundant Line Control function Troubleshooting Data to be Collected..... | 186 |
| 6.1.1 Command to collect materials..... | 187 |
| 6.1.2 Collecting Information by FJQSS (Information Collection Tool)..... | 190 |
| 6.1.3 Collecting debug information/Output command..... | 191 |
| 6.2 Packet Trace..... | 192 |
| 6.2.1 Collecting packet traces..... | 192 |
| Chapter 7 Command reference..... | 194 |
| 7.1 hanetconfig Command..... | 194 |
| 7.2 strhanet Command..... | 205 |

| | |
|--|------------|
| 7.3 stphanet Command..... | 207 |
| 7.4 dsphanet Command..... | 208 |
| 7.5 hanetobserv Command..... | 212 |
| 7.6 hanetparam Command..... | 220 |
| 7.7 hanetpoll Command..... | 224 |
| 7.8 dsppoll Command..... | 232 |
| 7.9 hanetnic Command..... | 236 |
| 7.10 strptl Command..... | 238 |
| 7.11 stppl Command..... | 239 |
| 7.12 hanetbackup Command..... | 239 |
| 7.13 hanetrestore Command..... | 240 |
| 7.14 hanethvrsc Command..... | 241 |
| 7.15 resethanet Command..... | 243 |
| 7.16 hanetgw Command..... | 245 |
| Appendix A Messages and corrective actions..... | 247 |
| A.1 Messages Displayed by Redundant Line Control function..... | 247 |
| A.1.1 Information message (number 0)..... | 248 |
| A.1.2 Error output message (numbers 100 to 500)..... | 248 |
| A.1.3 Console output messages (numbers 800 to 900)..... | 272 |
| A.1.4 Internal information output messages (no message number)..... | 284 |
| A.1.5 DR connection script error output messages..... | 284 |
| A.2 Messages Displayed in the Cluster System Logs..... | 286 |
| Appendix B Examples of configuring system environments..... | 287 |
| B.1 Example of configuring Fast Switching mode (IPv4)..... | 287 |
| B.1.1 Example of the Single system..... | 287 |
| B.1.2 Example of the Single system in Logical virtual interface..... | 289 |
| B.1.3 Configuring virtual interfaces with tagged VLAN..... | 292 |
| B.1.4 Example of the Cluster system (1:1 Standby)..... | 296 |
| B.1.5 Example of the Cluster system (Mutual Standby)..... | 298 |
| B.1.6 Example of the Cluster system (N:1 Standby)..... | 301 |
| B.1.7 Example of the Cluster system (Cascade)..... | 305 |
| B.2 Example of configuring Fast Switching mode (IPv6)..... | 309 |
| B.2.1 Example of the Single system..... | 309 |
| B.2.2 Example of the Single system in Logical virtual interface..... | 311 |
| B.2.3 Configuring virtual interfaces with tagged VLAN..... | 314 |
| B.2.4 Example of the Cluster system (1:1 Standby)..... | 317 |
| B.2.5 Example of the Cluster system (Mutual standby)..... | 320 |
| B.2.6 Example of the Cluster system (N:1 Standby)..... | 323 |
| B.2.7 Example of the Cluster system (Cascade)..... | 327 |
| B.3 Example of configuring Fast Switching mode (IPv4/IPv6)..... | 330 |
| B.3.1 Example of the Single system..... | 330 |
| B.3.2 Example of the Single system in Logical virtual interface..... | 334 |
| B.3.3 Configuring virtual interfaces with tagged VLAN..... | 337 |
| B.3.4 Example of the Cluster system (1:1 Standby)..... | 343 |
| B.3.5 Example of the Cluster system (Mutual standby)..... | 347 |
| B.3.6 Example of the Cluster system (N:1 Standby)..... | 351 |
| B.3.7 Example of the Cluster system (Cascade)..... | 356 |
| B.4 Example of configuring NIC switching mode (IPv4)..... | 362 |
| B.4.1 Example of the Single system without NIC sharing..... | 362 |
| B.4.2 Example of the Single system with NIC sharing..... | 364 |
| B.4.3 Example of the Single system in Physical IP address takeover function..... | 367 |
| B.4.4 Configuring virtual interfaces with tagged VLAN (synchronized switching)..... | 370 |
| B.4.5 Configuring virtual interfaces with tagged VLAN (asynchronized switching)..... | 374 |
| B.4.6 Example of the Cluster system (1:1 Standby)..... | 378 |
| B.4.7 Example of the Cluster system (Mutual standby) without NIC sharing..... | 382 |
| B.4.8 Example of the Cluster system (Mutual standby) with NIC sharing..... | 386 |

| | |
|---|------------|
| B.4.9 Example of the Cluster system in Physical IP address takeover function I..... | 389 |
| B.4.10 Example of the Cluster system in Physical IP address takeover function II..... | 393 |
| B.4.11 Example of the Cluster system (Cascade)..... | 396 |
| B.4.12 Example of the Cluster system (NIC non-redundant)..... | 400 |
| B.4.13 Example of the Cluster system (Virtual NIC)..... | 403 |
| B.5 Example of configuring NIC switching mode (IPv6)..... | 405 |
| B.5.1 Example of the Single system without NIC sharing..... | 405 |
| B.5.2 Example of the Single system with NIC sharing..... | 408 |
| B.5.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)..... | 411 |
| B.5.4 Configuring virtual interfaces with tagged VLAN (asynchronized switching)..... | 414 |
| B.5.5 Example of the Cluster system (1:1 Standby)..... | 418 |
| B.5.6 Example of the Cluster system (Mutual standby) without NIC sharing..... | 421 |
| B.5.7 Example of the Cluster system (Mutual standby) with NIC sharing..... | 425 |
| B.5.8 Example of the Cluster system (Cascade)..... | 429 |
| B.6 Example of configuring NIC switching mode (IPv4/IPv6)..... | 433 |
| B.6.1 Example of the Single system without NIC sharing..... | 433 |
| B.6.2 Example of the Single system with NIC sharing..... | 437 |
| B.6.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)..... | 441 |
| B.6.4 Configuring virtual interfaces with tagged VLAN (asynchronized switching)..... | 446 |
| B.6.5 Example of the Cluster system (1:1 Standby) without NIC sharing..... | 451 |
| B.6.6 Example of the Cluster system (Mutual Standby) without NIC sharing..... | 456 |
| B.6.7 Example of the Cluster system (Mutual Standby) with NIC sharing..... | 462 |
| B.6.8 Example of the Cluster system (Cascade)..... | 467 |
| B.7 Example of configuring GS/SURE linkage mode..... | 473 |
| B.7.1 Example of the Single system in GS/SURE connection function (GS communication function)..... | 473 |
| B.7.2 Example of the Single system in GS/SURE connection function (SURE communication function)..... | 475 |
| B.7.3 Example of the Single system in GS/SURE connection function (GS Hot-standby)..... | 476 |
| B.7.4 Example of the Single system in TCP relay function..... | 478 |
| B.7.5 Example of the Cluster system in GS/SURE connection function (GS communication function)..... | 480 |
| B.7.6 Example of the Cluster system in GS/SURE connection function (SURE communication function)..... | 483 |
| Appendix C Operations in Solaris Zones Environment..... | 487 |
| C.1 Overview of the Solaris Zones..... | 487 |
| C.2 Network Configuration of Solaris Zones..... | 487 |
| C.2.1 Network configuration of shared-IP zone..... | 488 |
| C.2.2 Network configuration of exclusive-IP zone..... | 488 |
| C.2.3 Network configuration of Kernel Zones..... | 489 |
| C.3 Support Set for Each Redundant Line Switching Mode..... | 490 |
| C.4 Operation of Redundant Line Switching Mode on Solaris Zones..... | 492 |
| C.4.1 Configuration to ensure reliable networks of shared-IP zone..... | 492 |
| C.4.1.1 Network high-reliability of shared-IP zone (Fast switching mode, GS/SURE linkage mode)..... | 492 |
| C.4.1.2 Network high-reliability of shared-IP zone (NIC switching mode)..... | 493 |
| C.4.2 Configuration to ensure reliable networks of exclusive-IP zone..... | 494 |
| C.4.2.1 Network high-reliability of exclusive-IP zone (NIC switching mode)..... | 495 |
| C.4.3 Configuration to ensure reliable networks of Kernel Zones..... | 495 |
| C.4.3.1 Network high-reliability of Kernel Zones (NIC switching mode)..... | 495 |
| C.4.3.2 Network high-reliability of Kernel Zones (GS/SURE linkage mode)..... | 496 |
| C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones..... | 497 |
| C.5.1 Configuration Procedure for Non-Global Zones..... | 498 |
| C.5.2 Configuration Procedure for Kernel Zones..... | 501 |
| C.6 Examples of Configuring System Environments..... | 504 |
| C.6.1 Configuration Example to Ensure Network Reliability of Shared-IP Zone..... | 504 |
| C.6.1.1 Example of configuration with Fast switching mode (IPv4)..... | 504 |
| C.6.1.2 Example of configuration with Fast switching mode (IPv6)..... | 507 |
| C.6.1.3 Example of configuration with Fast switching mode (IPv4/IPv6)..... | 511 |
| C.6.1.4 Example of configuration with NIC switching mode (IPv4 logical IP takeover)..... | 515 |
| C.6.1.5 Example of configuration with NIC switching mode (IPv6 logical IP takeover)..... | 519 |

| | |
|--|-----|
| C.6.1.6 Example of configuration with NIC switching mode (IPv4/IPv6)..... | 523 |
| C.6.1.7 Example of configuration with GS/SURE linkage mode..... | 528 |
| C.6.2 Configuration Example to Ensure Network Reliability of Exclusive-IP Zone..... | 532 |
| C.6.2.1 Example of configuration in the exclusive-IP zone (Physical IP takeover)..... | 532 |
| C.6.2.2 Example of configuration with tagged VLAN interfaces (synchronized switching)..... | 535 |
| C.6.2.3 Example of configuration with VNIC (Physical IP takeover)..... | 540 |
| C.6.3 Configuration Example to Ensure Network Reliability of Kernel Zones..... | 543 |
| Appendix D Operation in Oracle VM Environments..... | 544 |
| D.1 Overview of Oracle VM..... | 544 |
| D.2 Network Configuration of Oracle VM..... | 544 |
| D.3 Support Set for Each Redundant Line Switching Mode..... | 544 |
| D.4 Operation of Redundant Line Switching Mode in Oracle VM Environments..... | 544 |
| D.4.1 Configuration to ensure reliable networks in Oracle VM environment (Solaris 10)..... | 545 |
| D.4.2 Configuration to ensure reliable networks in Oracle VM environment (Solaris 11 or later)..... | 546 |
| D.5 Procedure for Configuring Redundant Line Control in Oracle VM Environments..... | 548 |
| D.6 Examples of Configuring System Environments..... | 548 |
| D.6.1 Example of configuration to ensure reliable networks in Oracle VM environment (Solaris 10)..... | 548 |
| D.6.2 Example of configuration to ensure reliable networks in Oracle VM environment (Solaris 11 or later)..... | 551 |
| Appendix E Cloning Environments..... | 555 |
| E.1 Designing network of the copy destination system..... | 555 |
| E.1.1 Designing the network of Fast switching mode..... | 556 |
| E.1.2 Designing the network of NIC switching mode..... | 556 |
| E.1.3 Designing the network of GS/SURE linkage mode..... | 557 |
| E.2 Copying the system image..... | 558 |
| E.3 Changing the setting of the copy destination system..... | 558 |
| E.3.1 Preparations..... | 558 |
| E.3.2 Changing the IP address of the physical interface..... | 559 |
| E.3.3 Changing the IP address of the virtual interface..... | 560 |
| E.3.4 Changing the IP address of the monitoring destination and the remote host..... | 561 |
| E.3.5 Changing the setting of cluster application (in cluster operation)..... | 562 |
| E.3.6 Enabling the changed setting..... | 562 |
| Appendix F Changes from previous versions..... | 564 |
| F.1 Changes from Redundant Line Control function 4.0 to version 4.1A10..... | 564 |
| F.1.1 New command..... | 564 |
| F.1.2 Incompatible commands..... | 564 |
| F.1.2.1 hanetbackup command..... | 564 |
| F.1.2.2 hanetrestore command..... | 564 |
| F.2 Changes from Redundant Line Control function 4.1A10 to version 4.1A20..... | 565 |
| F.2.1 New command..... | 565 |
| F.2.2 Incompatible commands..... | 565 |
| F.2.2.1 hanetconfig command..... | 565 |
| F.2.2.2 hanetpoll command..... | 565 |
| F.2.2.3 hanetobserv command..... | 566 |
| F.2.3 Other incompatibles..... | 566 |
| F.2.3.1 Resource state monitoring function for standby node..... | 566 |
| F.2.3.2 Interface state monitoring feature..... | 567 |
| F.3 Changes from Redundant Line Control function 4.1A20 to version 4.1A30..... | 567 |
| F.3.1 New command..... | 567 |
| F.3.2 Incompatible commands..... | 567 |
| F.3.2.1 hanetconfig command..... | 567 |
| F.3.2.2 hanetpoll command..... | 568 |
| F.3.2.3 strhanet command..... | 569 |
| F.3.2.4 stphanet command..... | 569 |
| F.3.2.5 dsppoll command..... | 570 |
| F.3.3 Other incompatibles..... | 571 |

| | | |
|------------|---|-----|
| F.3.3.1 | Activation timing of GS/SURE linkage mode on the cluster system..... | 571 |
| F.3.3.2 | Verifying the network address..... | 571 |
| F.3.3.3 | Logical number of NIC switching mode..... | 573 |
| F.4 | Changes from Redundant Line Control function 4.1A30 to version 4.1A40..... | 573 |
| F.4.1 | New command..... | 573 |
| F.4.2 | Incompatible command..... | 573 |
| F.4.3 | Other incompatibles..... | 573 |
| F.4.3.1 | Check for consistency between Solaris Zones and network configuration..... | 573 |
| F.4.3.2 | Reserve takeover virtual interface for fast switching mode..... | 574 |
| F.5 | Changes from Redundant Line Control function 4.1A40 to version 4.2A00..... | 575 |
| F.6 | Changes from Redundant Line Control function 4.2A00 to version 4.3A10..... | 575 |
| F.6.1 | New command..... | 576 |
| F.6.1.1 | hanetgw command..... | 576 |
| F.6.2 | Incompatible commands..... | 576 |
| F.6.2.1 | dspoll command..... | 576 |
| F.6.2.2 | hanetpoll command..... | 576 |
| F.6.3 | Other incompatibles..... | 577 |
| F.6.3.1 | Link status monitoring function..... | 577 |
| F.6.3.2 | User command execution function (Setup file for NIC switching mode)..... | 577 |
| F.6.3.3 | User command execution function (Setup file of the service for Redundant Line Control function)..... | 577 |
| F.6.3.4 | Virtual gateway..... | 578 |
| F.6.3.5 | Standby patrol..... | 578 |
| F.6.3.6 | RIP mode..... | 578 |
| F.6.3.7 | Self-checking function..... | 578 |
| F.6.3.8 | Change of the error output message (205)..... | 579 |
| F.7 | Changes from Redundant Line Control function 4.3A10 to version 4.3A20..... | 579 |
| F.7.1 | New command..... | 579 |
| F.7.2 | Incompatible command..... | 579 |
| F.7.3 | Other incompatibilities..... | 579 |
| F.7.3.1 | Collecting materials..... | 579 |
| F.8 | Changes from Redundant Line Control function 4.3A20 to version 4.3A40..... | 580 |
| F.8.1 | New command..... | 580 |
| F.8.2 | Incompatible command..... | 580 |
| F.8.3 | Other incompatibilities..... | 580 |
| F.8.3.1 | Kernel Zones..... | 580 |
| F.9 | Changes from Redundant Line Control function 4.3A40 to version 4.5A00..... | 580 |
| F.9.1 | New commands..... | 581 |
| F.9.2 | Incompatible commands..... | 581 |
| F.9.2.1 | hanetparam command..... | 581 |
| F.9.2.2 | hanetpoll command..... | 581 |
| F.9.3 | Other incompatible items..... | 582 |
| F.9.3.1 | Changing the installation directory..... | 582 |
| F.9.3.2 | Initial settings for link status monitoring..... | 582 |
| F.9.3.3 | Initial setting values for the standby interface inactivation method..... | 582 |
| F.9.3.4 | Detecting hang-up of the ping command..... | 582 |
| F.9.3.5 | Output messages to the console..... | 583 |
| F.9.3.6 | Fujitsu hot standby protocol..... | 583 |
| F.9.3.7 | Changing the startup timing of the HUB monitoring function..... | 584 |
| F.9.3.8 | Self-check function..... | 584 |
| F.10 | Changes from Redundant Line Control function 4.5A00 to version 4.5A10..... | 584 |
| Appendix G | Notice of supplemental information..... | 585 |
| G.1 | Changing Methods of Activating and Inactivating Interface..... | 585 |
| G.1.1 | Using NIC switching mode in shared-IP zone..... | 585 |
| G.2 | Frequently asked questions and answers..... | 585 |
| G.2.1 | I want to change the netmask settings or the IP address in the host file without changing the GLS definitions for the cluster system..... | 585 |

| | |
|---|-----|
| G.3 Troubleshooting..... | 586 |
| G.3.1 Communication as expected cannot be performed (Common to IPv4 and IPv6)..... | 586 |
| G.3.1.1 A default gateway is not set valid..... | 586 |
| G.3.1.2 Fails to activate a system or an interface in the NIS environment..... | 586 |
| G.3.1.3 Automatic address configuration lags behind for IPv6..... | 587 |
| G.3.1.4 Fails to communicate with GS in hot standby configuration..... | 587 |
| G.3.2 Virtual interface or the various functions of Redundant Line Control function cannot be used..... | 588 |
| G.3.2.1 An interface of NIC switching mode is not activated..... | 588 |
| G.3.2.2 It does not failback at the time of the restoration detection by standby patrol in NIC switching mode..... | 589 |
| G.3.2.3 Error detection message displays for standby patrol in NIC switching mode..... | 589 |
| G.3.2.4 Solaris Zones cannot be started..... | 589 |
| G.3.2.5 Services of Redundant Line Control function cannot be started (when NIC failed)..... | 590 |
| G.3.2.6 Services of Redundant Line Control function cannot be started (when inconsistency of file system occurred)..... | 593 |
| G.3.2.7 Fails to activate a virtual interface in NIC switching mode for IPv6..... | 593 |
| G.3.3 Failure occurs during operation (Common to both Single and Cluster system)..... | 597 |
| G.3.3.1 Switching takes place in NIC switching mode regardless of failure at the monitoring end..... | 597 |
| G.3.3.2 Takes time to execute an operation command or to activate a userApplication..... | 597 |
| G.3.3.3 TCP connection is not divided in GS/SURE linkage mode..... | 598 |
| G.3.3.4 A virtual driver hang up was detected by the Self-Check function..... | 598 |
| G.3.3.5 ping command to HUB monitoring destination hangs..... | 598 |
| G.3.4 Failure occurs during operation (In the case of a Cluster system)..... | 599 |
| G.3.4.1 Node switching is not executed in Fast switching mode..... | 599 |
| G.3.5 Failure occurs when using IPv6 address (Common to both Single and Cluster system)..... | 600 |
| G.3.5.1 Automatic address configuration malfunctions while using standby interface in NIC switching mode..... | 600 |
| G.3.6 Failure occurs while using IPv6 address (In the case of a Cluster system)..... | 600 |
| G.3.6.1 Fails to activate IPv6 takeover address..... | 600 |
| G.3.7 Resuming connection lags after switching (Common to both Single and Cluster system)..... | 600 |
| G.3.7.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode..... | 600 |
| G.3.8 Incorrect operation by the user..... | 601 |
| G.3.8.1 Accidentally deleted the virtual interface with ifconfig command..... | 601 |
| G.3.9 System in Solaris Zones..... | 601 |
| G.3.9.1 Patch application fails..... | 601 |
| G.3.10 SMF service using the GLS virtual IP..... | 602 |
| G.3.10.1 Startup of the service or connection to the server fails in SMF service using the GLS virtual IP address..... | 602 |
| Glossary..... | 603 |
| Index..... | 608 |

Chapter 1 Overview

This chapter discusses the concept of the redundant line control function provided by Global Link Services (hereinafter GLS).

1.1 What is redundant line control?

The redundant line control function provides a high-reliability communication infrastructure that supports continuous transmission in the event of a network path or card failure by making transmission routes redundant with multiple NIC (Network Interface Cards).

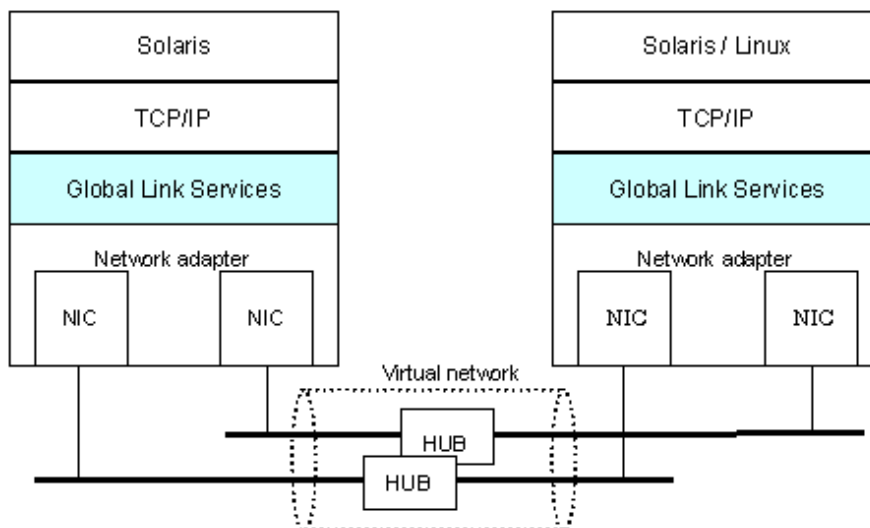
GLS enables the following four network control methods. For details on the virtual NIC mode, see "PRIMECLUSTER Global Link Services Configuration and Administration Guide 4.5: Redundant Line Control Function for Virtual NIC Mode."

Fast switching mode

In Fast switching mode, a redundant transmission route between Solaris servers or Linux servers in the same network is used so that the total amount of data transferred can be increased, and that the data communication can be continued even if the transmission route fails. It also enables higher levels of throughput through redundant transmission routes. GLS performs early failure detection, so when one transmission route fails, the failed route will be cut off then the system will be operated on a reduced scale. The compatible hosts are SPARC Servers, PRIMEPOWER, GP7000F, Fujitsu S series, GP-S, PRIMERGY, and PRIMEQUEST.

Note that fast switching mode cannot be used to communicate with hosts on the other networks beyond the router.

Figure 1.1 Fast switching mode

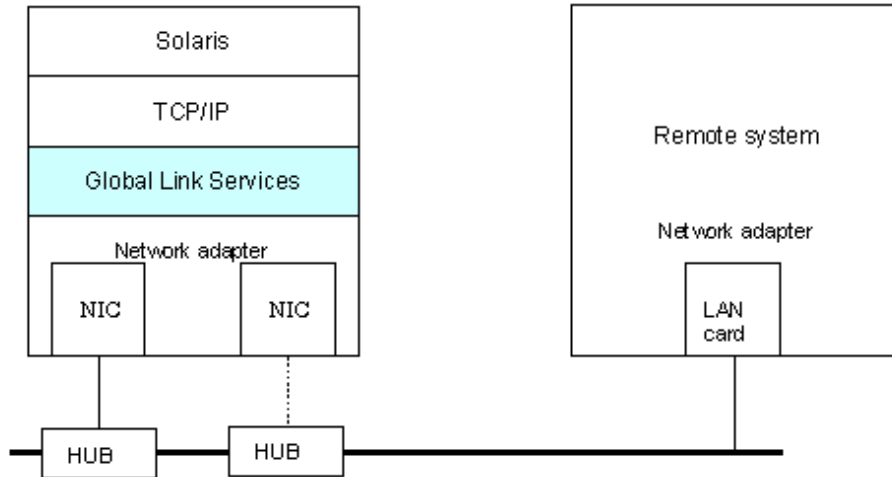


NIC switching mode

In NIC switching mode, redundant NICs (LAN cards) are connected to each other on the same network and used exclusively. If one transmission route fails, ongoing communications will be switched to the other transmission route. There are no restrictions on remote systems to communicate with.

Note that NIC switching mode can be used to communicate with any hosts on the other networks beyond the router.

Figure 1.2 NIC switching mode

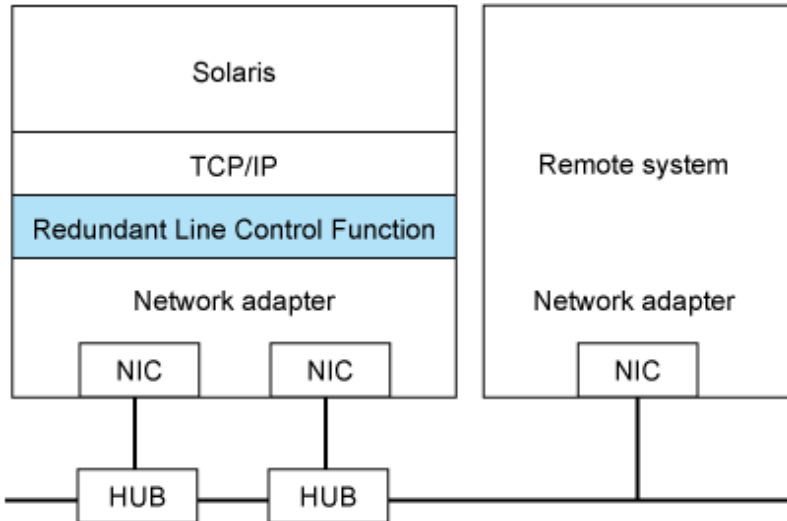


Virtual NIC mode

Virtual NIC mode provides a high-reliability communication by grouping multiple network interfaces on the same network as one virtual interface. If one transmission route fails, ongoing communications will be switched to the other transmission route. There are no restrictions on remote systems to communicate with. When comparing the virtual NIC mode to the NIC switching mode which makes network interfaces on the same network redundant, there are the following features:

- Specifying IP addresses to be monitored is unnecessary by the fault monitoring function.
- In Solaris Zones environments, the configuration where virtual interfaces connect to zones is available.
- In Oracle VM environments, the configuration where virtual interfaces connect to virtual bridges is available.

Figure 1.3 Virtual NIC mode



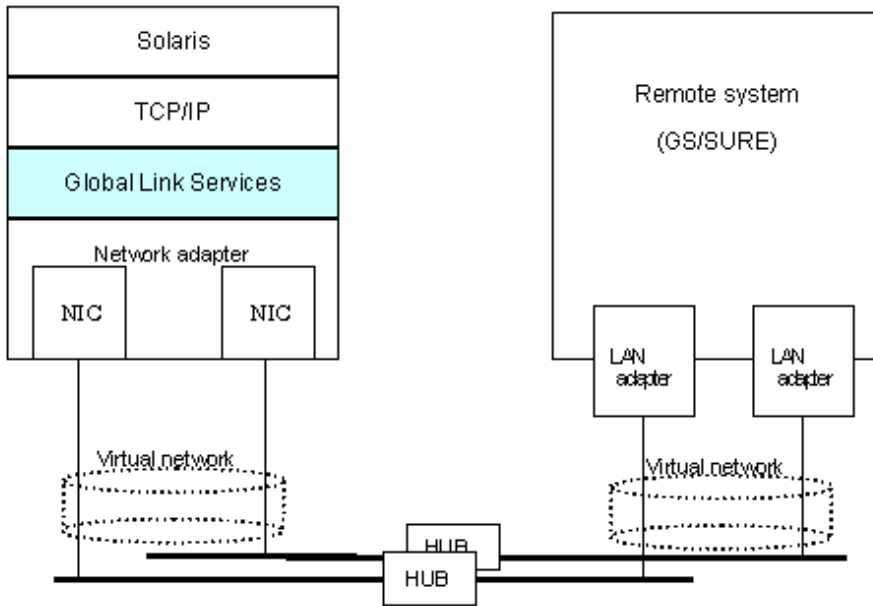
GS/SURE linkage mode

GS/SURE linkage mode enables the system to control lines by using a Fujitsu method for high-reliability communication between the system and Global Server or SURE SYSTEM. In this mode, duplicated lines are used concurrently. During normal operation, lines are automatically assigned to each TCP connection for communication. In the event of a fault, the system disconnects the faulty line and operates on a reduced scale by moving the TCP connection to the normal line. This mode provides the following connection functions (Hereinafter GS refers to Global Server and SURE refers to SURE SYSTEM).

GS/SURE connection function

It is possible to directly connect to GS and SURE on the same LAN.

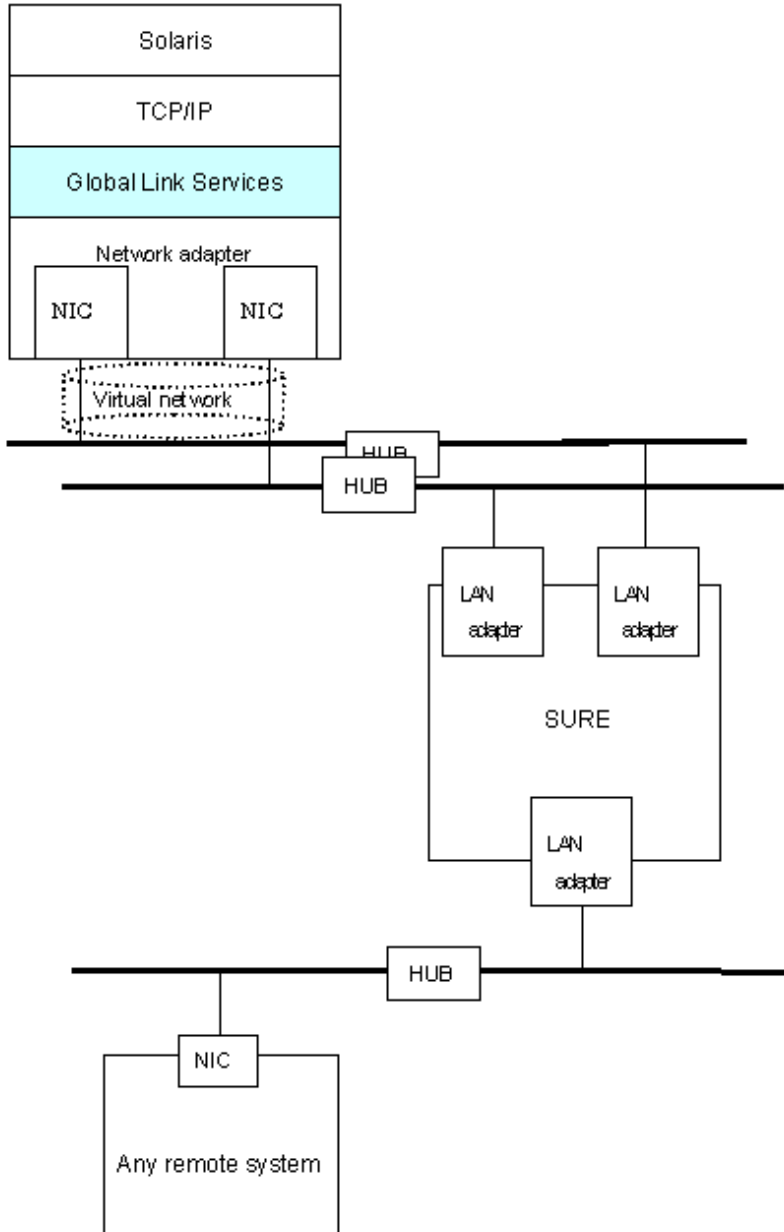
Figure 1.4 GS/SURE linkage mode (GS/SURE connection function)



TCP relay function

It is possible to connect to an optional system by relaying a TCP connection with SURE. This function is available only when a relay device is SURE.

Figure 1.5 GS/SURE linkage mode (TCP relay function)



1.1.1 Functional comparison

Table 1.1 Function comparison (1) and Table 1.2 Function comparison (2) compare the functions of each network switching mode.

Table 1.1 Function comparison (1)

| Redundant line switching method | | Fast switching mode | NIC switching mode |
|---------------------------------|---------------------------------------|--|--|
| Network control | | Makes both of redundant transmission routes active and uses them concurrently. A stream of data is sent on a TCP connection. | Activates and uses one redundant transmission route exclusively and deactivates the other route. |
| Fault monitoring | Detectable failures | NIC, cable, HUB, remote host | NIC, cable, HUB |
| | Fault monitoring Monitoring method | Monitors framework between the NIC of the host and that of the remote host. If the frame | Monitors HUB using the ping command. If the HUB communication is disrupted, a |

| Redundant line switching method | | Fast switching mode | NIC switching mode |
|---------------------------------|-----------------------------|----------------------------|---|
| | | | communication is disrupted, a transmission route failure will be detected. |
| | | Failure detection time | 5 to 10 seconds (Default) |
| | | | transmission route failure will be detected. |
| | | Recovery monitoring method | <ul style="list-style-type: none"> - When an error is detected by ping: 22 to 27 seconds (Default) - When a NIC link down is detected: 2 to 7 seconds (Default) |
| | | Recovery detection time | 1 to 5 seconds (Default) |
| | Recovery monitoring | Recovery monitoring method | Monitors framework between the NIC of the host and that of the remote host. If the frame communication is disrupted, a transmission route failure will be detected. |
| | | Recovery detection time | 1 to 15 seconds (Default) |
| | Fault monitoring start/stop | | Automatically starts along with virtual interface activation and stops along with its deactivation. |
| | | | Automatically starts along with virtual interface activation and stops along with its deactivation. Manual startup or stop of fault monitoring is also allowed with the operational command. |
| Line switching | Switchover | | Automatically disconnects a failed transmission route and uses the other transmission route. Manual disconnection of the failed route is also allowed with the operational command. |
| | Switchback | | Automatically deactivates NIC of a failed transmission route and activates a standby NIC. Manual switching operation is also allowed with the operational command. |
| | Switchback | | If a failed transmission route is recovered, it will automatically rejoin an ongoing operation. Manual rejoining is also allowed with the operational command. |
| | | | If a failed transmission route is recovered, it will automatically rejoin operation as a standby NIC. Manual rejoining is also allowed with the operational command. |
| Conditions | Remote hosts | | SPARC Servers, PRIMEPOWER, GP7000F, GP-S, Fujitsu S series, PRIMERGY, PRIMEQUEST |
| | IP addresses | | Arbitrary host |
| | Solaris Zones | | IPv4 address, IPv6 address |
| | | | IPv4 address, IPv6 address |
| | | | Operated on a global zone. Ensures a high-reliability communication infrastructure on both of the global and shared-IP zones. |
| | | | Operated on a global zone, an exclusive-IP zone, or Kernel Zones. Ensures a high-reliability communication infrastructure regardless of the zone type. |

Table 1.2 Function comparison (2)

| Redundant line switching method | Virtual NIC mode | GS/SURE linkage mode |
|---------------------------------|--|---|
| Network control | Activates and uses one redundant transmission route exclusively and deactivates the other route. | Makes both of redundant transmission routes active and uses |

| Redundant line switching method | | Virtual NIC mode | GS/SURE linkage mode | |
|---------------------------------|-----------------------------|--|--|---|
| | | | them concurrently. A stream of data is sent on a TCP connection. | |
| Fault monitoring | Detectable failures | NIC, Cable failure, HUB | NIC failure, Cable failure, HUB failure, Remote host failure (system failure) | |
| | Fault monitoring | Monitoring method | If the link status of NIC becomes link down, a transmission route failure will be detected. Also, if the reception is not returned within the specified time by exchanging heartbeat messages between NICs on the local host, a transmission route failure will be detected. | |
| | | Failure detection time | <ul style="list-style-type: none"> - When an error is detected by heartbeat messages: 8 to 11 seconds (Default) - When a NIC link down is detected: 1 second (Default) | 25 to 30 seconds (Default) |
| | Recovery monitoring | Recovery monitoring method | If the reception is returned within the specified time by exchanging heartbeat messages between NICs on the local host, a transmission route recovery will be detected. | Monitors a remote host using the ping command. If the system receives a reply from the remote host within a specified time, transmission route recovery will be detected. |
| | | Recovery detection time | 1 to 3 seconds (Default) | 1 to 5 seconds (Default) |
| | Fault monitoring start/stop | | Automatically starts along with virtual interface activation and stops along with its deactivation. | Automatically starts along with virtual interface activation and stops along with its deactivation. Manual startup or stop of fault monitoring is also allowed with the operational command. |
| Line switching | Switchover | Automatically goes around a failed transmission route and continues the communication. Manual disconnection of the failed route is also allowed with the operational command. | Automatically disconnects a failed transmission route and uses the other transmission route. Manual disconnection of the failed route is also allowed. | |
| | Switchback | If a failed transmission route is recovered, it will automatically rejoin an ongoing operation. Manual rejoining is also allowed with the operational command. | If a failed transmission route is recovered, it will automatically join communication. Manual rejoining is also allowed. | |
| Conditions | Remote hosts | Any host | GS (Global Server), SURE SYSTEM, ExINCA | |
| | IP addresses | IPv4 address, IPv6 address | IPv4 address | |
| | Solaris Zones | Operated on a global zone. Ensures a high-reliability communication infrastructure on a global zone, | Operated on a global zone and Kernel Zones. Ensures a high-reliability communication | |

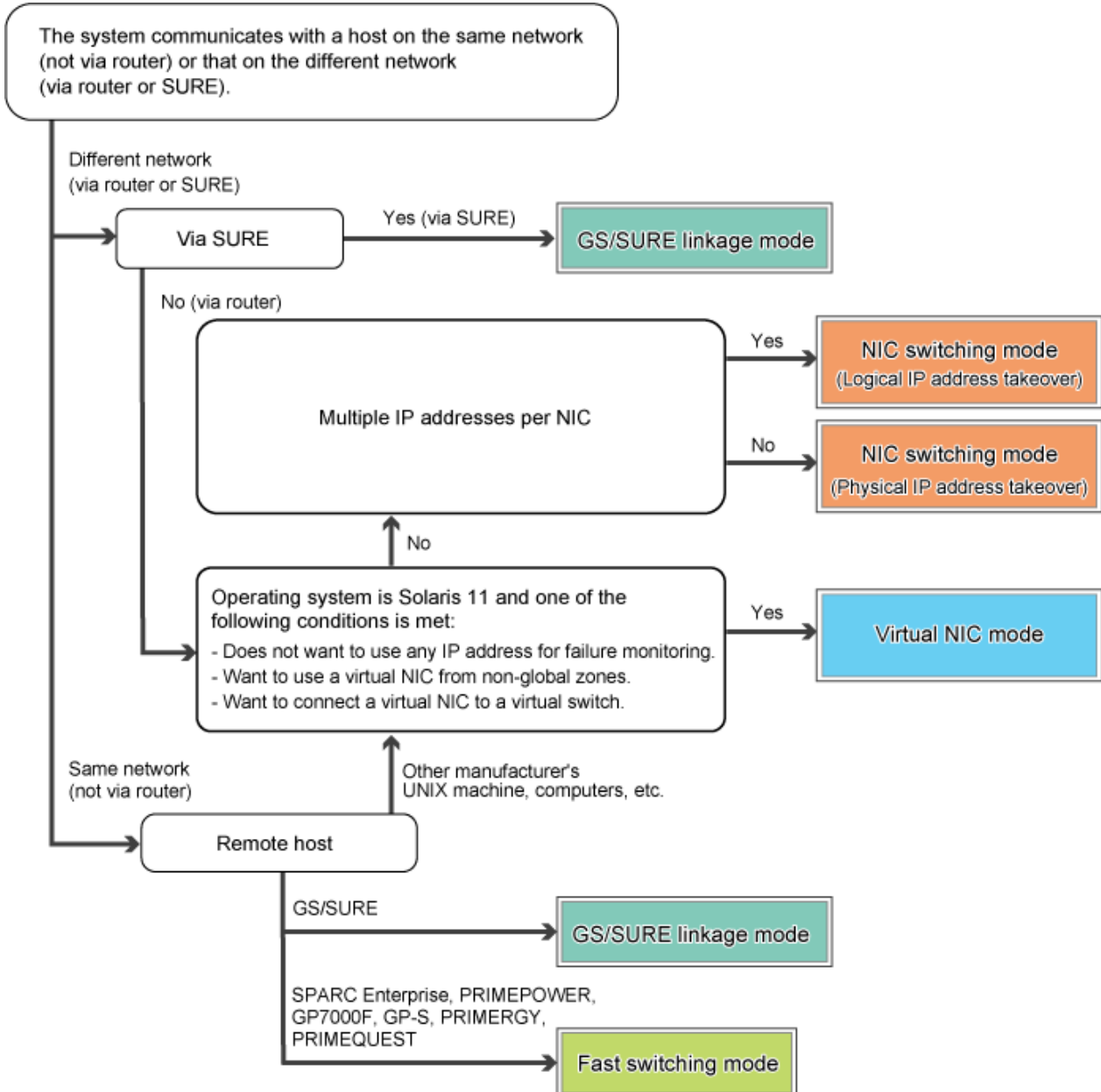
| Redundant line switching method | Virtual NIC mode | GS/SURE linkage mode |
|---------------------------------|------------------------------------|--|
| | non-global zone, and Kernel Zones. | infrastructure on the global zone, shared-IP zone, and Kernel Zones. |

1.1.2 Criteria for selecting redundant line control methods

You are supposed to select a redundant line control method according to your system operational conditions.

The flow chart for shown in [Figure 1.6 Redundant line control method decision flow chart](#) will assist in determining the redundant line control method that would be the most effective for you.

Figure 1.6 Redundant line control method decision flow chart



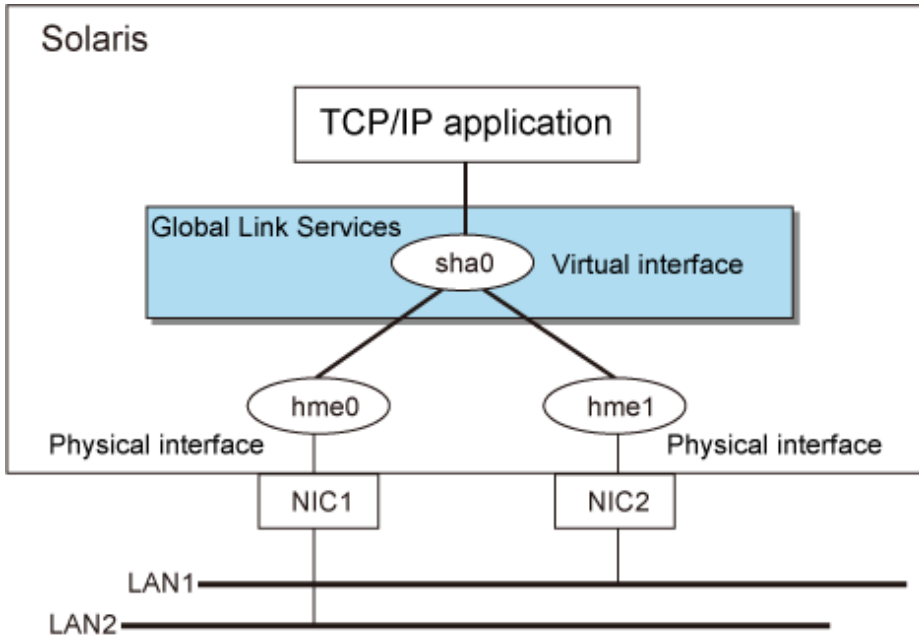
1.2 Redundant line control effects

The redundant line control function supports a high-reliability control network in terms of flexibility and fault-resistance.

1.3 System Configuration

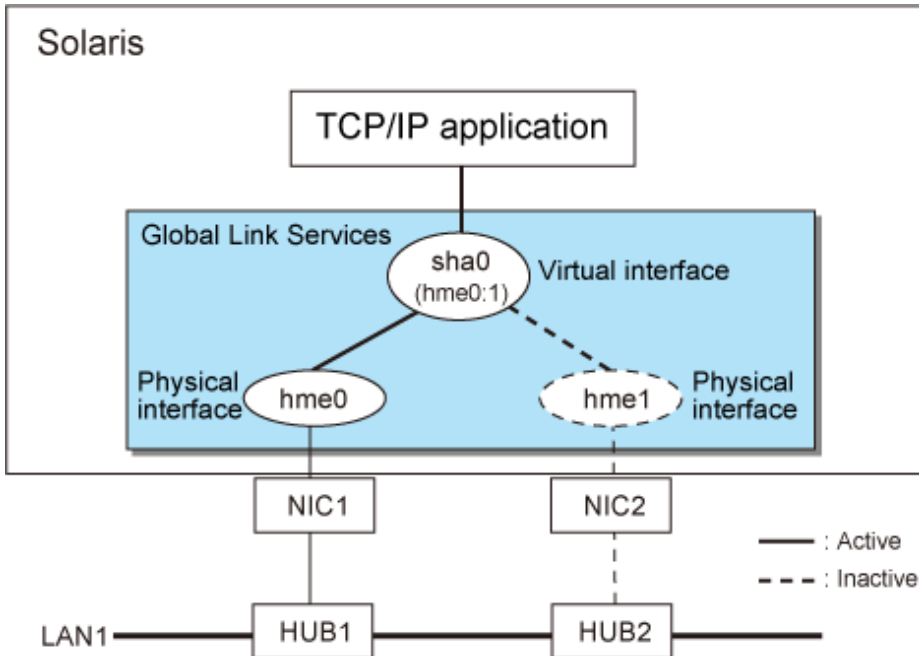
Fast switching mode

Figure 1.7 Fast switching



NIC switching mode

Figure 1.8 NIC switching mode



GS/SURE linkage mode

Figure 1.9 GS/SURE linkage mode (GS/SURE connection function)

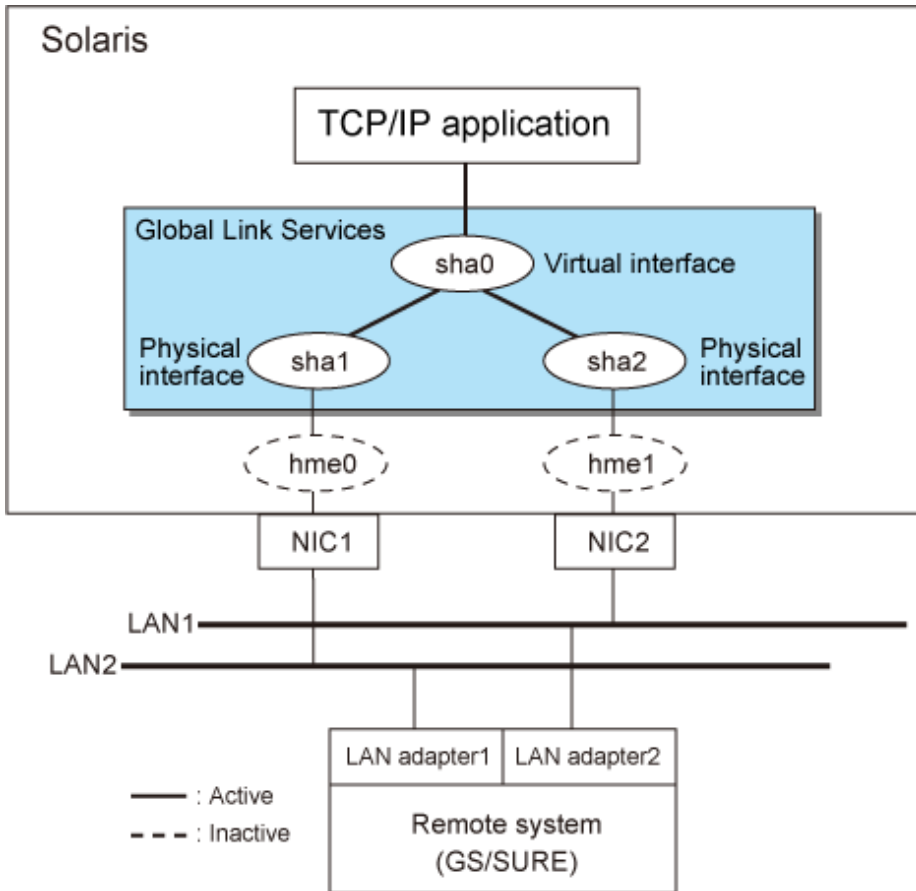
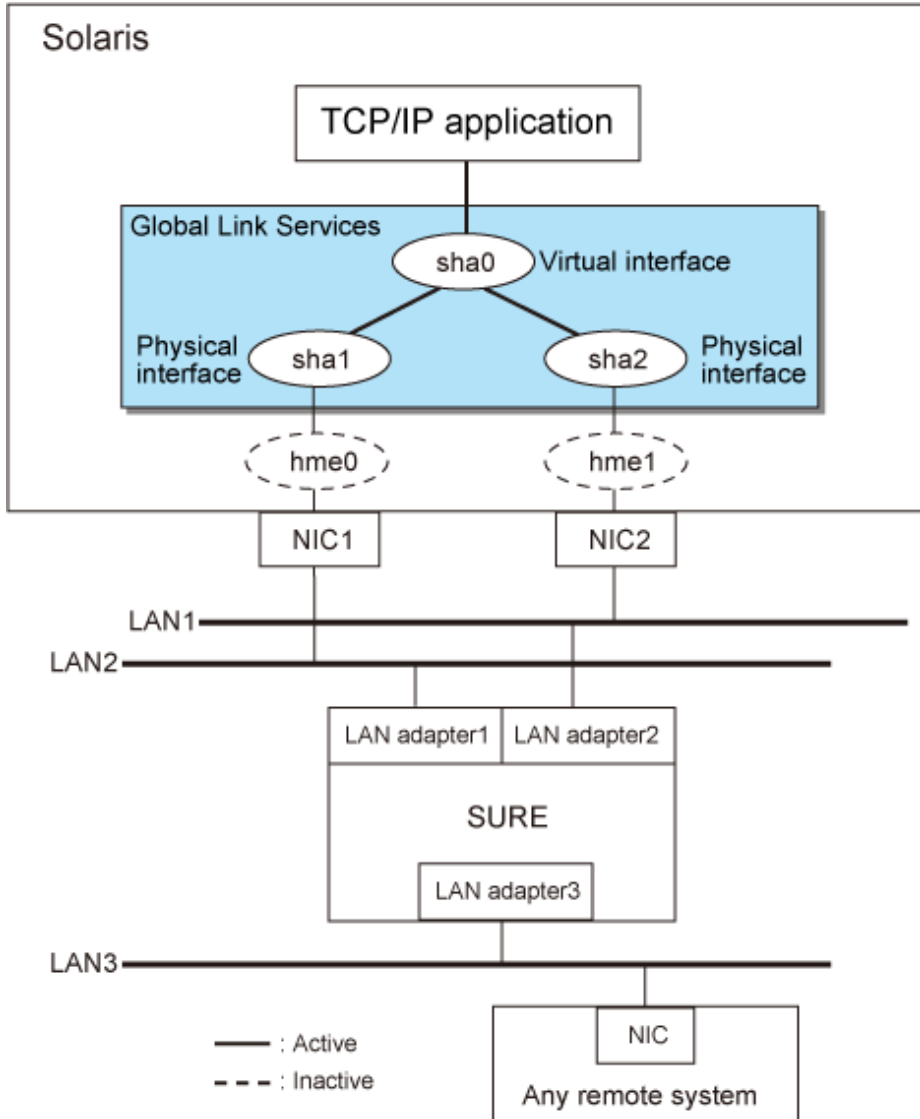


Figure 1.10 GS/SURE linkage mode (TCP relay function)



Redundant Line Control function consists of the following components:

| | | |
|-------------------------------|---|--|
| Main unit | SPARC Servers | |
| NIC (Network Interface Cards) | LAN card installed on the main unit and cards supported by the main unit | |
| HUB (NIC switching mode) | IP address information must be configured for HUB, e.g. HUB with SNMP agent | |
| Operating system (OS) | <ul style="list-style-type: none"> - Solaris 10 - Solaris 11 or later | |
| Interfaces | Physical interface | Generated by each NIC. The interface name is determined by the NIC type (e.g. hmeX and qfeX). In GS/SURE linkage mode, physical interfaces are generated through redundant line control. The interface name is shaX. |
| | Tagged VLAN interface | Logical interface generated by NIC that supports a tagged VLAN (IEEE802.1Q). The interface name varies depending on NIC type (e.g. ce1000, fjgi2001) |

| | | |
|----------------|--|---|
| | Virtual interface | <p>Generated through redundant line control (e.g. sha0 and sha1).</p> <p>Network applications can communicate using a virtual IP address assigned to the virtual interface.</p> <p>In NIC switching, the virtual interface name is used technically although no virtual interface is generated. A logical IP is allocated to the actual network so that the network applications enable communication through the logical IP address.</p> |
| | Other interfaces | <p>Link aggregation (with LACP) interfaces (aggr0, aggr1, etc.) and virtual NICs (vnic0, vnic1, etc.) connected to a virtual bridge are available.</p> |
| Network number | Fast switching mode and GS/SURE linkage mode | <p>A different network number is assigned to each physical interface and a virtual interface.</p> <p>In Figure 1.7 Fast switching, three network numbers must be prepared for the three interfaces.</p> |
| | NIC switching mode | <p>Only one number is assigned to each network. No virtual interface is generated</p> |
| IP address | Fast switching mode | <p>An IP address must be allocated to each physical interface and a virtual interface. If there are two or more virtual interfaces, an IP address will be allocated to each virtual interface. Both IPv4 address and IPv6 address can be used.</p> |
| | NIC switching mode | <p>An IP address must be allocated to each logical interface. If there are two or more logical interfaces, an IP address will be allocated to each logical interface. Both IPv4 address and IPv6 address can be used.</p> |
| | GS/SURE linkage mode | <p>An IP address must be allocated to each physical interface and a virtual interface. If there are two or more virtual interfaces, an IP address will be allocated to each virtual interface. Only IPv4 can be used.</p> |

Chapter 2 Feature description

This chapter outlines the functions and features of GLS.

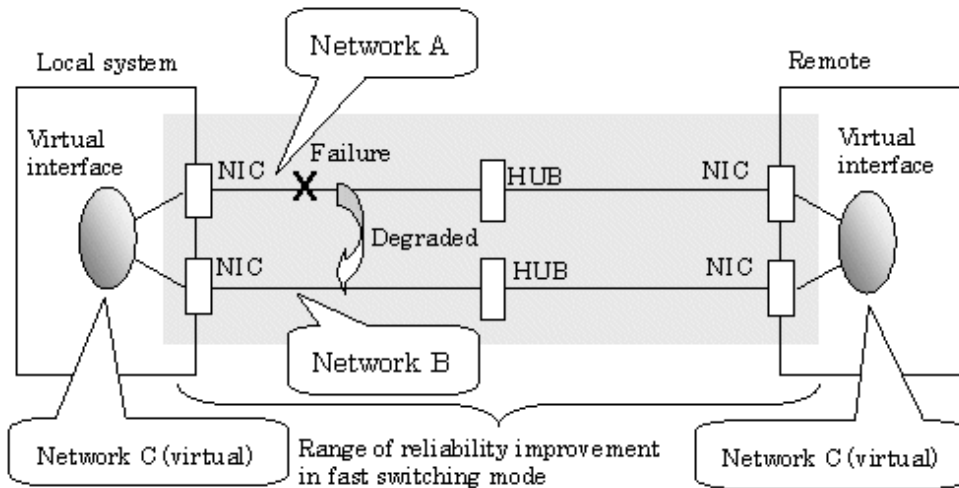
2.1 Overview of Functions

2.1.1 Fast switching mode

In this mode, each multiple NIC (Network Interface Card) is connected to a different network and all of these NICs are activated and then used concurrently. Each outgoing packet is transmitted via an appropriate line according to the line conditions (whether or not any failure has occurred).

Also, an interface that is virtual (called a virtual interface in this document) is generated so that multiple NICs can be seen as one logical NIC. A TCP/IP application can communicate with the remote system by using an IP address (called a virtual IP address in this document) set in this virtual interface as its own IP address of the local system, irrespective of the physical network redundant configuration.

Figure 2.1 Example of duplicated operation in Fast switching mode



Connection type

A system with which communication is to be carried out is connected to the same network and is not allowed to connect to a different network.

Features

In the event of a failure, lines can be switched swiftly in a short period of time without affecting the applications. Since redundant lines are all activated, each line can be used for different purposes, enabling the efficient use of resources.

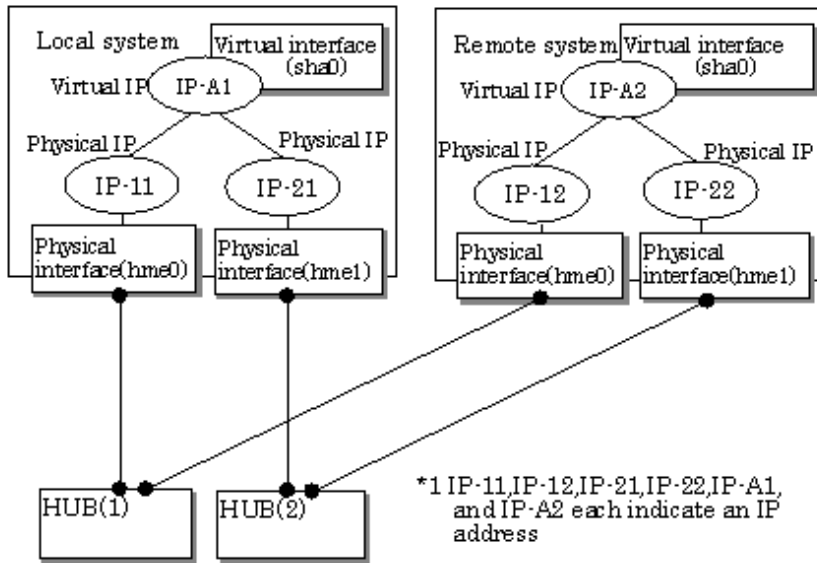
Example of recommended application

This mode is appropriate, for example, to communications between the application server and database server in a three-tier client-server system.

System configuration

Figure 2.2 System configuration for Fast switching mode shows a system configuration for Fast switching mode:

Figure 2.2 System configuration for Fast switching mode



The following explains each component and its meaning:

Physical interface

Indicates a physical interface (such as hme0 and hme1) of the duplicated NIC.

Physical IP

Indicates an IP address attached to a physical interface. This IP address is always active. Available IP addresses are IPv4 and IPv6 address.

Virtual interface

Indicates a virtual interface (such as sha0) so that the duplicated NIC can be seen as one NIC.

Virtual IP

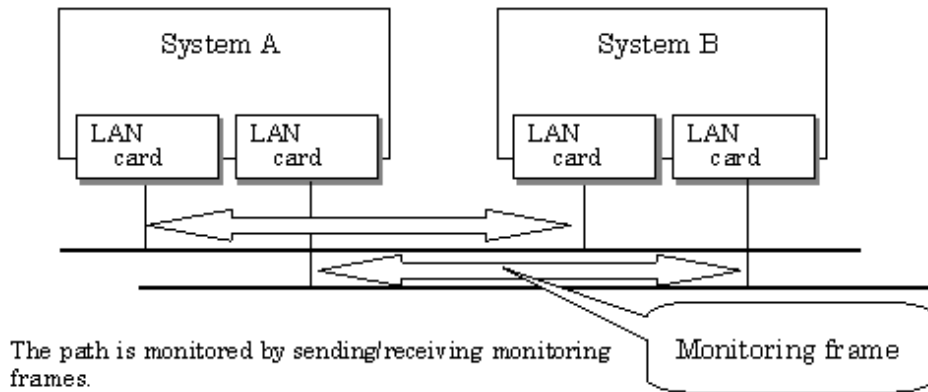
Indicates a source IP address to be allocated to the virtual interface for communication with the remote hosts. Available IP addresses are IPv4 and IPv6 address.

2.1.1.1 Fault monitoring function

Fault monitoring

Sends a dedicated monitor frame to the other system's NIC at regular intervals (a default value is five seconds. It is possible to change by the hanetparam command) and waits for a response. When received a response, decides that a route is normal, and uses it for communication until next monitoring. When received no response, decides that an error occurred, and not use it for communication until decides it is normal at next monitoring. Monitoring is done in a NIC unit that the other device equips.

Figure 2.3 Monitoring method in Fast switching mode



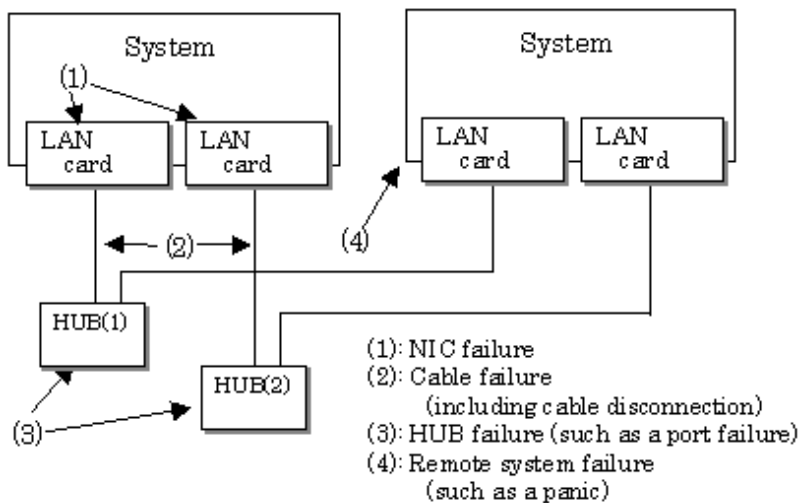
Switching time

If a failure occurs in a multiplexed line, disconnecting the line takes about 10 seconds.

Detectable failures

The following failures can be detected:

Figure 2.4 Detectable failures in Fast switching mode



Because the failures (1) - (4) appear to be the same failure, a type of the failure cannot be specified. Each device has to be checked to make this determination.

Fault monitoring start/stop

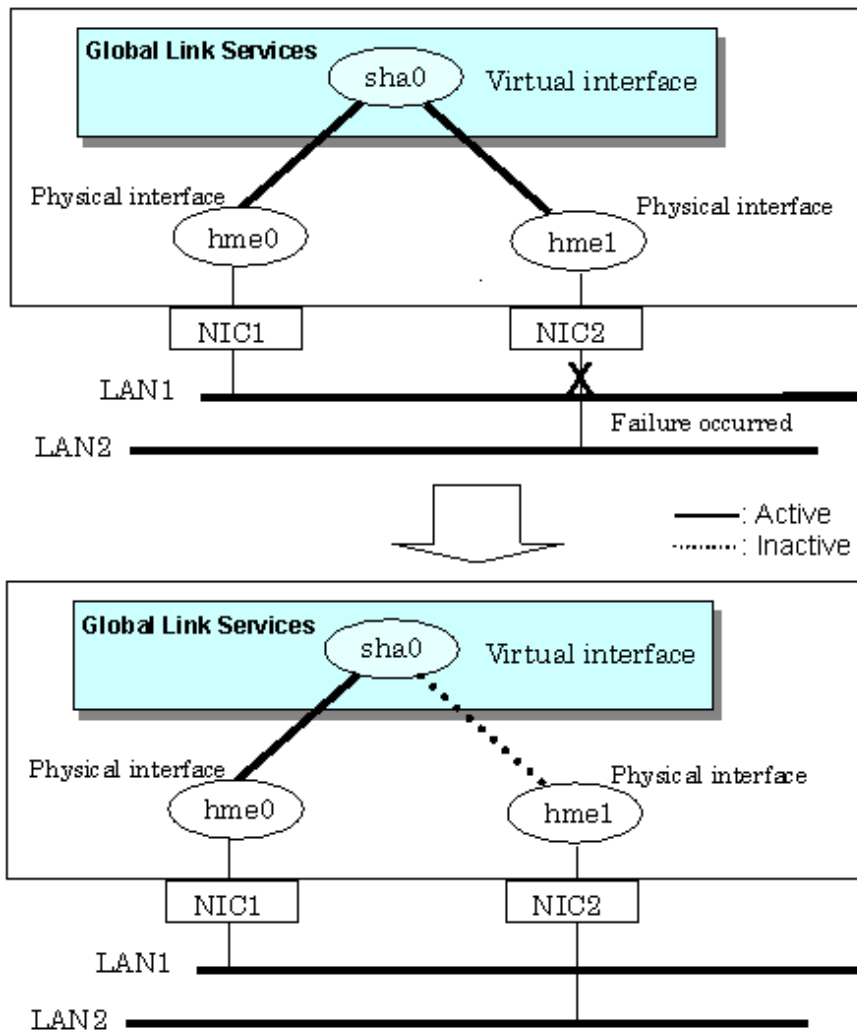
Monitoring is started automatically when the virtual interface is activated. Inactivation of virtual interface automatically stops monitoring. In cluster operation, the system allows each node to be started or stopped independently.

2.1.1.2 Switching function

Switching operation

A line detected its failure is automatically eliminated from network routes, and the only normal lines take over communication routes. Therefore, if at least one normal line remains, the communication can continue without rebooting the system. It is also possible to disconnect a specific line manually by using the operational command (hanetnic command).

Figure 2.5 Outline of switching operation performed when a failure occurs in Fast switching mode



Failback operation

If the faulty line of a physical interface is recovered, the physical interface is automatically restored for normal communication. If a line was disconnected manually, the failback of the line needs to be performed manually to restore the original status.

2.1.1.3 Connectable remote host

An associated host is able to communicate with the following systems:

- SPARC Servers
- PRIMEPOWER
- GP7000F
- GP-S
- Fujitsu S series
- PRIMERGY
- PRIMEQUEST

2.1.1.4 Available application

The requirement for user applications that can be operated in this mode is as follows:

- Application using the TCP or UDP.

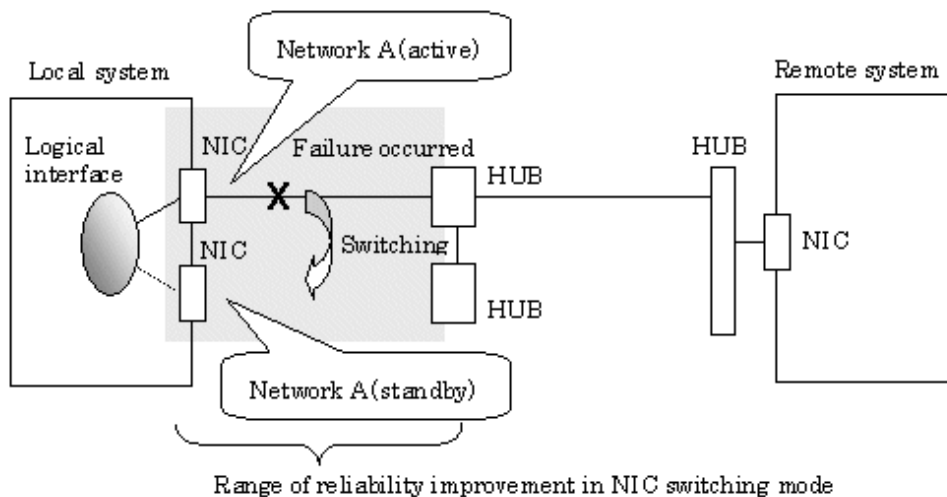
2.1.1.5 Notes

- When assigning IPv4 address to the virtual interface, IPv4 address must be assigned to all the redundant physical interfaces.
- If assigning IPv6 address to the virtual interface, IPv6 address must be assigned to all the redundant physical interfaces.
- If assigning both IPv4 and IPv6 to the virtual interface, these two forms of an IP address must be assigned to all the redundant physical interfaces.
- No multi-cast IP address can be used.
- Do not change the name of the virtual interface and the interface that is made redundant with the virtual interface. If names are changed, virtual interfaces are not properly activated and deactivated.

2.1.2 NIC switching mode

In this mode, duplicated NICs are connected to the same network and switching control of lines is performed based on the exclusive use (During normal operation, one NIC is made to go "up" for communication). A TCP/IP application can conduct communication with the remote system, irrespective of NIC switching, by using an IP address set in this "up" physical interface as its own local system IP address.

Figure 2.6 Example of duplicated operation in NIC switching mode



Information

NIC switching mode handles logical interface as a takeover interface. When using physical interfaces hme0 and hme1, the takeover interface becomes hme0:1 and hme1:1. Note that it is possible to takeover physical interface without using logical interface. Look under section "2.1.2.2 Switching function" for details on NIC switching mode.

Connection type

Duplicated NICs are connected to the same network. The remote system with which communication is to be carried out can be connected to either the same network or a different network via routers.

Features

If each network device (such as the HUB and routers) has the duplicating function in a multi-vendor environment, this mode is effective when improving overall reliability in combination with these devices. In this case, the range of duplication is defined for each vendor.

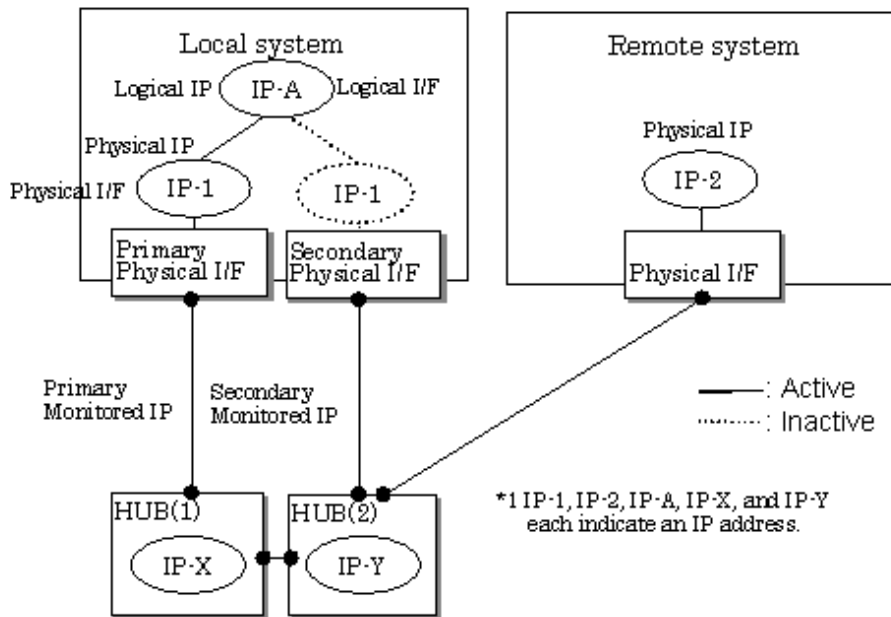
Recommended application areas

This mode is appropriate, for example, to communications in a multi-vendor environment in which UNIX servers and PC servers of other companies are mixed.

System configuration

Figure 2.7 System configuration in NIC switching mode shows a system configuration for NIC switching mode:

Figure 2.7 System configuration in NIC switching mode



The following explains each component and its meaning:

Primary physical interface

Indicates, of the duplicated NICs, the physical interface to be used first by activating it.

Secondary physical interface

Indicates the physical interface to be used after switching when a line failure is detected in the Primary physical interface.

Physical IP

Indicates an IP address attached to the Primary or Secondary physical interface. This IP address is always active. IPv4 address can be used for a physical interface. In case of IPv6, a link local address is automatically set as a physical IP address.

Primary monitored IP

Indicates the IP address of a monitored device (HUB) obtained when the Primary physical interface is used. In NIC switching mode, it is possible to use both IPv4 and IPv6 addresses as an address form.

Secondary monitored IP

Indicates the IP address of a monitored device (HUB) obtained when the Secondary physical interface is used. In NIC switching mode, it is possible to use both IPv4 and IPv6 address as an address form.

Logical IP

Indicates a local IP address for communication with the remote device. In NIC switching mode, it is possible to use both IPv4 and IPv6 addresses as an address form. When using a physical IP address takeover function, it is not activated. Please refer to "[2.1.2.2 Switching function](#)" about a physical IP address takeover function.

2.1.2.1 Fault monitoring function

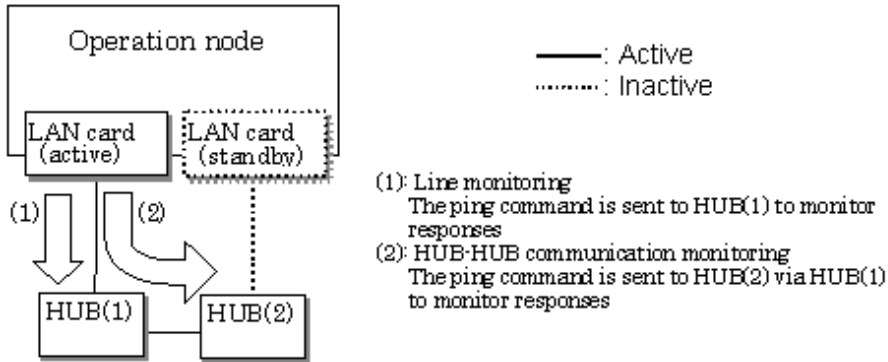
Fault monitoring

The ping command is issued periodically to the HUB connected to the NIC currently operating and its response is monitored. Optionally, HUB-to-HUB communication can be monitored.

If a failure is detected in the NIC currently operating, the system switches to the standby NIC and similar monitoring starts from the standby NIC side. Then, if a failure is also detected with the standby NIC, line monitoring stops.

When using a standby patrol function, monitoring starts automatically at the recovery of all transfer routes.

Figure 2.8 Monitoring method in NIC switching mode

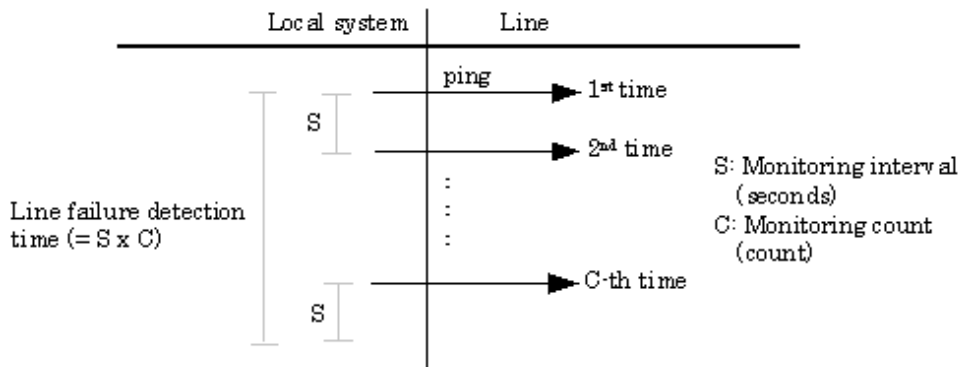


Switching time

The estimated switching time of a line is indicated by "monitoring interval (sec)" multiplied by "monitoring count (count)." The monitoring interval can be set in the range of 1 to 300 seconds and the monitoring count can be set in the range of 1 to 300 times. By default, they are 5 seconds and 5 times respectively. For details, see ["3.6.6.3 Transfer route error detection time for NIC switching mode."](#)

Even if the ping command failed immediately after started monitoring, it is not regarded as a communication line failure until the waiting time (sec) for the Ethernet linkup passed. It is possible to set the waiting time for linkup in a range of 1 to 300 seconds and a default value is 60 seconds. However, if the specified value is less than "monitoring interval" multiplied by "monitoring count," the system ignores the specified link-up time and adopts the time calculated by multiplying "monitoring interval" by "monitoring count."

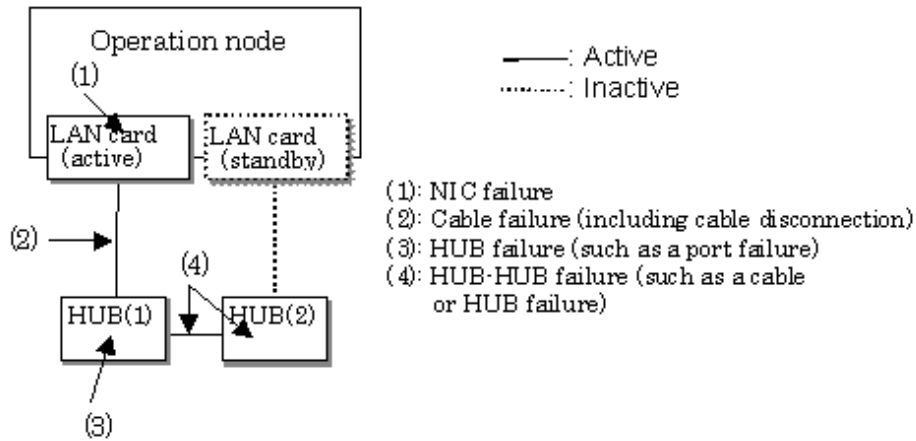
Figure 2.9 Fault detection time in NIC switching mode



Detectable failures

The following failures can be detected:

Figure 2.10 Effective monitoring range in NIC switching mode



Because the failures in (1) to (3) appear to be the same failure, it is not possible to determine under which of the four failure types these failures should be classified. Each device has to be checked to make this determination.

Monitoring start/stop timing

The line monitoring in NIC switching mode is automatically started when the system is activated and is automatically stopped when the system is stopped. In cluster operation, the line monitoring of each node is started and stopped independently. It is also possible to start or stop the line monitoring manually using the operational command (hanetpoll command).

2.1.2.2 Switching function

Switching operation

Switching operation changes the status of an active NIC into "inactive" state and then changes the status of standby NIC to "active" so that standby NIC can run as a new active device. At this point, IP addresses (physical IP and logical IP) are taken over and then an ARP request packet is broadcasted, in which the MAC address/IP addresses of the local node are set as the source.

It is possible to choose either a logical IP address takeover function or a physical IP address takeover function as an IP takeover mode. Both a logical IP address and a physical IP address are taking over at the time of logical IP address takeover function use. Only a physical IP address is taking over at the time of physical IP address takeover function use, without activating a logical IP address.

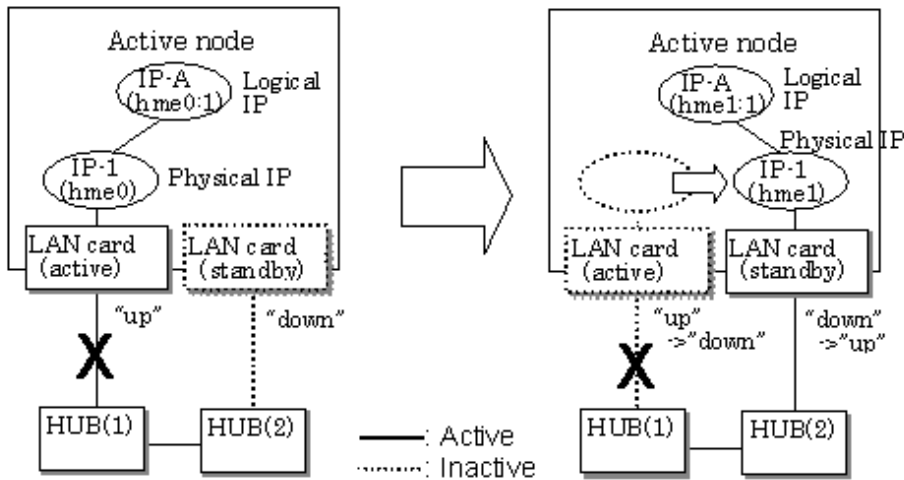
When using an IPv6 address, it is not possible to use a physical IP address takeover function.

[Figure 2.11 Outline of switching operation performed when a failure occurs in NIC switching mode](#) shows an example of node internal switching.

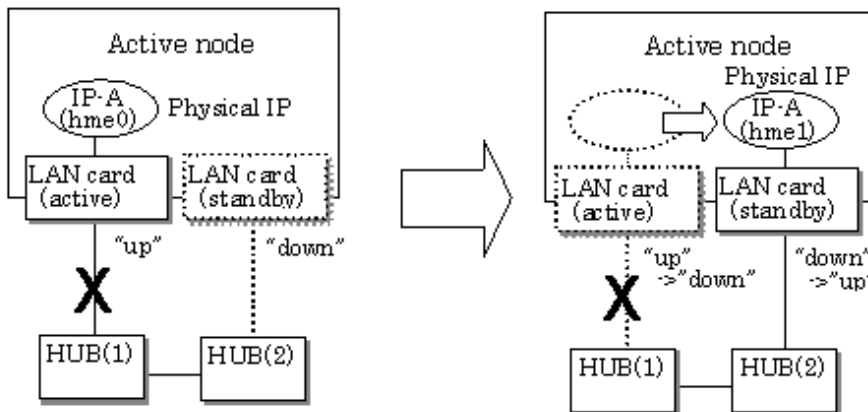
When a failure is detected, a console message is output to the syslog file (/var/adm/messages). If a failure occurs when HUB-to-HUB communication monitoring is enabled, a console message is output to the syslog file (/var/adm/messages).

Figure 2.11 Outline of switching operation performed when a failure occurs in NIC switching mode

- Logical IP address takeover function



- Physical IP address takeover function



Failback operation

If a relevant NIC recovers after NIC switching occurs due to failure detection, you must switch it back manually via `hanetnic change` command.

Running this command makes recovered NIC to operate as an active NIC and recovers the system. In addition, if you setup a Standby Patrol Function, it automatically fails back the defective NIC without manually executing `hanetnic change` command.

Furthermore, in the case where all the redundant NICs encounter failure, the line monitoring terminates. In such a case, you must restart the process via `hanetpoll off/on` command after recovering the network as required.



See

For details on the command, see the following:

- ["7.7 hanetpoll Command"](#)

2.1.2.3 Connectable remote host

Any system can be connected.

2.1.2.4 Available application

The requirement for user applications that can be operated in this mode is as follows:

- Application using the TCP or UDP.
- Applications must be operational on a system to which multiple NICs are connected and on which multiple IP addresses are defined. (This system is called a multi-home host.) For example, a socket application needs to operate with its local IP address fixed with the bind function or set to any value. (Remote party applications do not check the IP address.)

2.1.2.5 Notes

- If assigning IPv4 address to the virtual interface, IPv4 address must be assigned to all the redundant physical interfaces.
- If assigning IPv6 address to the virtual interface, IPv6 address must be assigned to all the redundant physical interfaces.
- If assigning both IPv4 and IPv6 to the virtual interface, these two forms of an IP address must be assigned to all the redundant physical interfaces.
- No multi-cast IP address can be used.
- Do not change the name of the virtual interface and the interface that is made redundant with the virtual interface. If names are changed, virtual interfaces are not properly activated and deactivated.

2.1.3 GS/SURE linkage mode

In this mode, each of multiple NICs (Network Interface Cards) is connected to a different network. Then, all the NICs are activated and used concurrently. Outgoing packets are assigned to the lines in units of TCP connections.

Thus, different lines are used for different connections for communication. If a failure occurs on one of the lines, communication can continue using another line, offering improved line reliability.

As with Fast switching mode, a virtual interface is created and then a virtual network is allocated to it. A TCP/IP application can carry out communication with the remote system, irrespective of the physical network redundant configuration, by using a virtual IP address set in this virtual interface as its own local system IP address.

Figure 2.12 Example of duplicated operation in GS/SURE linkage mode

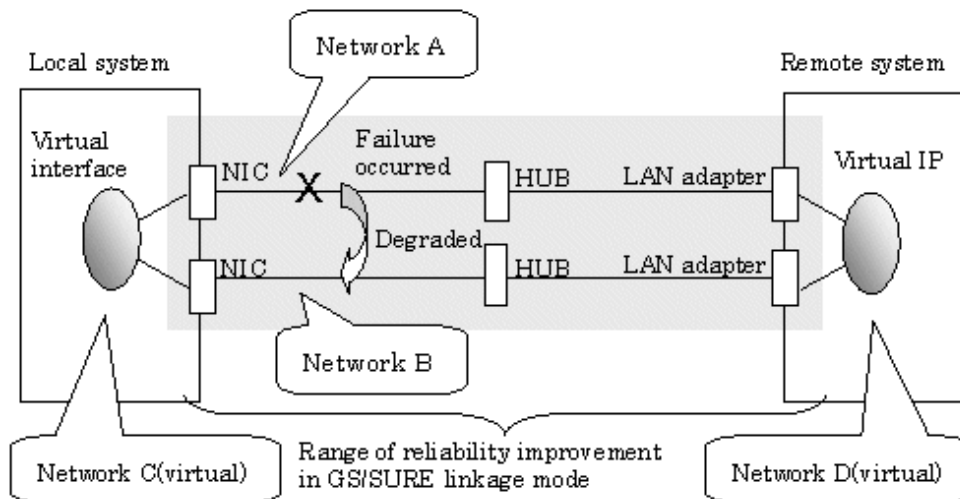
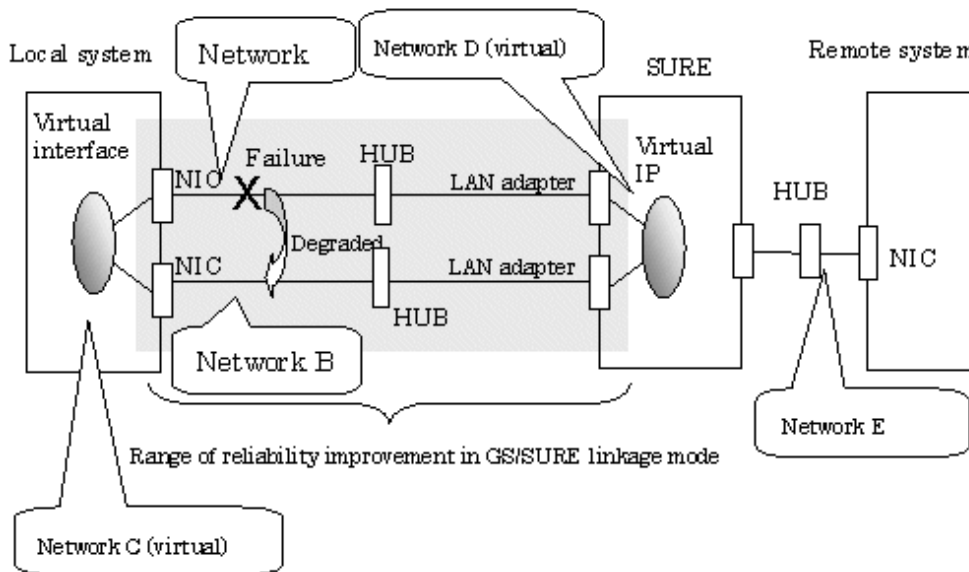


Figure 2.13 Example of duplicated operation in GS/SURE linkage mode (TCP relay function)



Connection type

If the GS/SURE linkage communication function is to be used, the systems among which communication is to be carried out must be connected on the same network. Connecting systems on different networks is not allowed.

If the TCP relay function is to be used, the local system and the remote system on a different network can communicate with each other via SURE.

Features

Lines are used in units of TCP connections for communication. If a failure occurs on a line, processing can continue on another line that is normal. Since all the redundant lines are activated for use, each of the lines can be directly used for a different purpose, enabling efficient use of resources.

Examples of recommended application

GS/SURE linkage mode is appropriate, for example, for communication in a multi-server environment where GS/SURE and GP are mixed or for IP-based reconstruction of network infrastructures of a legacy system.

System configuration

Figure 2.14 System configuration in GS/SURE linkage mode and Figure 2.15 System configuration in GS/SURE linkage mode (TCP relay function) show a system configuration of GS/SURE linkage mode (GS/SURE communication function) and of GS/SURE linkage mode (TCP relay function), respectively.

Figure 2.14 System configuration in GS/SURE linkage mode

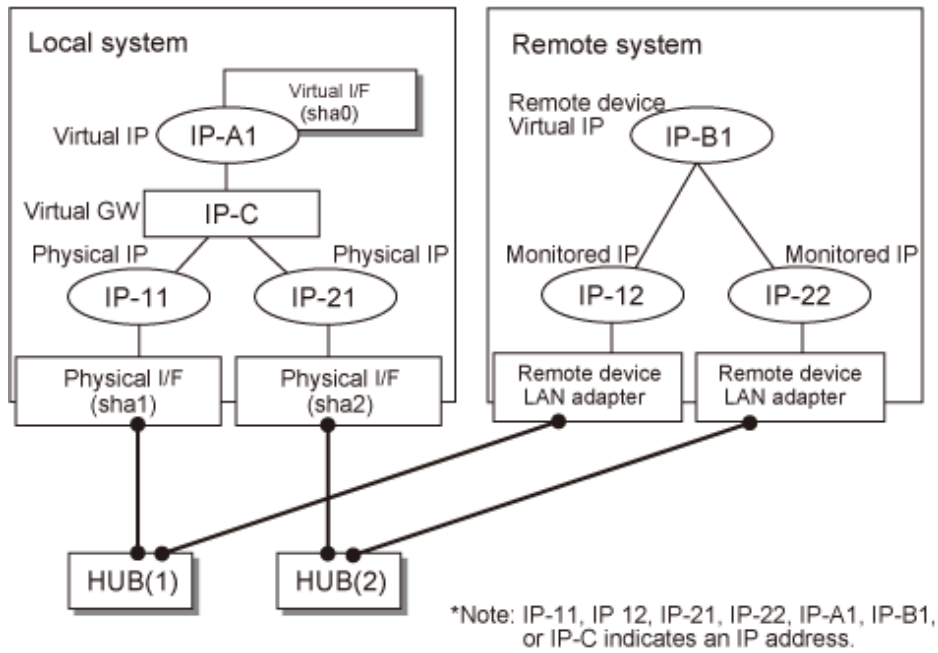
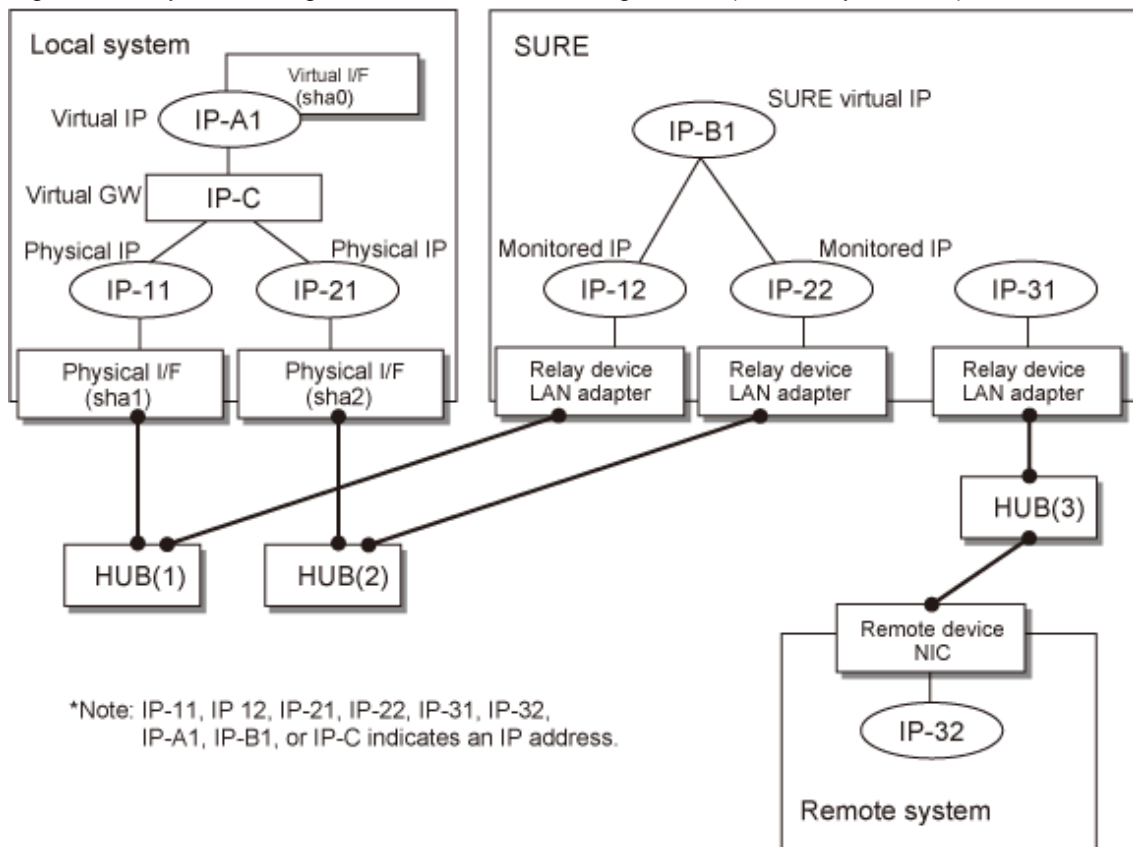


Figure 2.15 System configuration in GS/SURE linkage mode (TCP relay function)



The following explains each component and its meaning:

Physical interface

Indicates a physical interface (such as sha1 and sha2) of the duplicated NIC.

Physical IP

Indicates an IP address to be attached to a physical interface. This IP address is always active. Use the IP address to manage a node by using the cluster operation management view, etc. IPv4 address can be used for a physical interface.

Virtual interface

Indicates a virtual interface (such as sha0) used to handle duplicated NICs as one NIC.

Virtual IP

Indicates a local IP address to be attached to a virtual interface for communication with remote devices. This IP address is activated on the active node. In cluster operation, the IP address is taken over by the standby node when clusters are switched. IPv4 address can be used for a physical interface.

Virtual GW (Virtual Gateway)

Indicates a virtual gateway to be used for GS/SURE linkage mode. By setting the virtual gateway, the virtual IP will be automatically selected as the local IP address which is used during communication.

Relay device LAN adapter and remote device NIC

Indicates a NIC of the relay and remote devices.

Monitored IP

Indicates an IP set to the NIC of the remote device. This IP address is monitored. IPv4 address can be used for a physical interface.

Remote device virtual IP

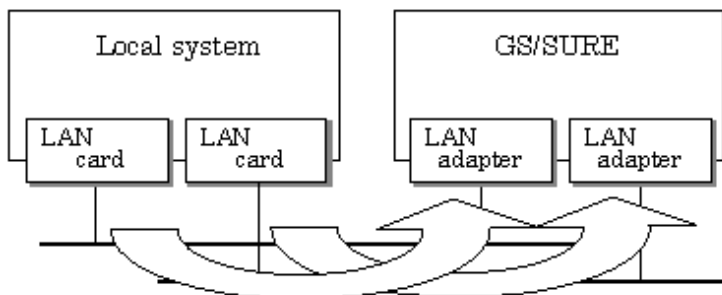
Indicates a virtual IP of the remote device with which communication should be carried out. IPv4 address can be used for a physical interface.

2.1.3.1 Fault monitoring function

Fault monitoring

The ping command is issued periodically to the LAN adapter of the remote system and its response is monitored. If no response is received within a specified period of time, the line is considered to be faulty. Also, if a fault notification (with a special packet) of a line is received from the remote system, the line is considered to be faulty.

Figure 2.16 Monitoring method in GS/SURE linkage mode



The ping command is issued to the real interface of the remote system to monitor the communication status.

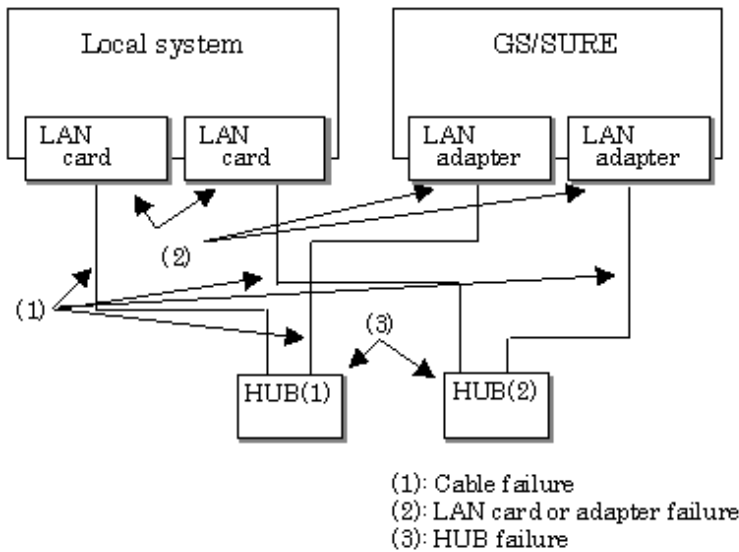
Switching time

The switching time of a line is indicated by "monitoring interval (sec)" multiplied by "monitoring count (count)." The monitoring interval can be set in the range of 1 to 300 seconds and the monitoring count can be set in the range of 1 to 300 times. By default, they are 5 seconds and 5 times, respectively.

Detectable failures

The following failures can be detected:

Figure 2.17 Detectable failures in GS/SURE linkage mode



Fault monitoring start/stop

Monitoring is started automatically when the virtual interface is activated. Monitoring is automatically stopped when the virtual interface is inactivated.

2.1.3.2 Switching function

Switching operation

A line whose failure is detected is automatically avoided, and only lines operating normally are used to continue communication.

Failback operation

If a faulty path of a physical interface is recovered, the line of the physical interface is automatically restored for normal communication. The failback of a line cannot be performed manually.

2.1.3.3 Connectable remote host

An associated host is able to communicate with the following systems:

When using a GS/SURE communication function:

- GS (Global Server)
- SURE SYSTEM
- ExINCA

When using a TCP relay function:

An optional system (Though a relay device is SURE SYSTEM only).

2.1.3.4 Available applications

The requirement for user applications that can be operated in this mode is as follows:

- Application using TCP/IP.

2.1.3.5 Notes

- When using a physical interface, it is necessary to assign the IPv4 address.

- If you omit virtual gateway settings in GS/SURE linkage mode, you need to enable dynamic routing. For details, see "[3.2.2.4 System setup in GS/SURE linkage mode](#)".
- This mode cannot be applied for communication between Solaris servers, and between Solaris servers and Linux servers.
- Do not change the name of the virtual interface and the interface that is made redundant with the virtual interface. If names are changed, virtual interfaces are not properly activated and deactivated.

2.2 Option Functions

[Table 2.1 Available option functions in each mode](#) shows the option functions that can be used in each mode.

Table 2.1 Available option functions in each mode

| Function | Mode | | |
|--|---------------------|--------------------|----------------------|
| | Fast switching mode | NIC switching mode | GS/SURE linkage mode |
| Multiple virtual interface definition | A | A | A |
| Cluster failover because of a line failure | A | A | A |
| Sharing function of physical interface | A | A | N |
| Multiple logical virtual interface definition | A | - | N |
| Single physical interface definition | A | A | A |
| HUB monitoring | N | A | N |
| Communication target monitoring | - | N | A |
| Standby patrol | - | A | - |
| Automatic failback | - | A | - |
| Dynamic adding/deleting/switching of interfaces used | A | A | A |
| User command execution | N | A | A |

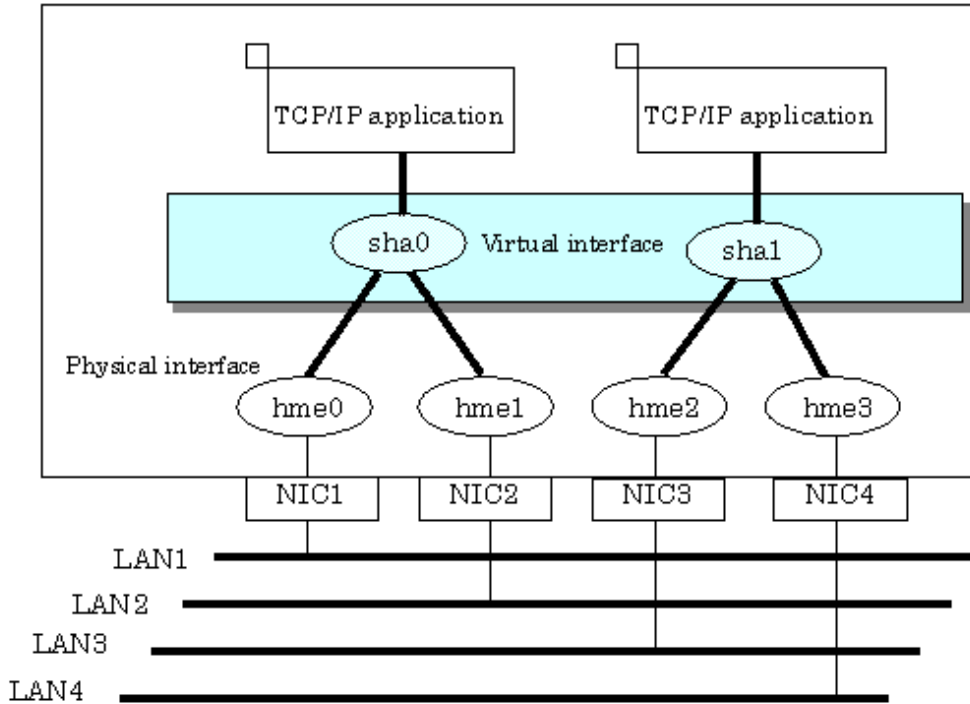
[Meaning of the symbols] A: Supported, N: Not supported, -: Support is not required

2.2.1 Configuring multiple virtual interfaces

Multiple virtual interfaces can be defined in a single system. With this capability, redundancy in the entire transfer route is available for the system such as an application gateway, which requires multiple networks. As a result, applying multiple virtual interfaces provide high network reliability.

[Figure 2.18 Two virtual interfaces being defined](#) below shows the concept of defining two virtual interfaces.

Figure 2.18 Two virtual interfaces being defined



2.2.2 Cluster fail-over when entire transfer routes fails

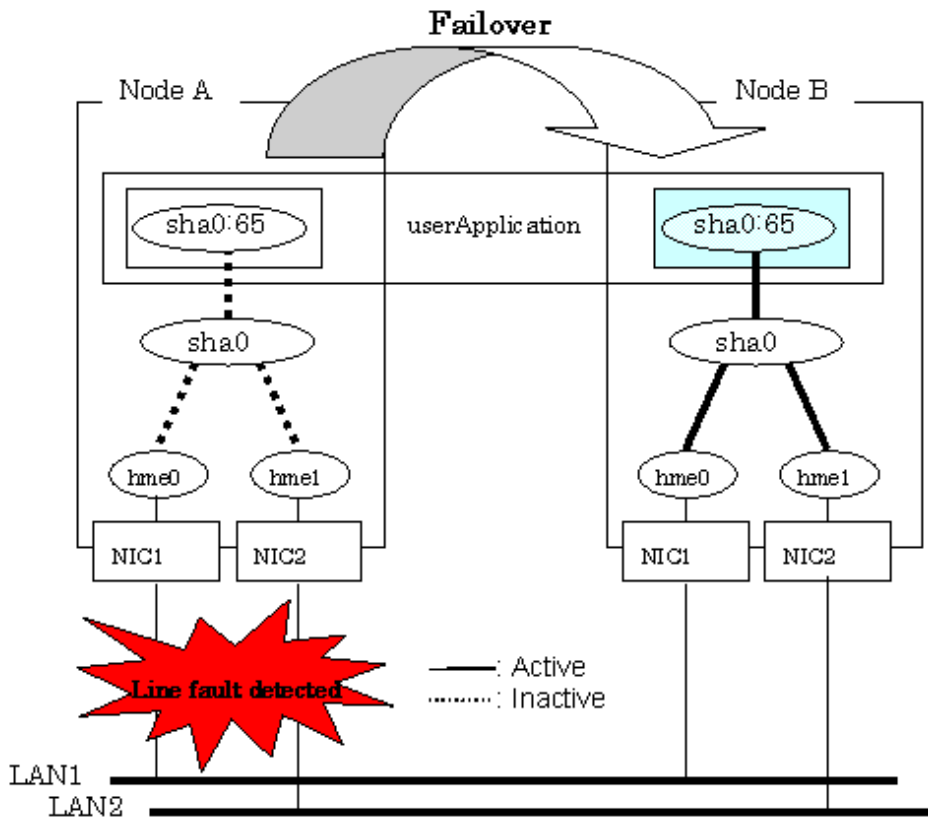
While operating a cluster, if every single transfer routes fail for a particular virtual interface, a cluster can switch over to the other cluster. With this capability, the system can be recovered, without administrator's interference, by performing switchover within the cluster when detecting failures in the entire transfer route. Cluster fail-over is enabled in the initial setup for duplex transfer route operation in Fast switching mode, NIC switching mode and GS/SURE linkage mode. This function is automatically configured when the cluster definition is defined.

[Figure 2.19 Cluster failover due to line fault](#) shows example of fail-over to node B when communication is disabled via both hme0 and hme1 bundled with virtual interface sha0 on node A.

Information

The following is an example of Fast switching mode and this applies to NIC switching mode as well.

Figure 2.19 Cluster failover due to line fault



2.2.3 Sharing physical interface

If multiple virtual interfaces are created, these interfaces can share one or all physical interfaces. This is called "sharing physical interface".

Using this capability, it is possible to:

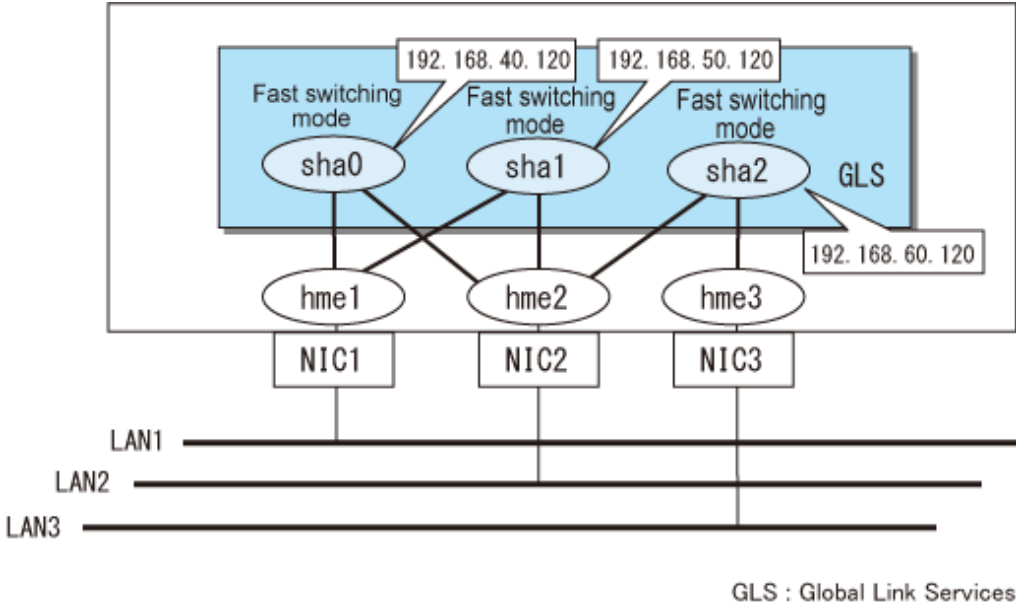
- Decrease the number of NICs used for the redundancy operation, and make effective use of limited resource in Fast switching mode.
- Configuring multiple IP addresses on a single NIC in NIC switching mode and use different IP address for each application.

2.2.3.1 Using Fast switching mode

In the virtual interface, which institutes Fast switching mode, one portion or entire physical interfaces can be shared. Though, sharing is not possible for the physical interface and virtual interface of NIC switching mode and GS/SURE linkage mode.

Figure 2.20 Example of sharing physical interface (1) shows an example of three virtual interfaces in Fast switching mode, sha0, sha1, and sha2 sharing three physical interfaces hme1, hme2, and hme3.

Figure 2.20 Example of sharing physical interface (1)



2.2.3.2 Using NIC switching mode

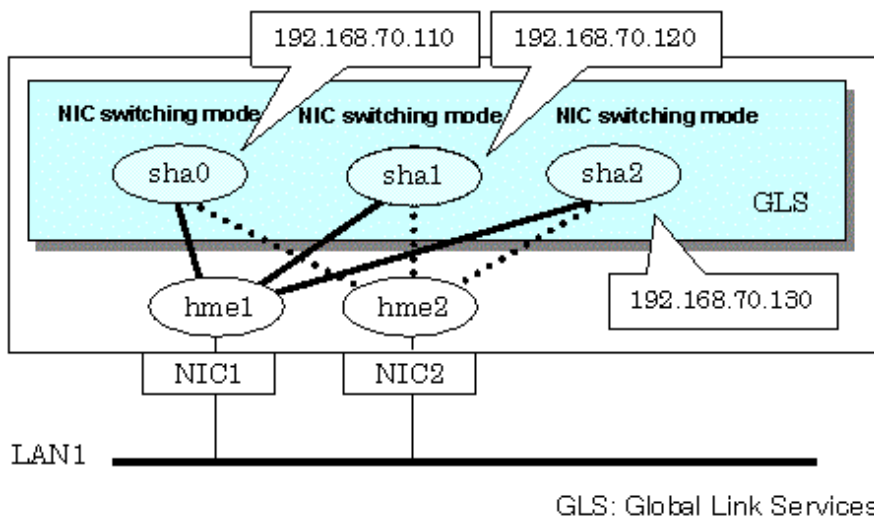
Within several virtual interfaces of NIC switching mode (logical IP takeover), if all the names of the physical interfaces and the values of the physical IP addresses are equivalent, then it is possible to share the physical interface. Sharing a portion of physical interface is not allowed. Nevertheless, sharing is not possible for NIC switching mode (physical IP takeover). In addition, sharing physical interface with the virtual interface is not possible for Fast switching mode and GS/SURE linkage mode.

Figure 2.21 Example of sharing physical interface (2) shows an example of three virtual interfaces sha0, sha1 and sha2 (all in NIC switching mode) sharing two physical interfaces hme1, and hme2.

Note

Assign the same network address to the virtual interfaces that share the physical interface.

Figure 2.21 Example of sharing physical interface (2)



2.2.3.3 Using GS/SURE linkage mode

Cannot share physical interface.

2.2.3.4 Notices

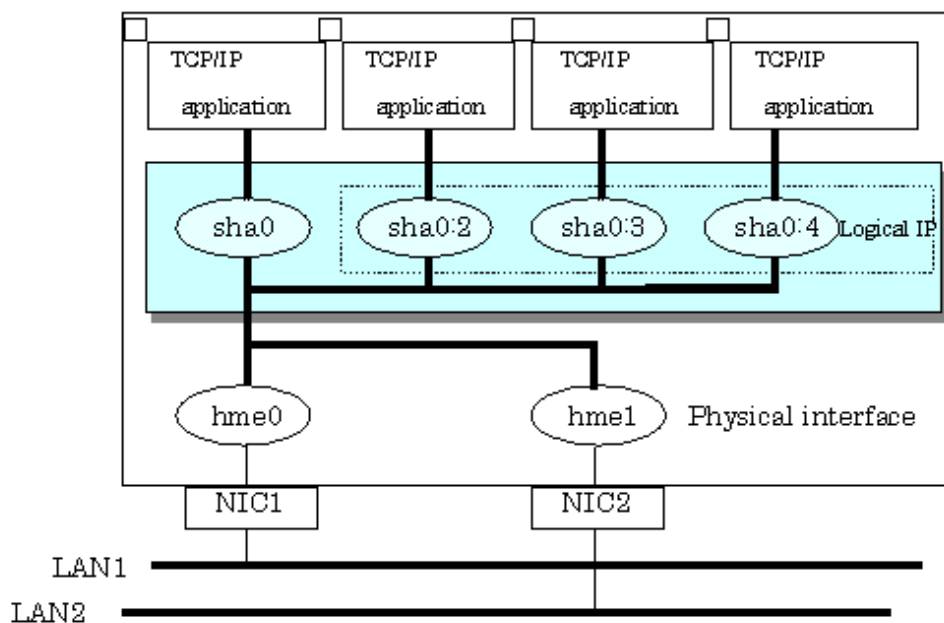
In Fast switching mode, NIC sharing is not possible within the virtual interface that can have IPv6 address. NIC sharing is possible between the virtual interfaces, which can have IPv4 address, or virtual interfaces, which can have IPv6 address and the virtual interfaces, which can have IPv4 address.

2.2.4 Configuring multiple logical virtual interfaces

It is possible to define several IP addresses (logical virtual interfaces) on a single virtual interface. Using this function, various IP addresses can be used for each application.

Figure 2.22 Logical virtual interfaces being defined shows an example of defining three IP addresses (logical virtual interface) on a single virtual interface sha0.

Figure 2.22 Logical virtual interfaces being defined



In the above figure, sha0:2 to sha0:4 are called logical virtual interfaces in this document. For each logical virtual interface, please assign the address in the same subnet as the virtual interface where the logical virtual interface belongs. For operation on a cluster system, please assign the address in the same subnet as the takeover address.

Note

- This function is only available for Fast switching mode. The other mode such as GS/SURE linkage mode does not apply.
- For NIC switching mode, if using physical interface sharing function, it can process (a process of allocating multiple IP addresses to one physical interface) equally as this function.

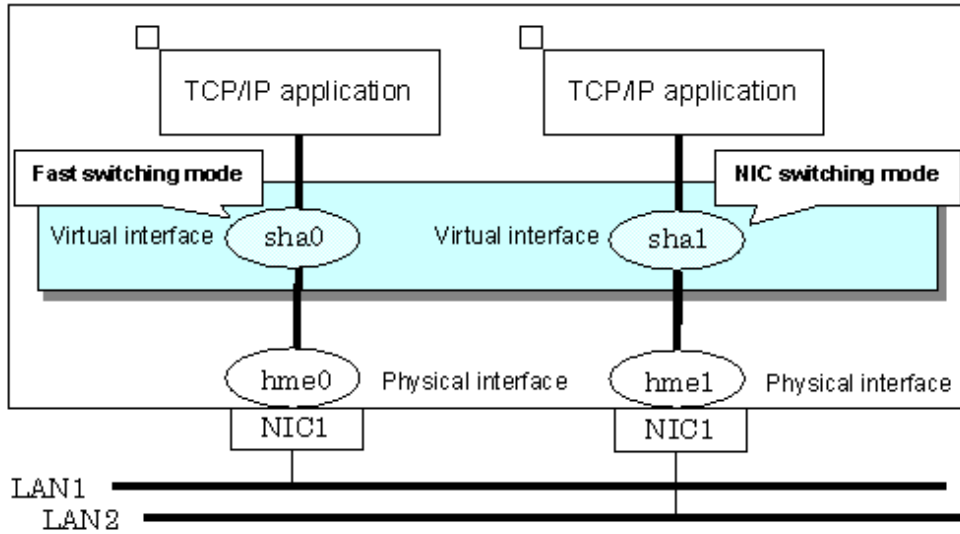
2.2.5 Configuring single physical interface

You can create a virtual interface, which has a single physical interface. This function enables failover because of a line failure even on a cluster system that has only one physical interface available for use.

You can also switch clusters of the virtual NIC mode by creating a virtual interface of NIC switching mode bundling virtual NIC of virtual NIC mode.

Figure 2.23 Single physical interface configuration shows an example of single physical interface configuration.

Figure 2.23 Single physical interface configuration



2.2.6 HUB monitoring function

The HUB monitoring function issues the ping command to adjacent HUB at regular intervals and switches the interface to be used when a line failure is detected or a hang-up of the ping command is detected. Up to two HUBs can be registered per virtual interface. This function is available exclusively for NIC switching mode.

Point

HUB monitoring function for NIC switching mode supports both configuration of the monitoring target for each virtual interface and start/stop of router monitoring.

This function can also monitor a transfer path between two HUBs (this is called HUB-to-HUB monitoring function). HUB-to-HUB monitoring function, detects a failure between two HUBs. This function can thus prevent a communication error from occurring due to NIC switching when a HUB-to-HUB failure occurs.

Note

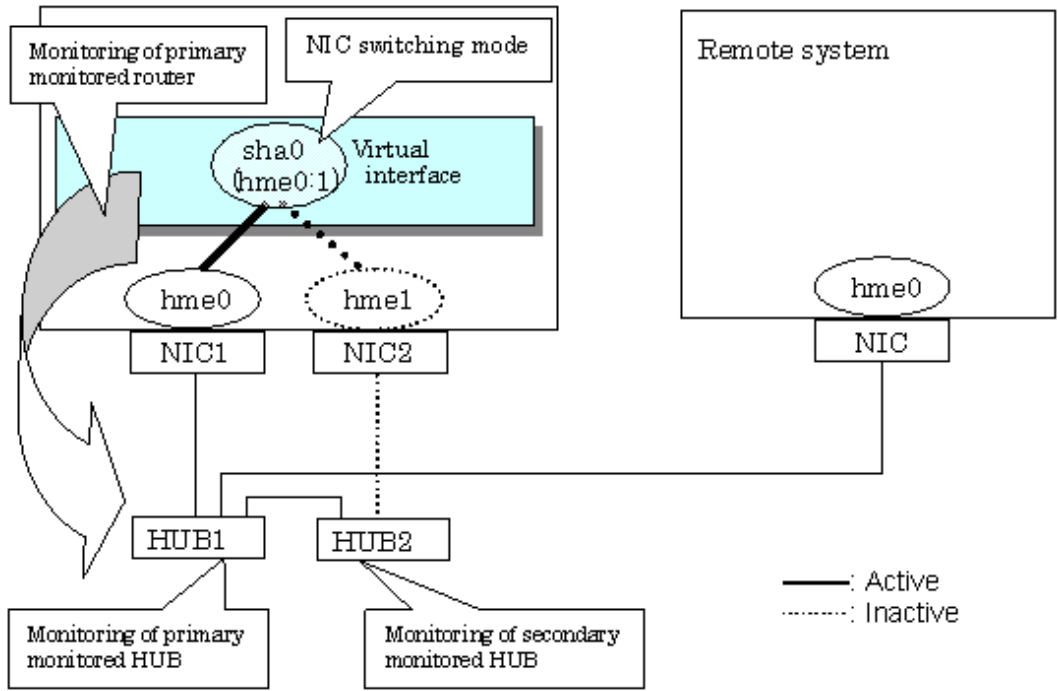
If no response after the ping command run for 30 seconds, the hang-up will be detected.

Information

If the standby patrol function is used, the HUB-to-HUB monitoring is not required because the standby patrol function is contained in HUB-to-HUB monitoring function. (See "2.2.8 Standby patrol function.")

Figure 2.24 HUB monitoring function shows an outline of the HUB monitoring function

Figure 2.24 HUB monitoring function



Point

If a hub cannot have an IP address, IP address of a host or a router that is connected to the hub can be monitored. However, if the monitored host or router stops, polling the host or router fails and a NIC switching event might occur. In order to prevent an unnecessary switching process, it is recommended to set up two monitoring targets, as well as enabling HUB-to-HUB monitoring function in case one of the monitoring targets stops.

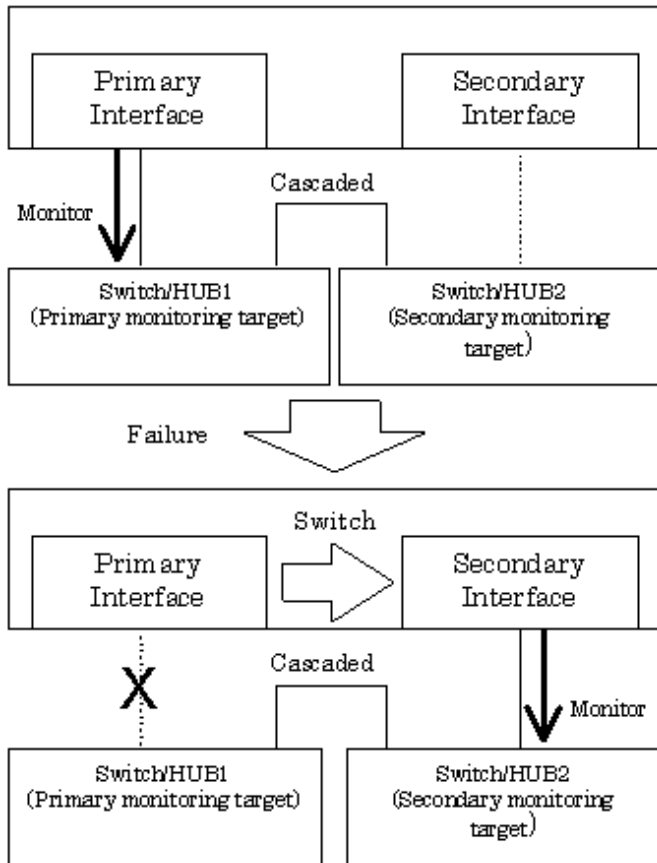
Note

- Refer to "7.7 hanetpoll Command" for configuration of HUB-to-HUB monitoring feature.
- When using a single HUB, you can have only one configuration for a remote end, however, all the multiplexing transfer paths become unavailable if the HUB breaks. Therefore, it is not recommended to operate with a single HUB.

2.2.6.1 Not using HUB-to-HUB monitoring feature

If the operation starts without HUB-to-HUB monitoring function, the primary HUB (HUB1 in the [Figure 2.25 HUB-to-HUB monitoring disabled](#)) is monitored using the ping command. When a failure is detected in the primary HUB, the NIC of the currently active system is inactivated and then the standby NIC is activated. After the standby NIC is activated, the secondary HUB (HUB2 in the [Figure 2.25 HUB-to-HUB monitoring disabled](#)) is monitored using the ping command.

Figure 2.25 HUB-to-HUB monitoring disabled



2.2.6.2 Using HUB-to-HUB monitoring feature

If the operation starts using the HUB-to-HUB monitoring function, the secondary HUB (HUB2 in the [Figure 2.26 HUB-to-HUB monitoring enabled \(failure on the secondary monitoring\)](#)) is monitored using the ping command.

When a failure is detected on the secondary hub, HUB-to-HUB monitoring function starts polling the primary hub, as well as polling the secondary hub (Switch/HUB1 in [Figure 2.26 HUB-to-HUB monitoring enabled \(failure on the secondary monitoring\)](#)).

(During this occasion, a monitoring failure message (No.872) regarding the secondary HUB will be output. Use this message to investigate the cause of the failure.)

Once the polling process on the primary HUB starts, this function then monitors both secondary and primary HUBs interchangeably. Monitoring process against the secondary HUB is recovery monitoring and it will stop monitoring the primary HUB when HUB-to-HUB monitoring function detects recovery of the secondary HUB. HUB-to-HUB monitoring function determines transfer path failure by checking the number of monitoring failures (the default is 5 times). If failures were detected repeatedly on both primary and secondary HUBs, then it determines there was transfer path failure. Note that a message (No.872) will be reported regarding the failure on the secondary HUB, therefore it is possible to recover the secondary HUB before the primary HUB switches to secondary HUB.

When a failure is detected on the primary HUB after switching to the secondary interface due to a transfer route error, a message (No.873) will be reported.

Figure 2.26 HUB-to-HUB monitoring enabled (failure on the secondary monitoring)

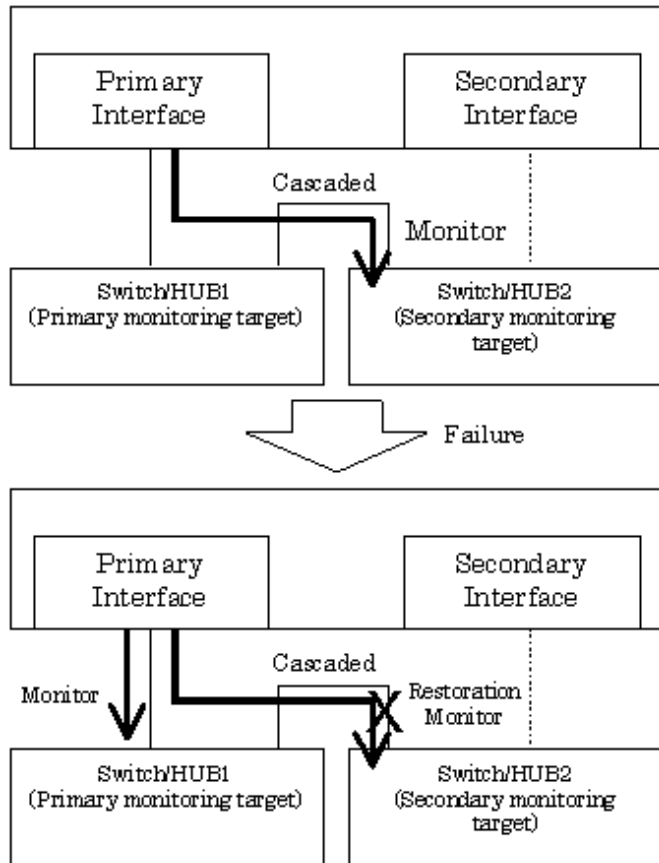
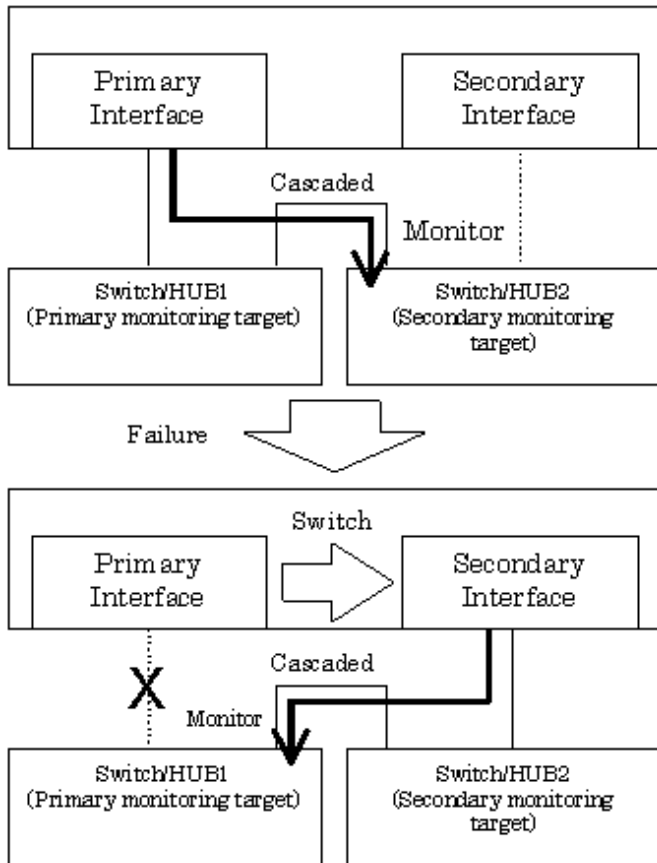


Figure 2.27 HUB-to-HUB monitoring enabled (failure on the primary monitoring)

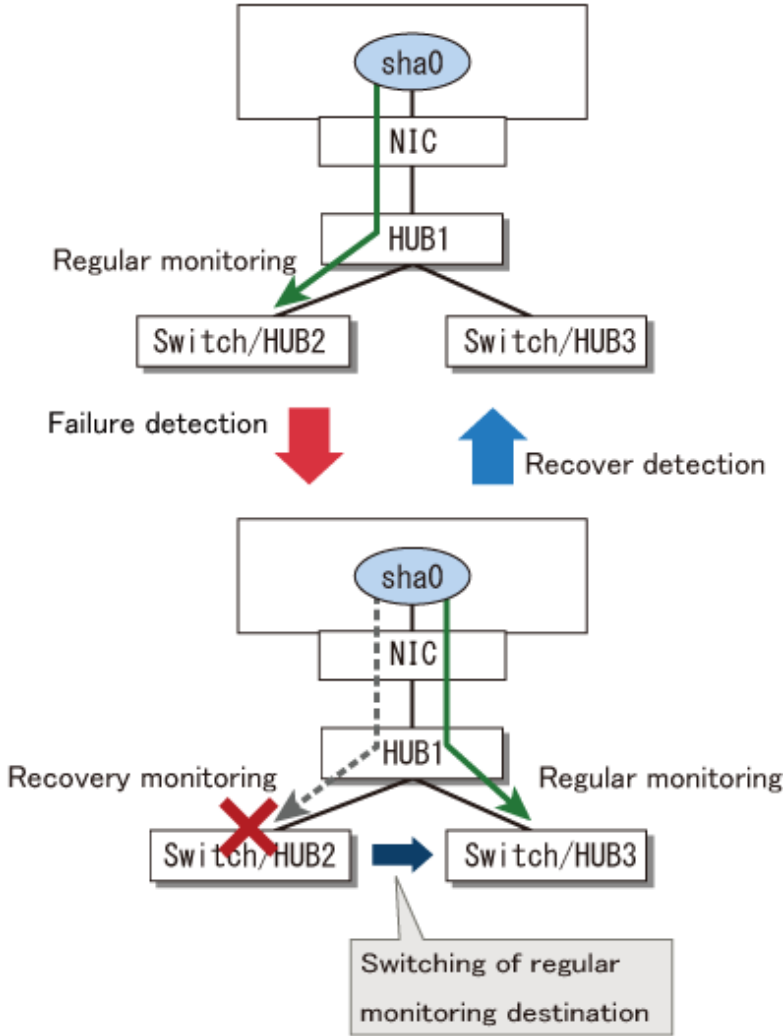


2.2.6.3 Multiple HUB monitoring of single physical interface

After the startup of transfer route monitoring of HUB monitoring function, the primary HUB (Switch/HUB2 in [Figure 2.28 Multiple monitoring of single physical interface](#)) is regularly monitored. When failure is detected in the primary HUB with the regular monitoring, regular monitoring of the primary HUB is stopped, and regular monitoring of the secondary HUB (Switch/HUB3 in [Figure 2.28 Multiple monitoring of single physical interface](#)) is started.

Also, recovery monitoring is started to the primary HUB at the same time. When failure is detected in the secondary HUB also with the regular monitoring, transfer route failure is determined. If transfer route failure is determined, HUB monitoring is stopped and switching of cluster application is performed. When recovery of primary HUB is detected (ping of recovery monitoring has succeeded) without detecting the failure from the secondary HUB, recovery monitoring to the primary HUB and regular monitoring to the secondary HUB are stopped. And then, regular monitoring to the primary HUB is restarted.

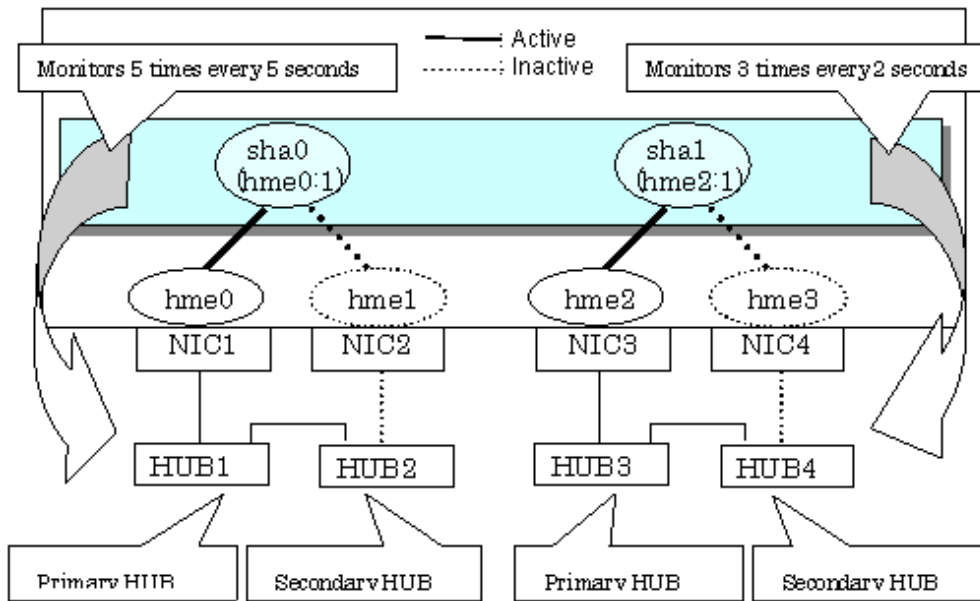
Figure 2.28 Multiple monitoring of single physical interface



2.2.6.4 Transfer path monitoring on individual virtual interface

On HUB monitoring function over NIC switching mode, it is possible for each virtual interface to set up start/stop of the transfer path monitoring, monitoring count, monitoring interval, and cluster failover in the case of network error. The setting in the following figure can be configured.

Figure 2.29 Monitoring on individual virtual interface



When changing monitoring interval and monitoring count

1. Set parameters by using the "hanetpoll on" command after setting the ping monitoring destination. Note that the value of Common monitoring information (Standard Polling Parameter) is set for any parameter options that are not set. In the following example, the monitoring interval (-s) and monitoring count (-c) are specified for sha1.

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -n sha1 -s 2 -c 3
```

2. Check individual parameters.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
[ Standard Polling Parameter ]
    interval(idle)    =    5( 60) sec
    times              =    5 times
    max_retry          =    5 retry
    repair_time        =    5 sec
    link detection     =    NO
    failover mode      =    YES

[ Polling Parameter of each interface ]
Name      Hostname/Polling Parameter
-----+-----+
sha0      192.13.80.251,192.13.80.252
          hub-hub poll      =    OFF
          interval(idle)    =    5( 60) sec
          times              =    5 times
          max_retry          =    5 retry
          repair_time        =    5 sec
          link detection     =    NO
          failover mode      =    YES

Name      Hostname/Polling Parameter
-----+-----+
sha1      192.13.81.251,192.13.81.252
          hub-hub poll      =    OFF
          interval(idle)    =    2( 60) sec
          times              =    3 times
          max_retry          =    5 retry
          repair_time        =    5 sec
```

```
link detection = NO
failover mode = YES
```

When restricting the failover in the case of HUB monitoring failure

1. Set parameters by using the "hanetpoll on" command after setting the ping monitoring destination. Note that the value of Common monitoring information (Standard Polling Parameter) is set for any parameter options that are not set. In the following example, the monitoring interval (-s), monitoring count (-c), and others are not specified, so Standard Polling Parameter will be set.

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -n sha0 -f no
```

2. Check individual parameters.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
[ Standard Polling Parameter ]
    interval(idle) = 5( 60) sec
    times          = 5 times
    max_retry      = 5 retry
    repair_time    = 5 sec
    link detection = NO
    failover mode  = YES

[ Polling Parameter of each interface ]
Name  Hostname/Polling Parameter
+-----+-----+
sha0  192.13.80.251,192.13.80.252
      hub-hub poll = OFF
      interval(idle) = 5( 60) sec
      times          = 5 times
      max_retry      = 5 retry
      repair_time    = 5 sec
      link detection = NO
      failover mode  = NO

Name  Hostname/Polling Parameter
+-----+-----+
sha1  192.13.81.251,192.13.81.252
      hub-hub poll = OFF
      interval(idle) = 2( 60) sec
      times          = 3 times
      max_retry      = 5 retry
      repair_time    = 5 sec
      link detection = NO
      failover mode  = YES
```

When restoring the parameters of the virtual interfaces individually set

1. Execute the "hanetpoll on" command to restore the parameters of the virtual interfaces individually set. In the following example, parameters set to the virtual interface sha0 are restored.

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -n sha0 -d
```

2. Check that individual parameters are deleted.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
[ Standard Polling Parameter ]
    interval(idle) = 5( 60) sec
    times          = 5 times
    max_retry      = 5 retry
    repair_time    = 5 sec
```

```

link detection      = NO
failover mode      = YES

[ Polling Parameter of each interface ]
Name  Hostname/Polling Parameter
-----+-----
sha0  192.13.80.251,192.13.80.252
      hub-hub poll      = OFF
      interval(idle)    = 5( 60) sec
      times              = 5 times
      max_retry          = 5 retry
      repair_time        = 5 sec
      link detection     = NO
      failover mode      = YES

Name  Hostname/Polling Parameter
-----+-----
shal  192.13.81.251,192.13.81.252
      hub-hub poll      = OFF
      interval(idle)    = 2( 60) sec
      times              = 3 times
      max_retry          = 5 retry
      repair_time        = 5 sec
      link detection     = NO
      failover mode      = YES

```



- For details on configuring monitoring target for each virtual interface, refer to "7.7 hanetpoll Command".
- When sharing NIC, you can set only the parameters of failovers for each virtual interface. Other parameters use values of the virtual interface initially defined.

2.2.7 Monitoring communicating host

In GS/SURE linkage mode, the ping command is issued against the IP address of the actual interface of the remote system at regular interval. In any one of the following cases, the route is switched and a reporting message will be output:

- A transfer path failure is detected.
- A hang-up of the ping command is detected.
- A failure notification is received from the remote system.

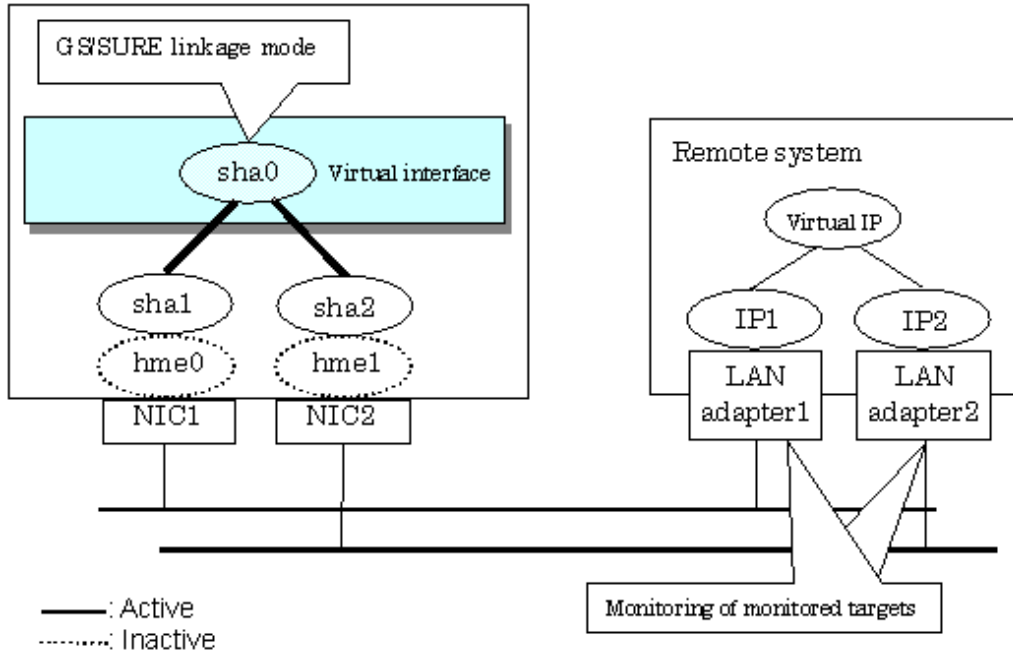
Then, communication is continued using other transfer path.

This function is used exclusively for GS/SURE linkage mode. In Fast switching mode, when the virtual interface activates, the process will be executed automatically. NIC switching mode is not capable of using this function.



If no response after the ping command run for 30 seconds, the hang-up will be detected.

Figure 2.30 Remote system monitoring function



2.2.8 Standby patrol function

A standby patrol function monitors the condition of the deactivated actual interface of a standby system in NIC switching mode.

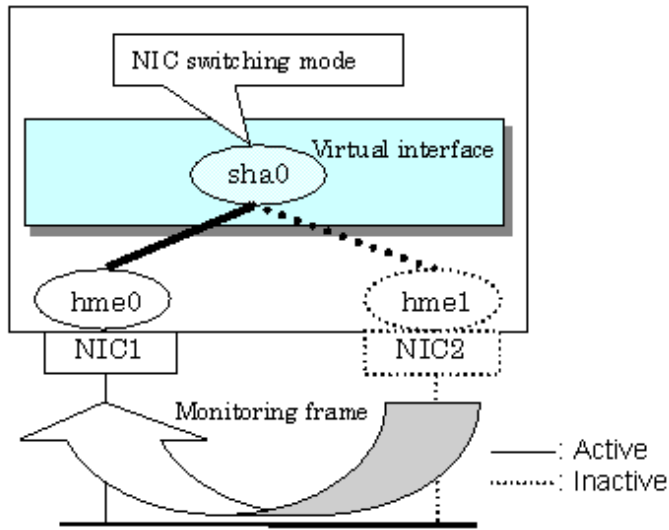
This brings the following effects:

- A message will be reported to the administrator when a failure occurs in standby interface. Therefore, the error of the standby interface can be detected before switching of the active interface.
- It is possible to fail-back automatically, when the standby interface recovers after switching to previous operation. (Automatic fail-back feature.)
- When the transfer path monitoring stops due to a failure in every one of the transfer paths, standby patrol feature allows to recover transfer path monitoring automatically.

Standby patrol starts when activated a system and when processed activation of the corresponding NIC switching mode, and stops automatically when a system stopped or when processed deactivation of the corresponding NIC switching mode. It is possible to operate manually. See "7.10 strptl Command" for starting standby patrol manually and "7.11 stppl Command" for stopping standby patrol.

See "2.2.9 Automatic fail-back function" for an automatic fail-back function.

Figure 2.31 Standby patrol function



Note

This feature is available exclusively for NIC switching mode. Modes such as Fast switching mode and GS/SURE linkage mode do not have standby interface. Thus, this feature does not apply to these modes.

2.2.9 Automatic fail-back function

In NIC switching mode, you can define the following by the standby patrol function.

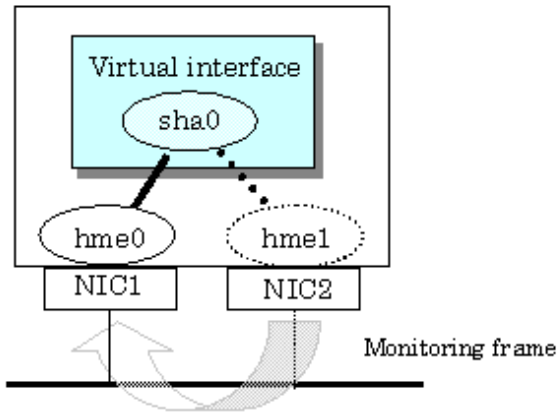
- "automatically perform fail-back immediately after recovering the faulted transfer path"
- "perform fail-back when the transfer path currently used encounters a failure"

For information on the setup, [Figure 2.32 Automatic fail-back function \(continued\)](#) and [Figure 2.33 Automatic failback function \(end\)](#) show the outline of the automatic fail-back function.

Figure 2.32 Automatic fail-back function (continued)

Initial status

—: Active
.....: Inactive



After a fault occurs

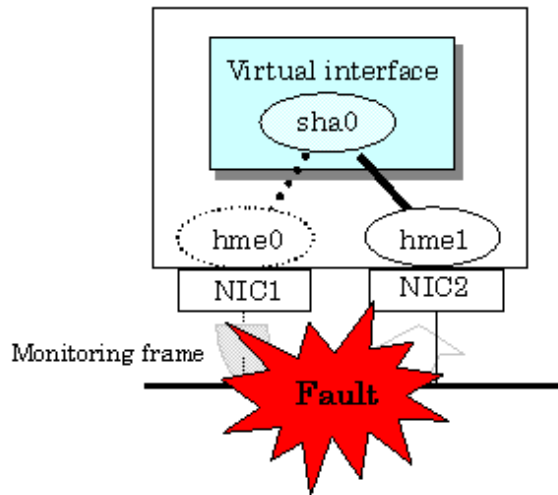
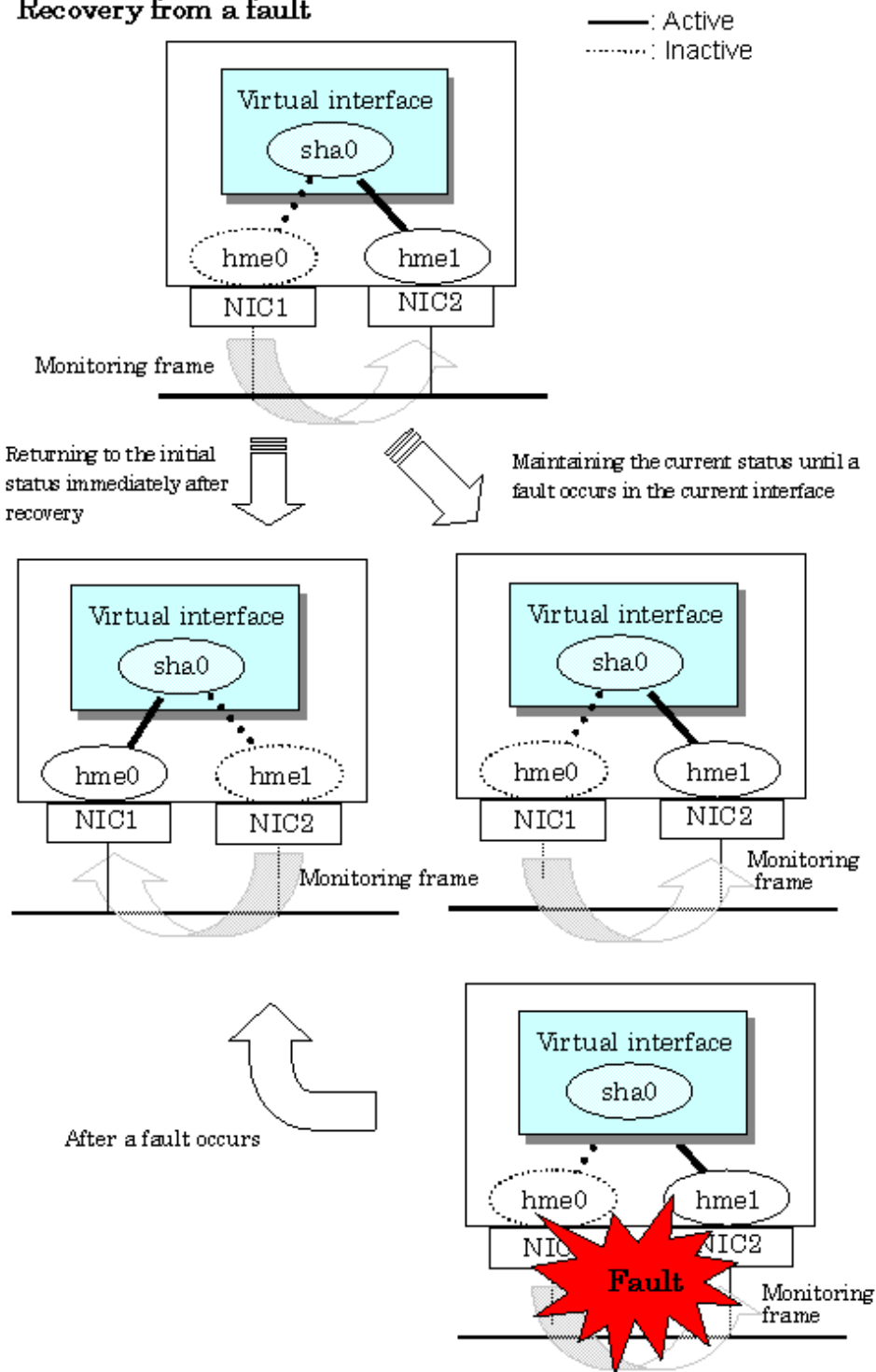


Figure 2.33 Automatic failback function (end)

Recovery from a fault



When specified other than HUB as a monitoring target device, occasionally automatic failback is not promptly executed after recovered the primary interface, depending on where an error occurred in a transfer route. Therefore, specify HUB as a monitoring target device to execute prompt failback.

Note

After the failed interface is recovered, if a running interface fails before the Standby patrol detects the No.885 message indicating interface recovery, NIC switchback will not be executed. If this occurs, the Standby patrol will consider that both of the NICs are disabled until it

detects the failed interface recovery. Recover the interface referring to "4.6.2 Recovery procedure from line failure in NIC switching mode".

2.2.10 Dynamically adding/deleting/switching physical interface

In Fast switching mode and GS/SURE linkage mode (the operation mode is "c"), it is possible to add/delete bundled physical interfaces with a virtual interface kept activated (dynamic). The hanetnic command adds/deletes dynamically. See "7.9 hanetnic Command" for the detail. Figure 2.34 Dynamic adding/deleting function of physical interfaces used shows the outline of actions when executed a command to add/delete the physical interface dynamically.

Dynamic addition/deletion commands of physical interfaces have two modes below.

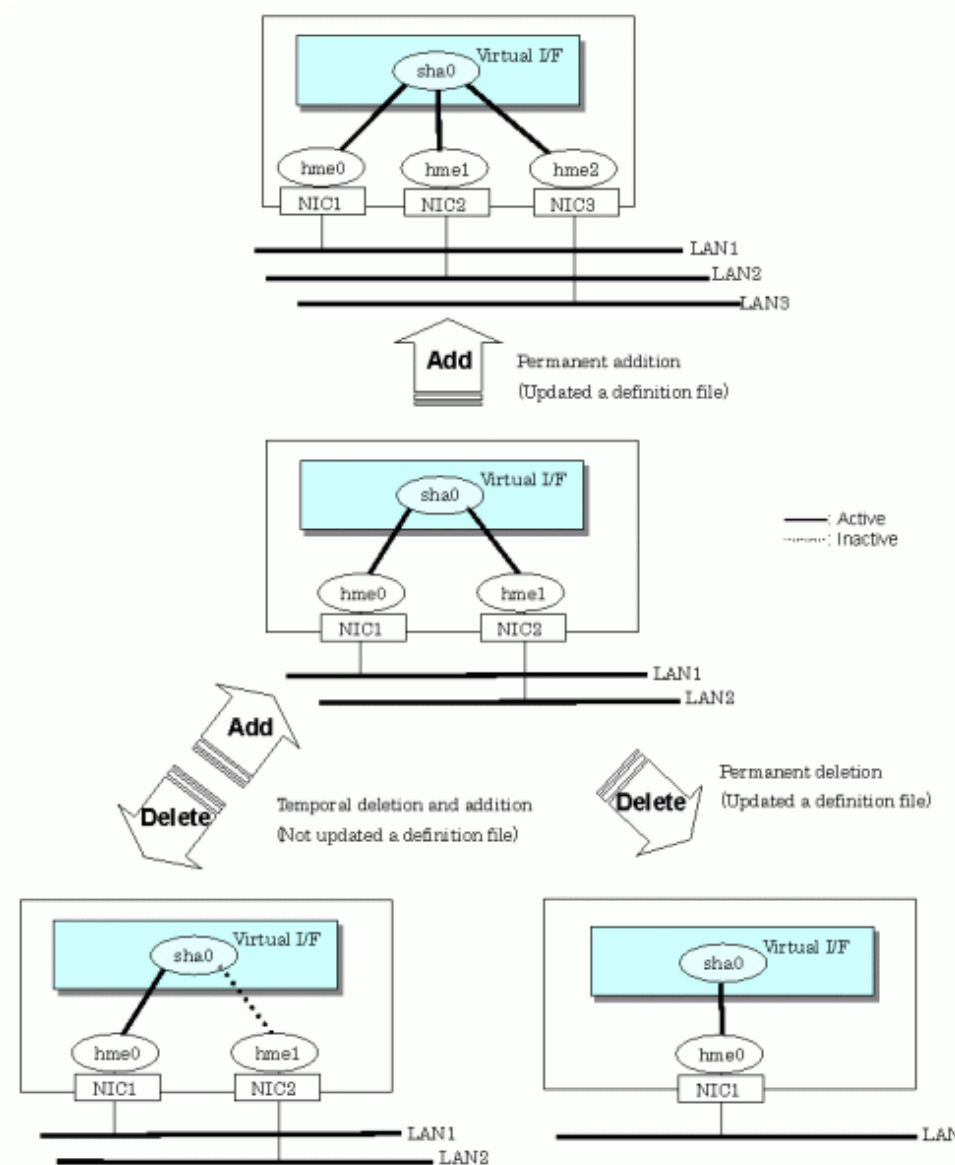
Temporal dynamic addition/deletion:

Operates physical interfaces to bundle without editing a configuration information file. Therefore, it automatically returns to the original state by operating a machine to reboot, etc. It is not possible to add other than the physical interface that was deleted by this mode when adding dynamically.

Permanent dynamic addition/deletion:

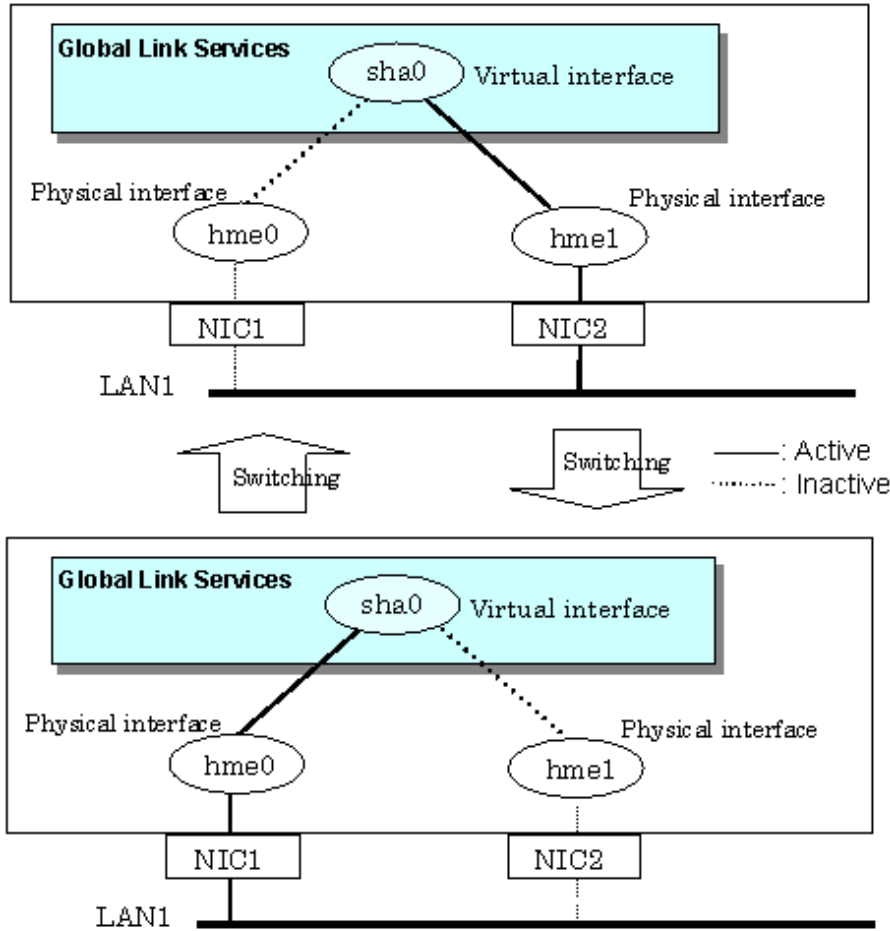
Edits a configuration information file. Therefore, changes are reflected even after operated a machine to reboot, etc.

Figure 2.34 Dynamic adding/deleting function of physical interfaces used



In NIC switching mode, it is possible to make changes manually so that the standby physical interface can be used while the currently operating interface is active (dynamic). [Figure 2.35 Dynamic switching function of physical interfaces used](#) shows an outline of operations performed when the physical interface switching command is executed. For information on the setup,

Figure 2.35 Dynamic switching function of physical interfaces used



2.2.11 User command execution function

A user-defined command can be executed at a specific timing, such as system start up or activation of a virtual interface.

 See

For information on the setup, see [Section "3.6.10 Setting User command execution function"](#).

 Note

It is not possible to use this function in virtual interfaces in Fast switching mode.

Timing to run is as follows:

(1) NIC switching mode

- Running a user command when activated or deactivated an IP address

Run a user specified command when activated or deactivated a logical IP address (when using a logical IP address takeover function) or a physical IP address (when using a physical IP address takeover function) by automatically switching due to an error in line

monitoring or by operating an operation command (activation, deactivation, or manual switching). Use this function to restart an application after activating or deactivating an IP address, to set the specified routing information, to delete the ARP information, and to change a MAC address.

- Running a user command when detected an error in a transfer route

Run a user specified command when an error in line monitoring is detected (such as LAN or HUB errors). Use this to notify a system administrator or an application of detecting an error.

- Running a user command when detected an error by standby patrol or recovery

Run a user specified command when an error in line monitoring or a recovery is detected by standby patrol. Use this to notify a system administrator or an application of detecting an error or recovery. When setting either of a monitoring interval ('-p' option) or the number of the times of continuous monitoring ('-o' option) of standby patrol to zero by a hanetparam command, it is not possible to use this user command execution function.

Figure 2.36 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (Continued.) and Figure 2.37 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (end.) show timing to run a user command when activated or deactivated an IP address in NIC switching mode (a logical IP address takeover function).

Figure 2.36 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (Continued.)

[When activated a system or a cluster service]

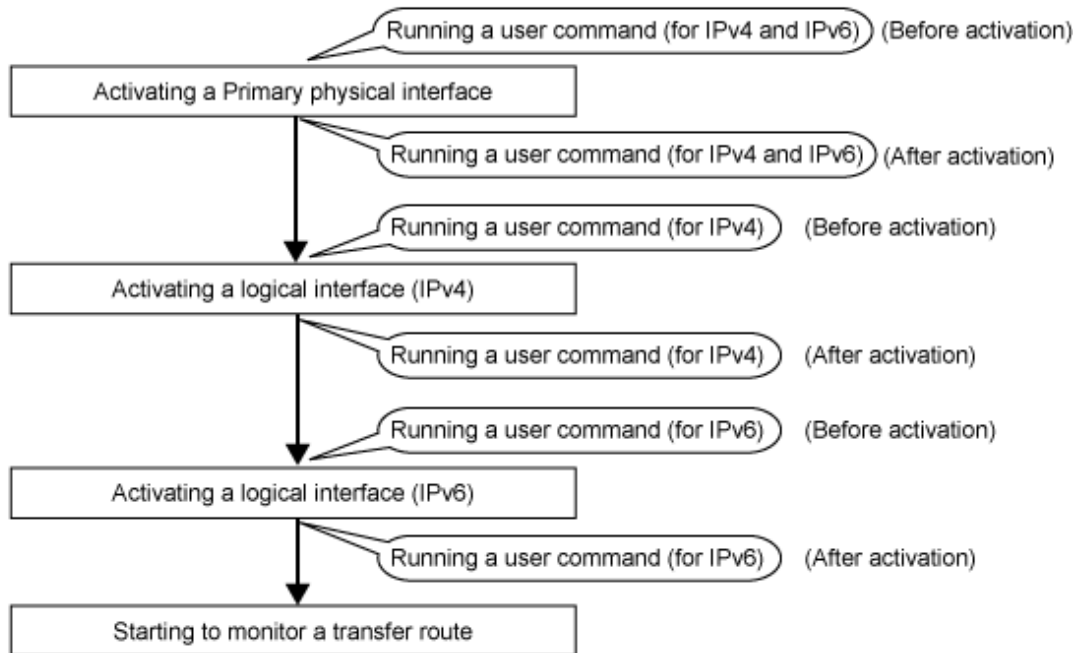


Figure 2.37 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (end.)

[When detected an error in a transfer route or when manually switched with a command]

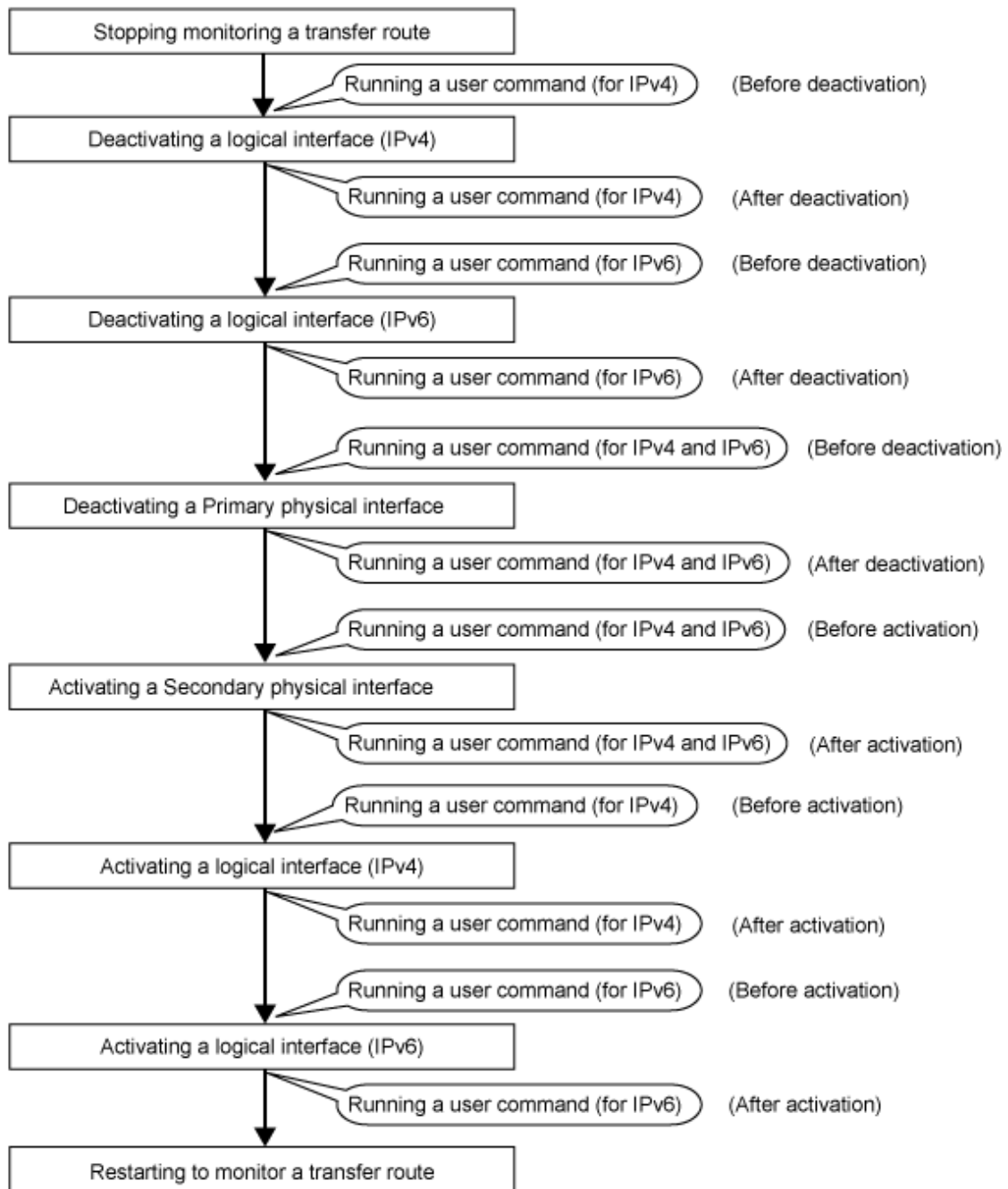
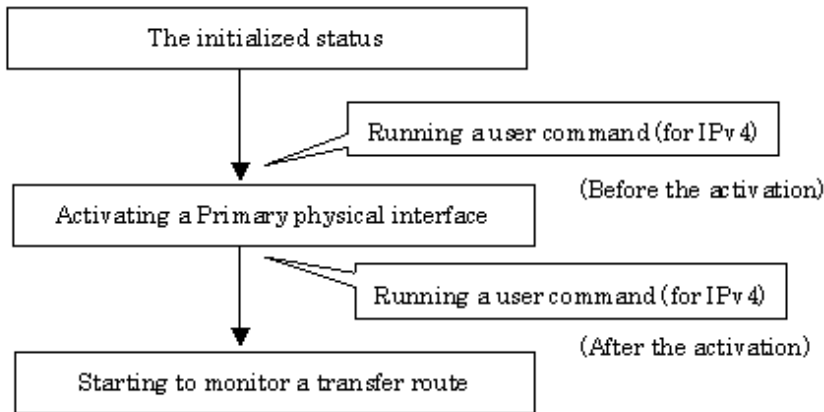


Figure 2.38 Timing of running a user command when activating or deactivating an IP address (a physical IP address takeover function) shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a physical IP address takeover function).

Figure 2.38 Timing of running a user command when activating or deactivating an IP address (a physical IP address takeover function)

[When activated a system or a cluster service]



[When detected an error in a transfer route or when manually switched with a command]

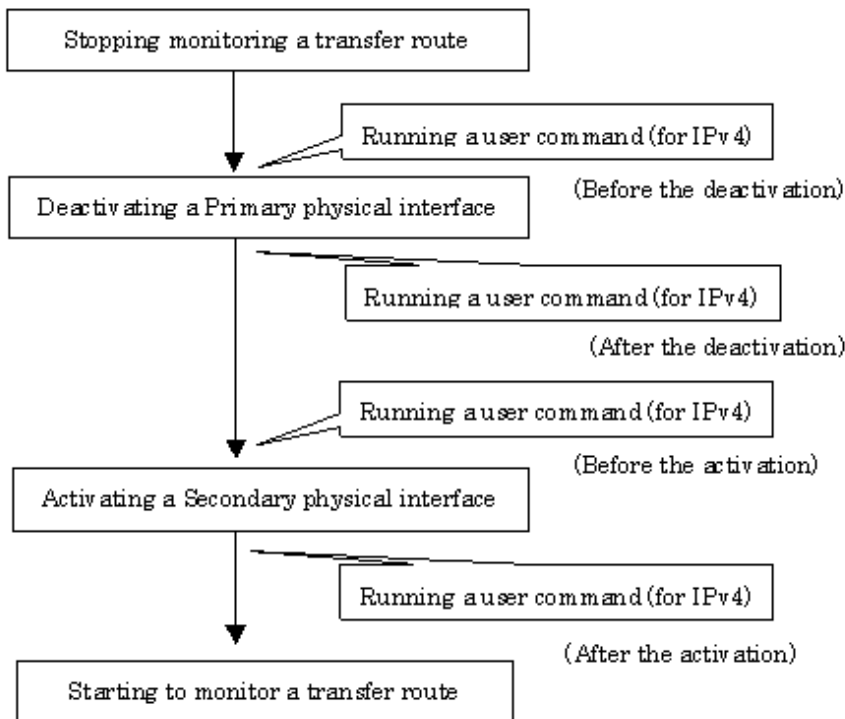
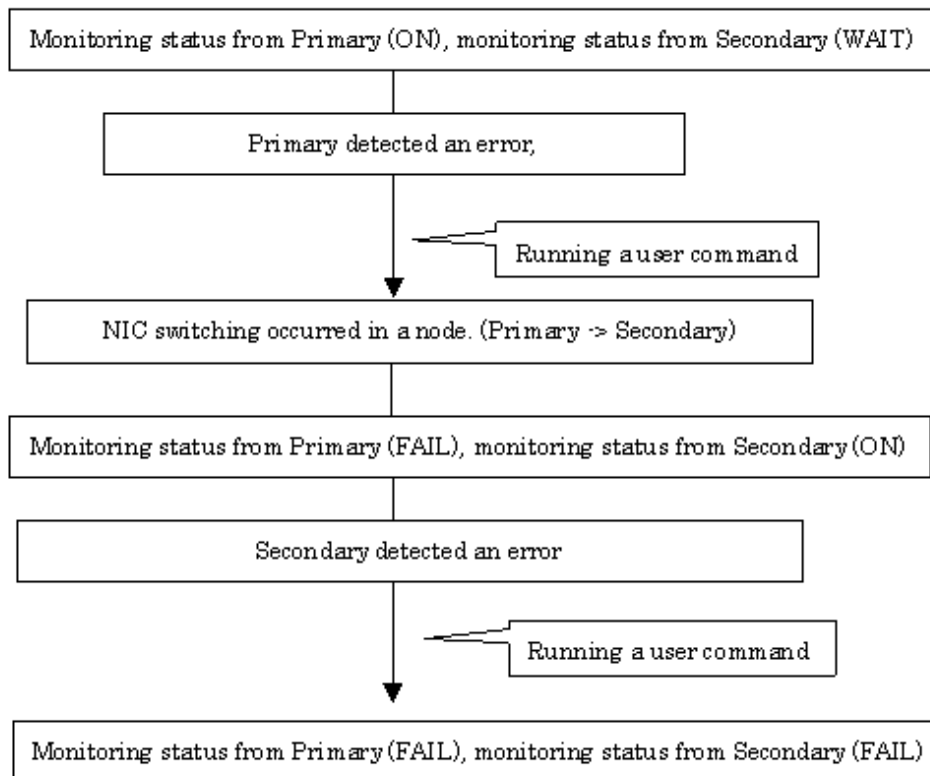


Figure 2.39 Timing of running a user command when detected an error in a transfer route shows timing to run a user command when detected an error in a transfer route in NIC switching mode

Figure 2.39 Timing of running a user command when detected an error in a transfer route

[When started to monitor a transfer route from a Primary interface]



[When started to monitor a transfer route from a Secondary interface]

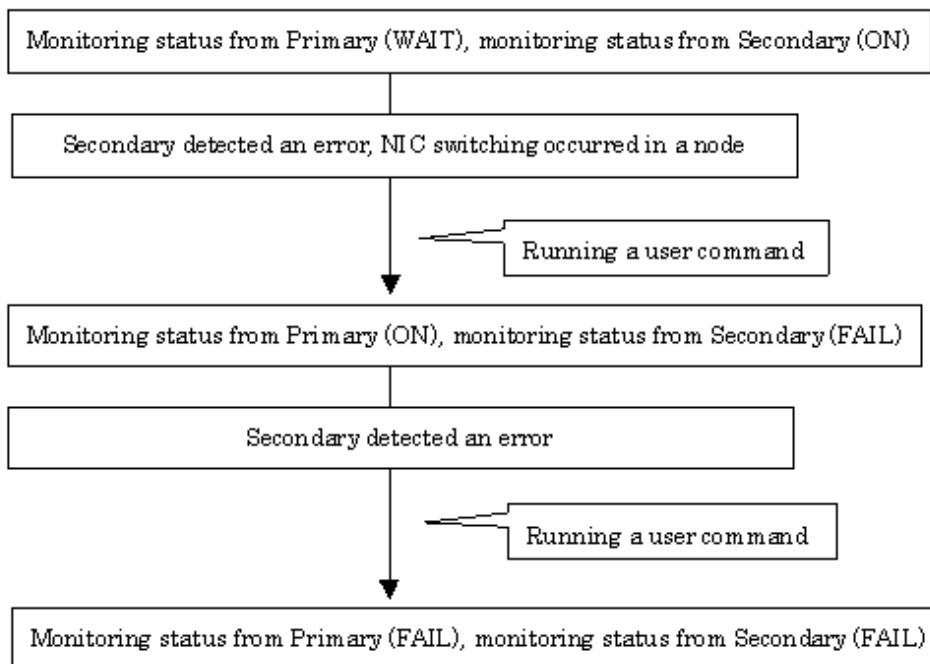
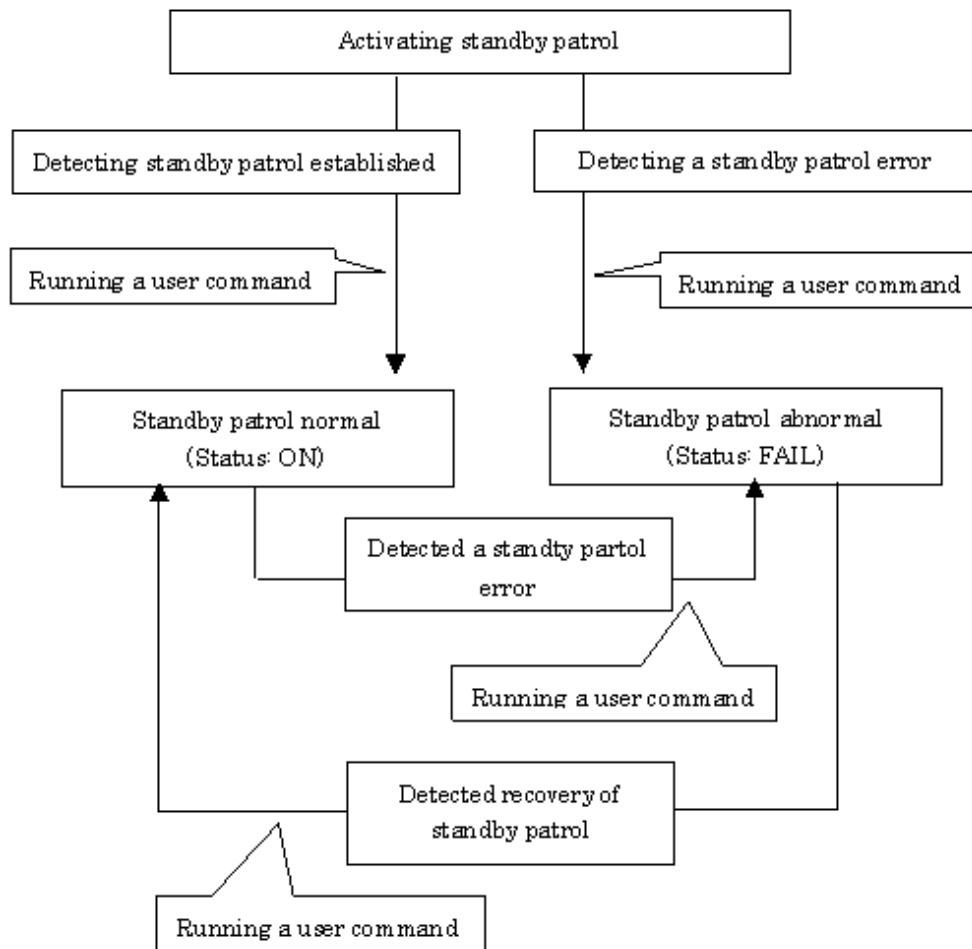


Figure 2.40 Timing of running a user command when detected a standby patrol error or recovery shows timing to run a user command when detected a standby patrol error or recovery in NIC switching mode.

Figure 2.40 Timing of running a user command when detected a standby patrol error or recovery



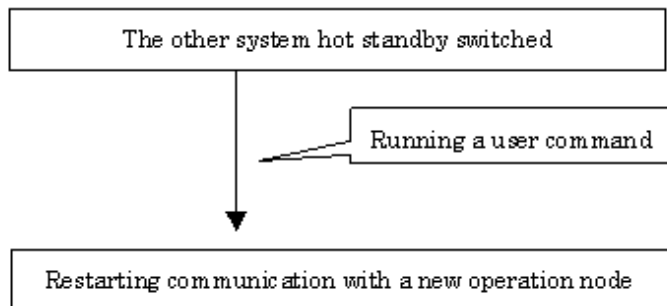
(2) GS/SURE linkage mode

- Running a user command when the other system hot standby switched
 Run a user specified command when hot standby switched at the GS side.
 Use this to notify a system administrator or an application of detecting an error.

Figure 2.41 Timing of running a user command when the other system hot standby switched shows timing to run a user command when the other system hot standby switched in GS/SURE linkage mode.

Figure 2.41 Timing of running a user command when the other system hot standby switched

[When the other system hot standby switched]



(3) Service for Redundant Line Control function

- Executing the user command on service startup

When the service for Redundant Line Control function starts up, for example, system startup or execution of the `resethanet -s`, execute the command specified by a user.

This service is used when starting or restarting an arbitrary service or application in conjunction with starting the service for Redundant Line Control function, or when configuring a static route for a virtual interface.

- Executing the user command when an error on GLS has been detected by the self-checking function

If an error has been detected by the self-checking function, execute the user command, which is used when you want to notify system administrators or applications of an error.

2.3 Other functions

Each mode supports the features shown in the [Table 2.2 Functions available for each mode](#).

Table 2.2 Functions available for each mode

| Function | Mode | | |
|--|---------------------|--------------------|----------------------|
| | Fast switching mode | NIC switching mode | GS/SURE linkage mode |
| Message output function when a line failure occurs | A | A | A |
| DR (Dynamic Reconfiguration) linkage | A | A | A |
| PHP (PCI Hot Plug) linkage | A | A | A |
| Interface status monitoring feature | B | A | X |
| Multiplex transfer route by Tagged VLAN interface | A | A | X |
| Self-checking function | A | A | A |

[Meaning of the symbols] A: Allowed, B: Allowed to only the cluster system, X: Not allowed

2.3.1 Message output when a line failure occurs

If a line failure is detected on a physical interface, an error message is displayed on the console. This function enables the real-time recognition of a line failure.

2.3.2 DR (Dynamic Reconfiguration) function

It is possible to use a Dynamic Reconfiguration function (hereinafter DR function) provided by the following models in GLS:

- SPARC M12-2S/ M10-4S
- SPARC Enterprise M4000/M5000/M8000/M9000



See the following manuals to use a DR function.

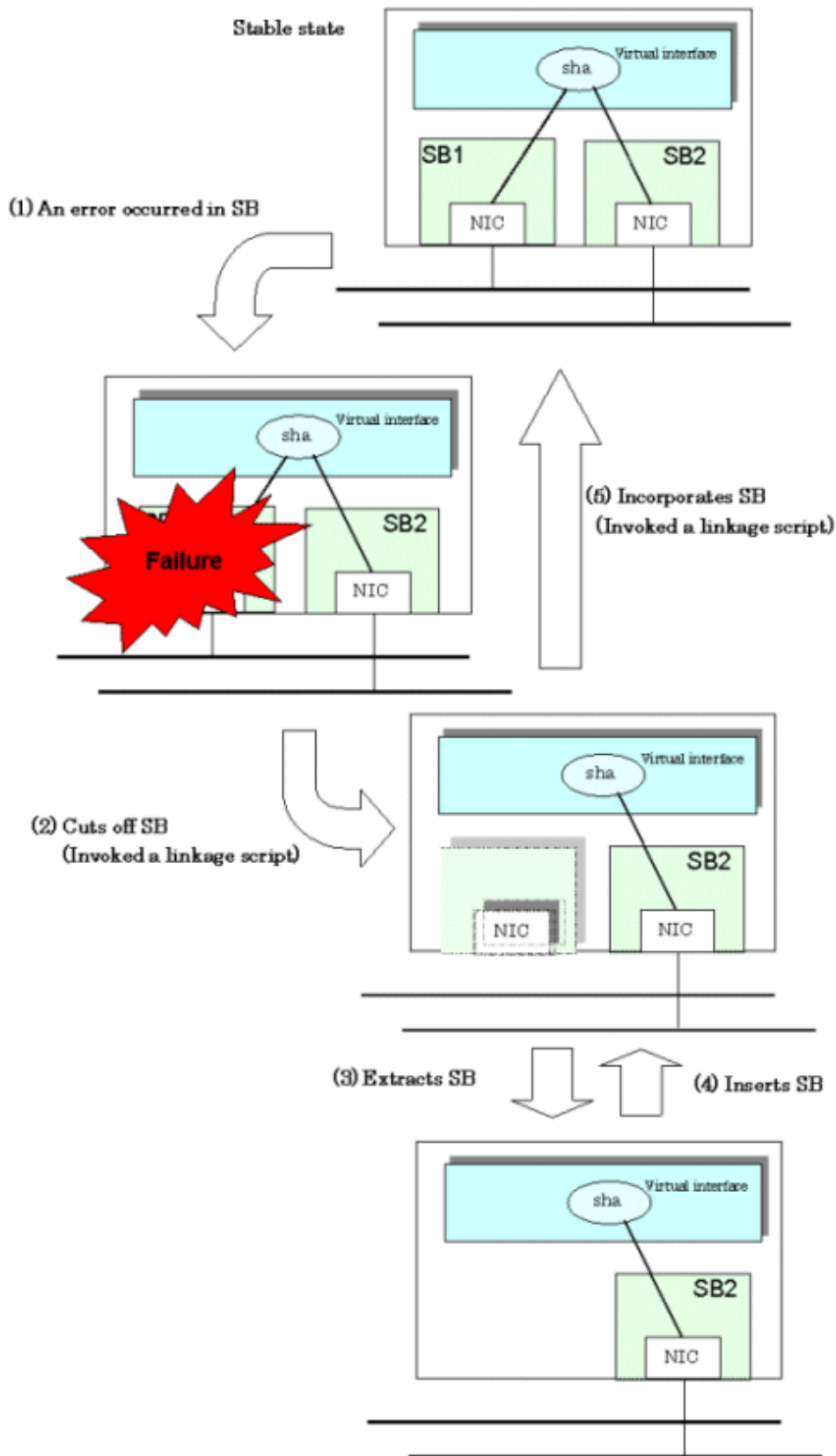
- When using the DR function of ESF (Enhanced Support Facility)
 - Enhanced Support Facility User's Guide For Dynamic Reconfiguration
 - Enhanced Support Facility User's Guide Dynamic Reconfiguration I/O device

- When using the DR function of XSCF (eXtended System Control Facility)
 - For SPARC M12-2S/ M10-4S
 - Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide
 - Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual
 - For SPARC Enterprise M4000/M5000/M8000/M9000
 - Dynamic Reconfiguration (DR) User's Guide
 - XSCF User's Guide
-

2.3.2.1 DR (Dynamic Reconfiguration) linkage function

A DR connection script, which enables automatic disconnection or embedding of an NIC in a redundant configuration, is provided to use the DR function of ESF in a Redundant Line Control function. When a DR connection script is invoked by executing a DR command, it disconnects or connects a virtual interface (sha0, etc.) and an actual interface (hme0, etc.). This makes it possible to execute a DR function without realizing an interface, a function, and a DR connection script used in various modes. "[Figure 2.42 Flow of exchanging system boards \(SB\) using a DR function](#)" shows a flow of exchanging system boards (SB) using a DR function.

Figure 2.42 Flow of exchanging system boards (SB) using a DR function





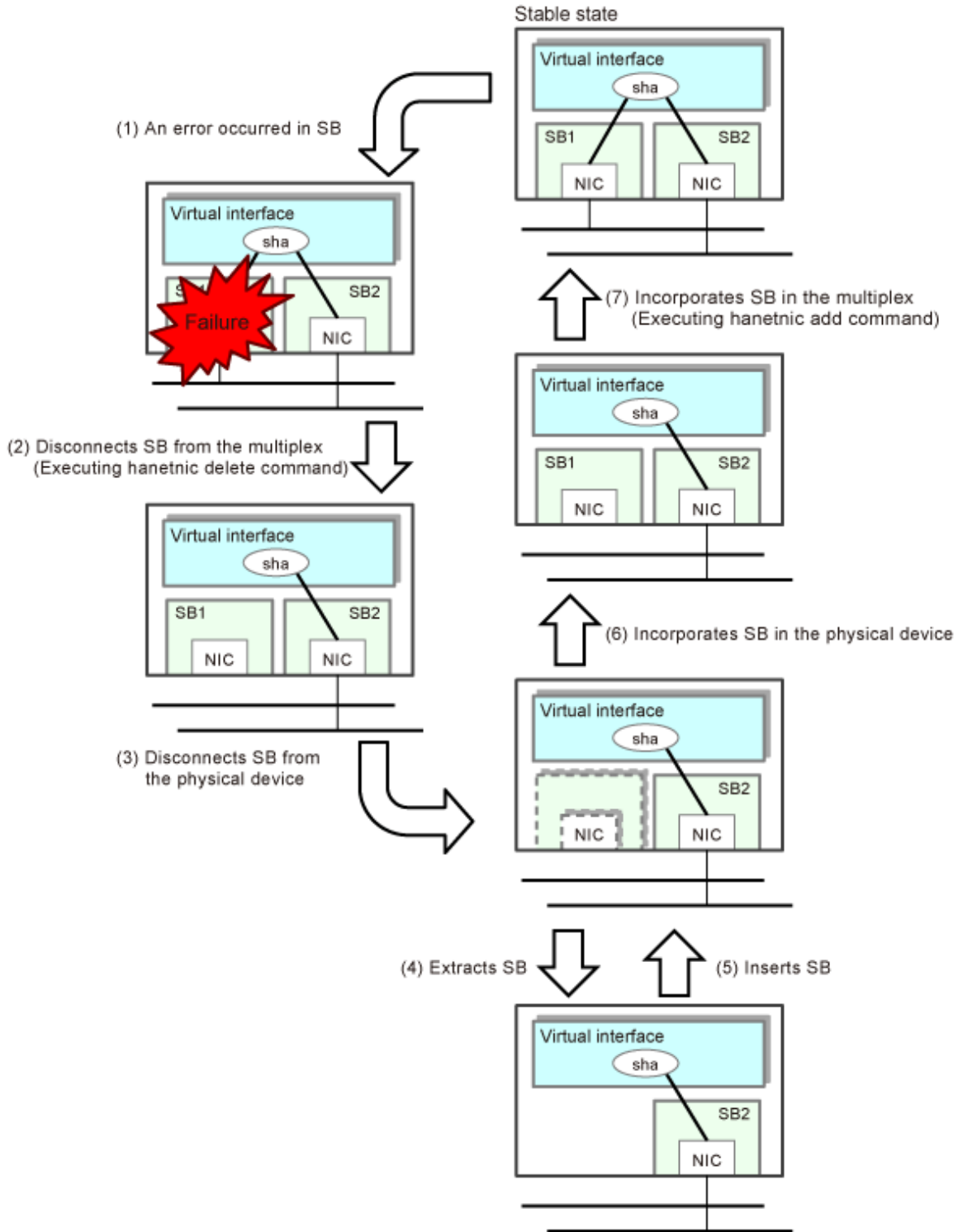
Note

The DR linkage script does not support the disconnecting/embedding of an NIC under a redundant virtual interface comprised of an IPv6 virtual interface and a tagged VLAN Interface. If disconnecting the system board with a DR command, manually disconnect the NIC built into the system board from the multiplex configuration first. Also, after performing the system board embedding, perform embedding to the multiplex configuration.

2.3.2.2 DR function of XSCF

When using DR function of XSCF, execute the "hanetnic delete" command to delete NIC from the redundant configuration before detaching the system board. Similarly, after attaching the system board, execute the "hanetnic add" command to add NIC to the redundant configuration. The following shows the flow chart of replacing the system board (SB) by the DR function of XSCF.

Figure 2.43 Flow of replacing the system board (SB) by the DR function of XSCF



See

- The concrete operation method varies depending on the redundant mode. For the operation method for the DR function of XSCF, see "4.5.2 Replacing the system board using the DR of XSCF."
- For details on the "hanetnic" command, see "7.9 hanetnic Command."

2.3.3 PCI Hot Plug (PHP) linkage

It is possible to use PCI Hot Plug function (hereinafter PHP function) provided by the following models in GLS:

- SPARC M12/ M10
- SPARC Enterprise M4000/M5000/M8000/M9000



Note

See the following manuals to use the PHP function.

- For SPARC M12
 - Fujitsu SPARC M12-1 Service Manual
 - Fujitsu SPARC M12-2/2S Service Manual
 - PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual
- For SPARC M10
 - Fujitsu M10-1/SPARC M10-1 Service Manual
 - Fujitsu M10-4/Fujitsu M10-4S/SPARC M10-4/SPARC M10-4S Service Manual
 - PCI Expansion Unit for Fujitsu M10/SPARC M10 Systems Service Manual
- For SPARC Enterprise M4000/M5000/M8000/M9000
 - SPARC Enterprise M4000/M5000 Servers Service Manual
 - SPARC Enterprise M8000/M9000 Servers Service Manual

Refer to "4.5.3 Replacement/Expansion PHP (PCI Hot Plug)" for details on how to operate PHP of Redundant Line Control function.

2.3.4 Interface status monitoring feature

By monitoring UP/Down status of an interface used in Redundant Line Control function, it is possible to recover the regular operation when a user mistakenly change Up/Down of a interface using ifconfig(1M) command. This feature automatically starts up when a virtual interface is activated.

The following is a list of interfaces available for recovery using this feature.

Table 2.3 Recoverable interfaces using interface status monitoring feature

| Mode | Single System | | | Cluster System | | |
|-----------------|------------------------------|------------------------|--------------|------------------------------|------------------------|--------------|
| | Virtual I/F (logical I/F) | Logical virtual I/F | Physical I/F | Virtual I/F (logical I/F) | Logical virtual I/F | Physical I/F |
| Fast switching | N | N | N | A | A | N |
| NIC switching | A | - | A | A | - | A |
| GS/SURE linkage | N | - | N | A | - | N |

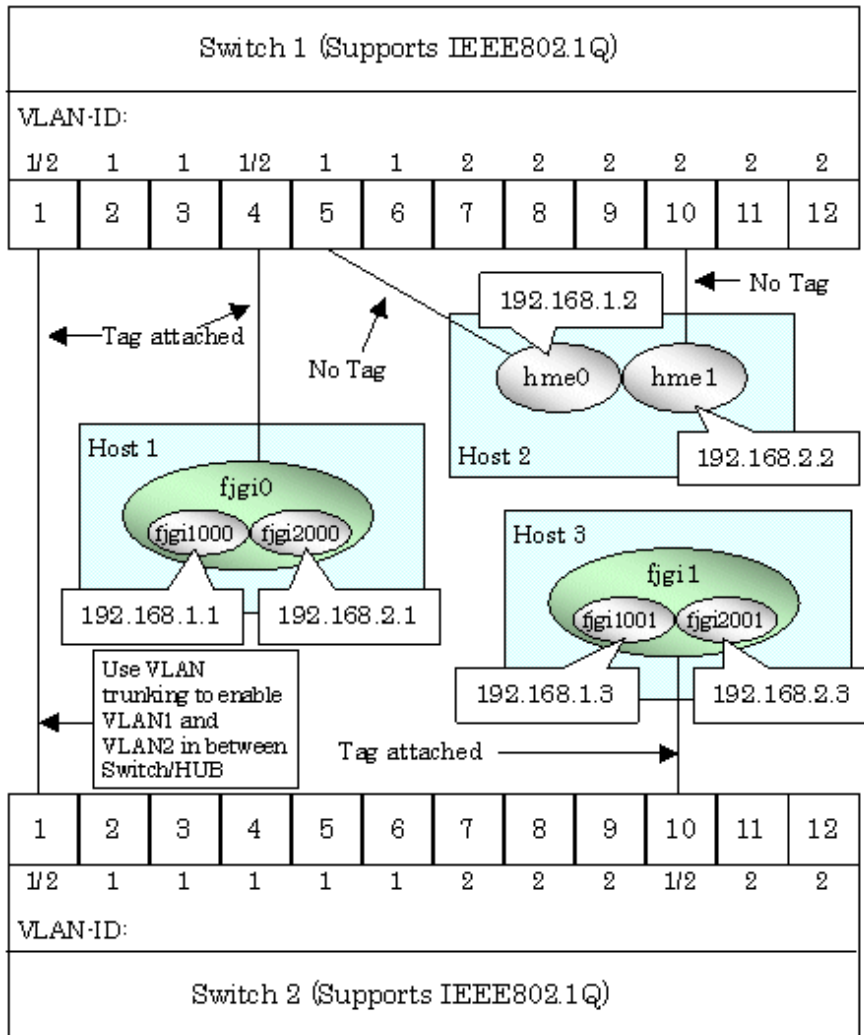
[Meaning of the symbols] A: Recoverable N: Non-recoverable -: No such combination

2.3.5 Multiplexing transfer route with Tagged VLAN interfaces

Tagged VLAN allows multiple virtual networks on a single transfer path by assigning an identifier or a tag on the packet for disparate network. In order to build a Tagged VLAN environment, please ensure that you have NICs and switches/hubs that satisfy "IEEE802.1Q" standard. The connection between switches/hubs that handles Tagged VLAN is called VLAN trunking. VLAN Trunking allows Tagged VLAN on each Switch/HUB to be handled on the same physical network cable.

The figure below shows the network structure that uses Tagged VLAN

Figure 2.44 Network structure using Tagged VLAN



In Figure 2.44 Network structure using Tagged VLAN, VLAN1(VLAN-ID:1) and VLAN2(VLAN-ID:2) are created on both Switch 1 and Switch 2, and port1 on both switches is used for VLAN Trunking.
 A physical interface "fjgi0" on Host 1 has two VLAN interfaces "fjgi1000" and "fjgi2000", and is connected to port 4 on Switch 1 that belongs to both VLAN1 and VLAN2. Host 1 uses "fjgi1000" and "fjgi2000" to transmit tagged frames.
 Similarly, a physical interface "fjgi1" on Host 3 has two VLAN interfaces "fjgi1001" and "fjgi2001", and is connected to port 10 on Switch 2 that belongs to both VLAN1 and VLAN2. Host 3 uses these VLAN interfaces to establish tagged frame communication.
 Host 2 achieves data communications on both VLAN1 and VLAN2 by connecting a physical interface "hme0" to port 5 that belongs to VLAN1, and another physical interface "hme1" to port 10 that belongs to VLAN2.

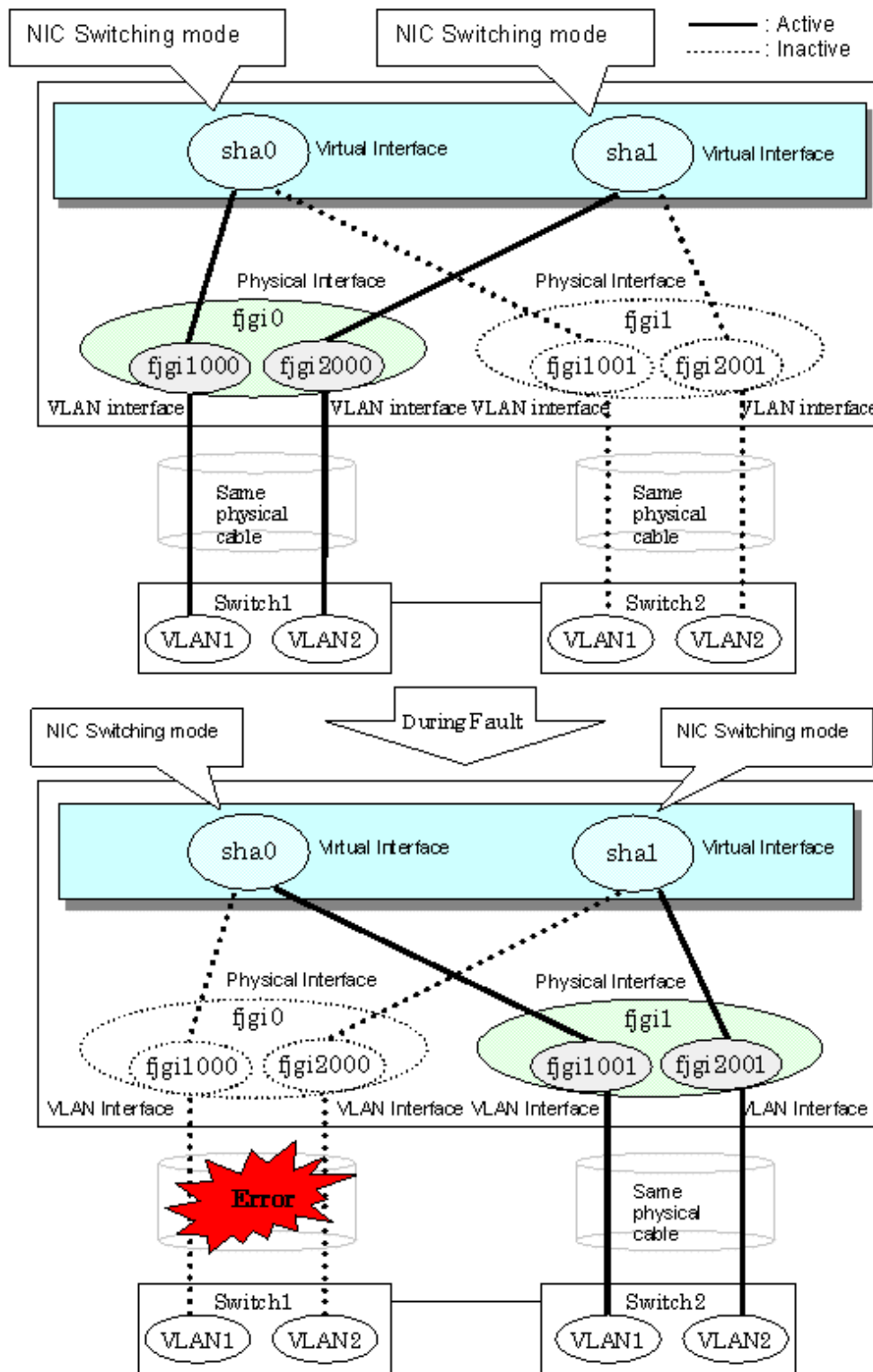
Note

- Ensure a switch/hub is configured to handle Tagged VLAN.
- When using a Tagged VLAN interface (fjgi1000 or fjgi2000), local and remote VLAN-ID must be identical. VLAN-ID is generated from a Tagged VLAN interface number truncating the last 3 digits. For example, in the case where a tagged VLAN interface is fjgi1000, VLAN-ID will be 1, and similarly for fjgi123001, the VLAN-ID for this interface comes to be 123.

2.3.5.1 Redundant Line Control function using Tagged VLAN interface

In Redundant Line Control Function, transfer paths can be multiplexed with tagged VLAN interfaces using an ethernet driver that complies with the tagged VLAN specification.

Figure 2.45 Using Tagged VLAN Interface architecture

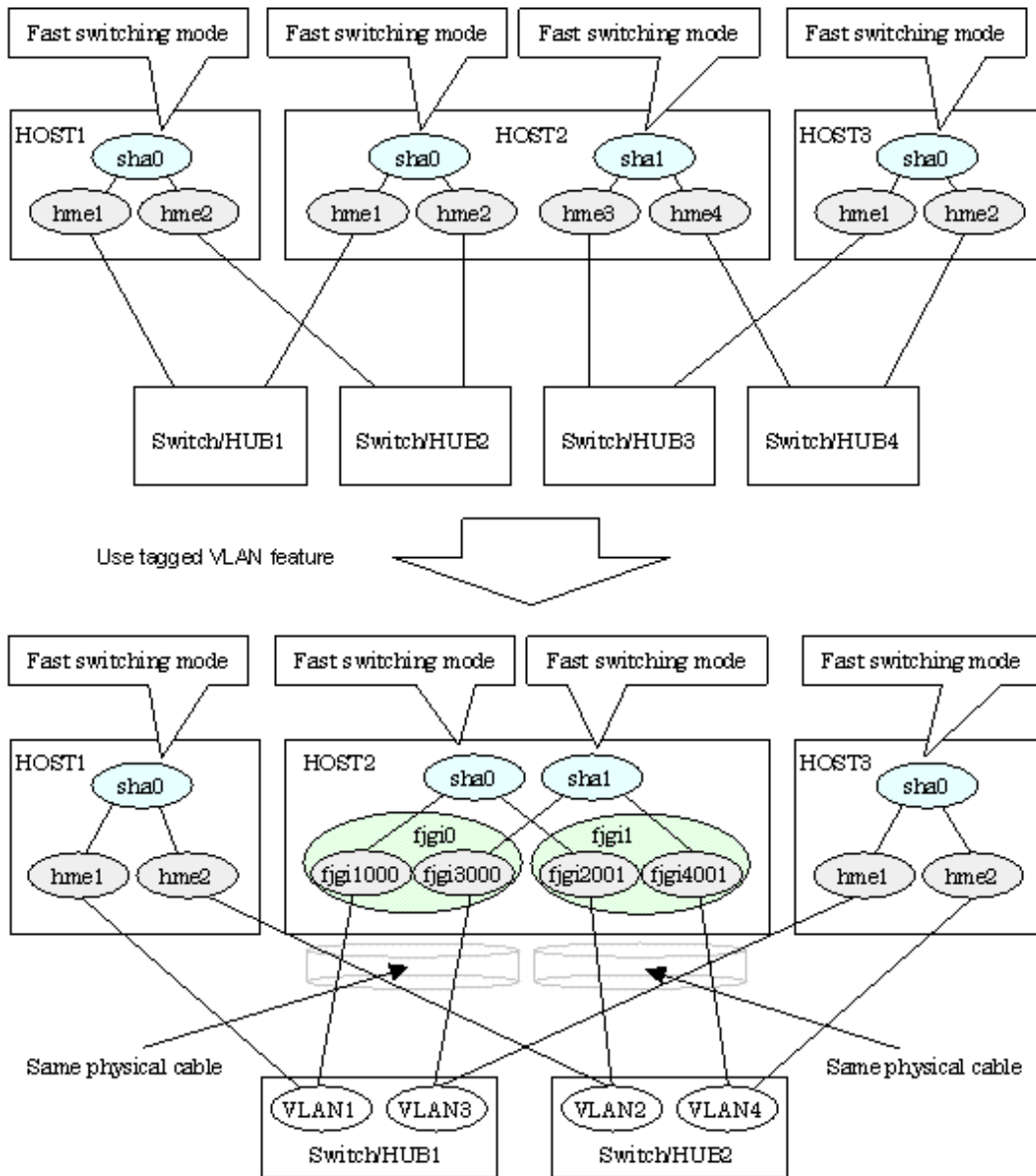


P Point

Even if switches/hubs or NICs come short, using tagged VLAN can provide sufficient number of transfer routes in various network architectures.

When building a server system as three-layered model, it is possible to implement transfer route multiplexing feature on an environment where number of Switch/HUB and NIC is constrained.

Figure 2.46 When Switch/HUB and NIC come short.



The following modes support a Tagged VLAN.

- Fast switching mode
- NIC switching mode

Note

Multiplexed transfer routes with Tagged VLAN cannot be used in GS/SURE linkage mode.

See

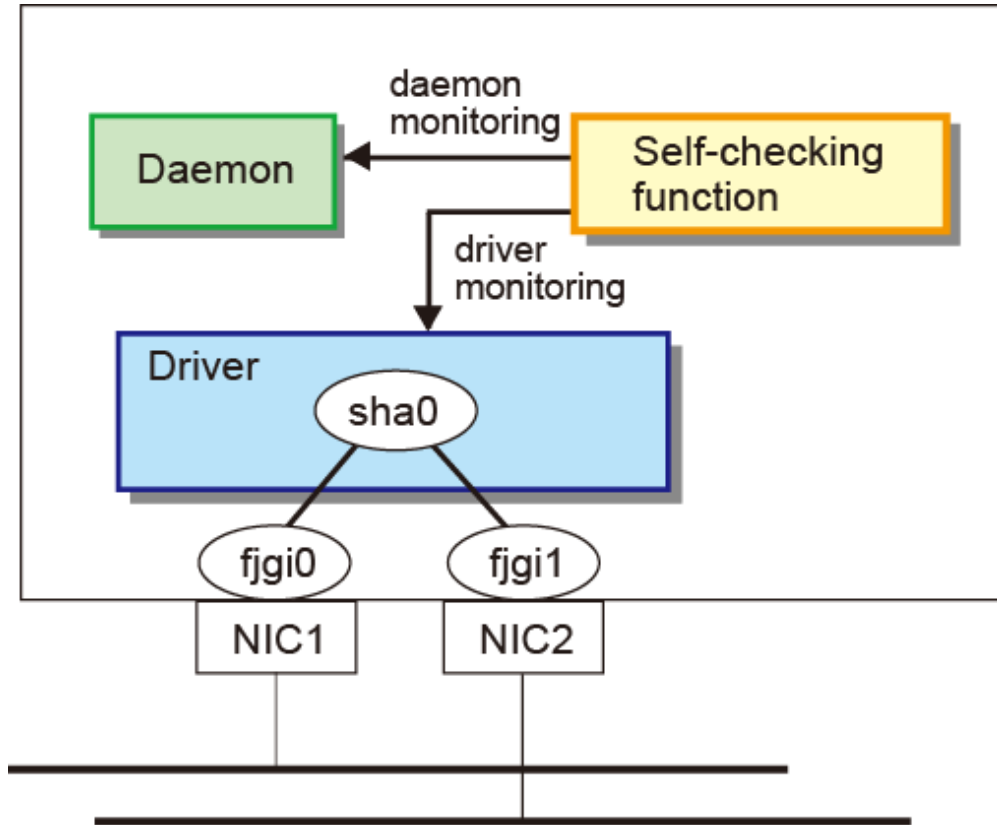
For details on using Tagged VLAN for other modes, refer to "3.7.3 Transfer route multiplexing with Tagged VLAN interface".

2.3.6 Self-checking function

GLS provides highly reliable transfer routes by using the control daemon and virtual driver.

The self-checking function monitors those states periodically and notifies to users if an error occurs. The function is enabled automatically.

Figure 2.47 Self-checking function

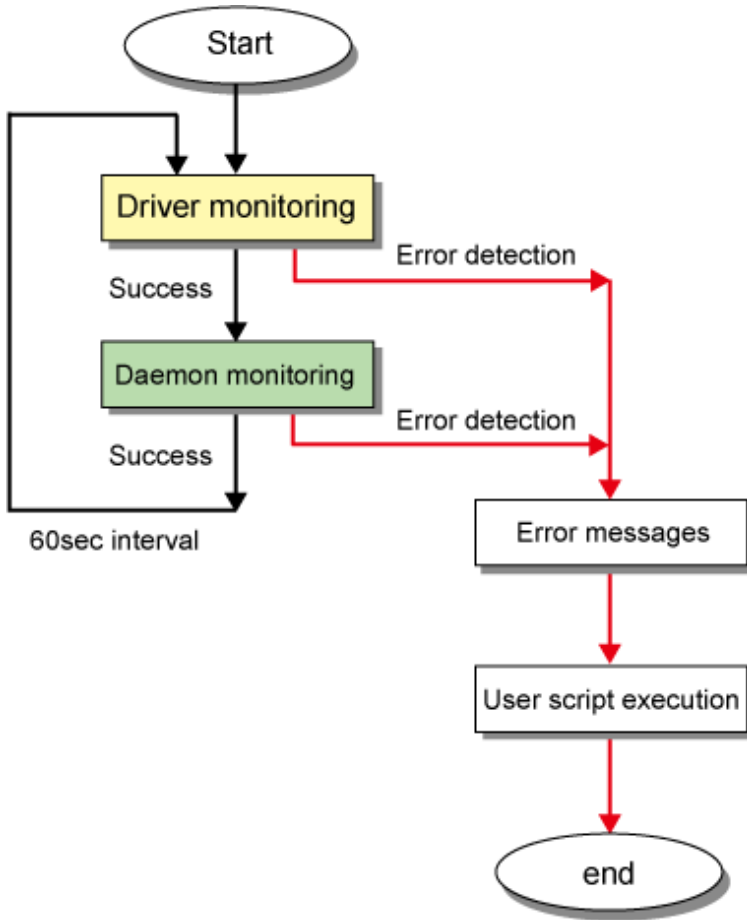


Note

The self-checking function does not detect the system wide errors or hangs. Use the cluster for these.

The following describes how the monitoring is performed with the self-checking function. The virtual driver and control daemon are monitored periodically.

Figure 2.48 Error detection of the self-checking function



The monitoring targets are as follows. A system wide hang or error status cannot be detected.

| Monitoring target | Error type | Error detection method |
|-------------------|---------------------------|---|
| Driver | Hung-up | No response from the virtual driver for 60 seconds |
| | I/O Error | Information is not received from the driver five times in a row |
| Daemon | Hung-up | There is no response from the control daemon for 300 seconds |
| | I/O error | Information is not received from the control daemon five times in a row |
| | Stopped process detection | There is no control daemon process |

If an error has been detected, the following messages will be output to the syslog. After that, the monitoring function stops. To restart monitoring, reboot the system after collecting troubleshooting information.

- An error occurred in the virtual driver

The following message is output and the monitoring function stopped.

```
ERROR: 97427: sha driver error has been detected. code=xxx
```

xxx: error type (hungup or I/O error)

- An error occurred in the control daemon

The following message is output. After that, if there is no response from the control daemon for 300 seconds, the monitoring function will stop.

```
ERROR: 97627: hanetctld error has been detected. code=xxx
```

xxx: error type (hungup, I/O error, or stopped process)

However, if the control daemon recovered, the following message will be output and the monitoring will continue.

```
ERROR: 97727: hanetctld recovery has been detected.
```

Note that placing a script in the following location allows the script to be executed when an error is detected. For more details, see "[3.6.10 Setting User command execution function.](#)"

```
/etc/opt/FJSVhanet/script/system/monitor
```

Information

Rebooting the system is recommended after the monitoring function stopped.

If a hung-up or an I/O error was detected due to temporary system load, the self-check function can be restored by restarting it as below.

```
# svcadm restart fjsvhanet-poll
```

If the self-check function failed to be restarted, collect materials for examination, and then contact field engineers to report the error message.

In this case, an error may have been occurred or the system resources may be low. To resolve these problems, reboot the system.

2.4 Notes

2.4.1 General

Notes on setting a configuration:

- The minimum and maximum number of virtual and logical virtual interface can be defined is 1 to 64.
- The number of physical interfaces can be used for redundancy on a single virtual interface is within 1 to 8 for Fast switching and GS/SURE linkage mode. For NIC switching mode, the range is within 1 to 2.
- The number of logical virtual interfaces that can be defined to a single logical virtual interface is within 1 to 63.
- When using the tagged VLAN interface in Solaris 11 or later environment, do not specify the VLAN link name to create the tagged VLAN interface. Use the automatically generated interface name.

Automatically generated interface name

"net" + VLAN-ID + instance number (*1)

*1: The instance number is represented by 3-digit number XXX (from 000 to 999).

Example: If VLAN-ID is 12 and the NIC name is net3, the automatically generated VLAN interface name will become "net12003".

- The interface name that is bundled by the virtual interface must be specified within 11 characters.
- If VLAN is not used, an interface name that can be recognized as the VLAN interface name cannot be specified for the interface bundled by the virtual interface. For example, if an integer followed by "net" is 1000 or larger such as "net12003", this interface name cannot be specified.
- To use all host names and IP addresses used in a Redundant Line Control function, they must be defined in /etc/inet/ipnodes files of the local system.

- The system automatically determines the length of MTU for an interface. Nonetheless, it is possible to change the length of MTU using user command execution function. For changing MTU length, refer to "[3.6.10 Setting User command execution function](#)". Note that the length of MTU cannot be modified in other redundant modes.
- The IPMP virtual interface (ipmpX) cannot be made redundant.

Notes on the operation:

- It is not possible to use a multicast IP address in a Redundant Line Control function.
- Do not execute a DR linkage function in a machine that runs the cluster operation.
- Do not operate physical interfaces that a virtual interface bundles with an ifconfig command.
- GLS does not support Verified Boot.

The following warning messages may be output to the syslog. However, these messages do not disrupt the system configuration or system operation. No action is required.

```
WARNING: Signature verification of module /usr/kernel/drv/sparcv9/rvnet failed
WARNING: Signature verification of module /usr/kernel/drv/sparcv9/rvnetcf failed
WARNING: Signature verification of module /usr/kernel/drv/sparcv9/sha failed
```

- When using Fast switching mode or GS/SURE linkage mode, the following warning messages may be output to the system log during OS startup or while running hotplug(1M) command of Solaris standard, cfgadm(1M) command, and ldm(1M) command. However, these messages do not disrupt the system configuration or system operation. No action is required.

(*shaX*: predefined Virtual NIC name)

```
IP: get_link_resource for shaX error(operation failed)
IP: get_link_resource(shaX) failed
```

Notes on applications:

- When an application uses TCP, the data lost when an error occurred in a transfer route is guaranteed by resending from TCP and reaches the other system in the end. Therefore, TCP connection is not disconnected and there is no error in communication. However, it is necessary to set a timer value longer than the time to finish disconnecting/switching a transfer route when an application monitors a response by such timer. When TCP connection is disconnected by the reason such as incapability to change a timer value, reestablish the TCP connection and recover the communication.
- The data lost at the time of an error in a transfer route is not guaranteed when an application uses the UDP. It is necessary to execute a recovery process such as sending the data by the application itself.
- It is not possible to use DHCP (a server function and a client function) as the application in a Redundant Line Control function.
- When using NTP as an application, it is necessary to activate an IP address that a Redundant Line Control function controls before activating an NTP daemon. No special operation is required when activating a system because a Redundant Line Control function is activated before an NTP daemon. However, when manually activated an IP address with an operation command or when running cluster operation, reactivate an NTP daemon after an IP address is activated.

Notes on Solaris Zones:

- If a zone is activated, an interface in the shared-IP zone cannot be deactivated.
If you want to change or delete the redundant line control function settings, it is necessary to stop the zone first.
- For a shared-IP zone, if a virtual interface does not exist in a zone, the zone cannot be activated.
Before starting the zone, activate the virtual interface.
- If the shared-IP zone is started after NIC is switched from the primary interface to the secondary interface in NIC switching mode, it might take up to 20 seconds to enable communication in the zone.
- For a shared-IP zone, if the zone is set to use the secondary interface in NIC switching mode, a network interface in the zone will automatically be switched to the primary interface when a virtual interface is activated.
- An IP address specified for a shared-IP zone and that for a virtual interface must be different.
If the same IP is specified for both, zone startup or virtual interface activation will fail.

2.4.2 Duplicated operation by Fast switching mode

- Redundant Line Control function must be operating on each system that performs duplicated operation by Fast switching mode.
- In Fast switching mode, one virtual network is configured to the redundant transfer route. Therefore, a new network number or a subnet number to this virtual network is necessary.
- Only one NIC interface is connectable on one network. It is not possible to connect more than one interface on the same network.
- Any combination is possible for redundant NICs. When combined those of different transfer abilities, the communication ability is suppressed by the one of less transfer ability. Therefore, it is recommended to combine the same kind of NICs and to make them redundant.
- In Fast switching mode, a dedicated Ethernet frame is used. Therefore, when operating VLAN (Virtual LAN), occasionally it is not possible to communicate depending on the setting of VLAN. In such a case, either to stop using VLAN or to change the setting of VLAN so that it becomes possible to use an optional Ethernet frame.
- The interface created by SR-IOV cannot be used.
- Do not set the hostmodel parameter which is configured with ipadm command to strong, because communication with virtual interface will be disabled.

2.4.3 Duplicated operation via NIC switching mode

- One unit of HUB to be connected in NIC switching mode is sufficient, but communication may not be conducted normally if the HUB has MAC learning capabilities. In such a case, add a HUB to make a HUB-to-HUB connection and then connect the cable to each HUB (See "[Figure 2.7 System configuration in NIC switching mode](#)" of "[2.1.2 NIC switching mode](#)").
- It is not possible to use a standby patrol function when the type of interface to use is "mpnetX (a logical interface of a multipath)".
- Communication with a multicast IP address is executed using a physical interface corresponding to a node name (uname -n). When used this interface in NIC switching mode, it is not possible to communicate with a multicast IP address. This occasionally outputs a following WARNING message from in.rdisc when activated a system:
in.rdiscd[xxx]: setsockopt(IP_DROP_MEMBERSHIP): Cannot assign requested address
To prevent the output of this message, disable the service svc:/network/routing/rdisc and do not activate in.rdisc.
- In a standby patrol function of NIC switching mode, a dedicated Ethernet frame is used. Therefore, when operating VLAN (Virtual LAN), occasionally it is not possible to use a standby patrol function depending on the setting of VLAN. In such a case, either to stop a standby patrol function or VLAN, or change the setting of VLAN so that it becomes possible to use an optional Ethernet frame.
- In NIC switching mode, it is necessary to use a HUB to which an IP address can be set in order to monitor errors by the ping command. If the IP address cannot be set, an IP address of other device connected to the HUB can be used. However, be sure that if an error occurs in the device, the error is treated as a transfer route error.
- When using an IPv6 virtual interface with Solaris 10, create an /etc/hostname6.interface file corresponding to a Primary physical interface so that an in.ndpd daemon is activated at activating a system. When the in.ndpd daemon is not activated, an IPv6 address is not configured automatically. When creating a /etc/hostname6.interface file, make it empty without fail.
- When using an IPv6 virtual interface, an in.ndpd daemon is occasionally reactivated not to delay configuring an IPv6 address automatically due to the LinkUp delay of Ethernet. A message "SIGHUP: restart and reread config file" is output from the in.ndpd daemon following this, however, this is not an error.
- To operate ping monitoring over the system that runs firewall, configure the firewall so that ping can pass through the firewall. Otherwise, it fails to operate ping monitoring. The firewall settings must be the same for both of the primary and secondary interfaces.
- When using an IPv6 virtual interface in an environment where the address autoconfiguration with an IPv6 router is not in use, assign a link local address to the monitored IP.
- In Solaris 11 or later environment, if the setting of IPv6 address by ipadm create-addr is not performed for the physical interfaces bundled by a virtual interface of IPv6 or dual stack configuration, it may fail the activation of virtual interfaces. In this case, set the IP address by using ipadm create-addr command.

2.4.4 Duplicated operation via GS/SURE linkage mode

- In GS/SURE linkage mode, the system uses duplicated paths concurrently but it cannot be expected to improve the throughput.

- Be sure to set a function to monitor the other side to communicate when using GS/SURE linkage mode. See "[7.5 hanetobserv Command](#)" as to how to set.
- In GS/SURE mode, data communication with SPARC Servers, PRIMEPOWER, GP7000F, Fujitsu S series, GP-S, PRIMERGY, or PRIMEQUEST is not possible.
- In GS/SURE linkage mode, the route to the virtual IP address of the destination system is recognized by using the RIP protocol. Set the RIP advertisement on the GS/SURE system (destination system). In this mode, RIPv1 is supported.
- In GS/SURE linkage mode, communication with up to four hosts is possible. Communication with the fifth host or later is not possible.
- It is not possible to operate under the subnet environment of the variable length in GS/SURE linkage mode. The same value must be assigned to all subnet masks for virtual interfaces.
- Only one connectable NIC interface is provided on a single network for the local system. Multiple interfaces cannot be connected on the same network.
- When using LR, CLCU, or LANC2 as the LAN adapter for the global server PRIMEFORCE, use "channel embedded system."
- When using GS/SURE linkage mode, you must specify the definition to use the following functions for the network definition of VTAM-G TISP on the global server PRIMEFORCE:
 - Connection function with LAN duplication
 - Recovery function from network failure
 - Recovery function from host failure (Hot standby by dynamic switching of the system address)
- For details on definition, see "OSIV VTAM-G TISP Handbook."
- Do not connect to other servers between the local system and the remote system (GS server/ SURE SYSTEM) in GS/SURE linkage mode.
- For GS Hot-standby, the node that received the down notification by the TNOTIFY command from GS is recognized as the communication target.
- If a TNOTIFY command is executed to GLS from GS, GLS returns the processing result 80.

Chapter 3 Environment configuration

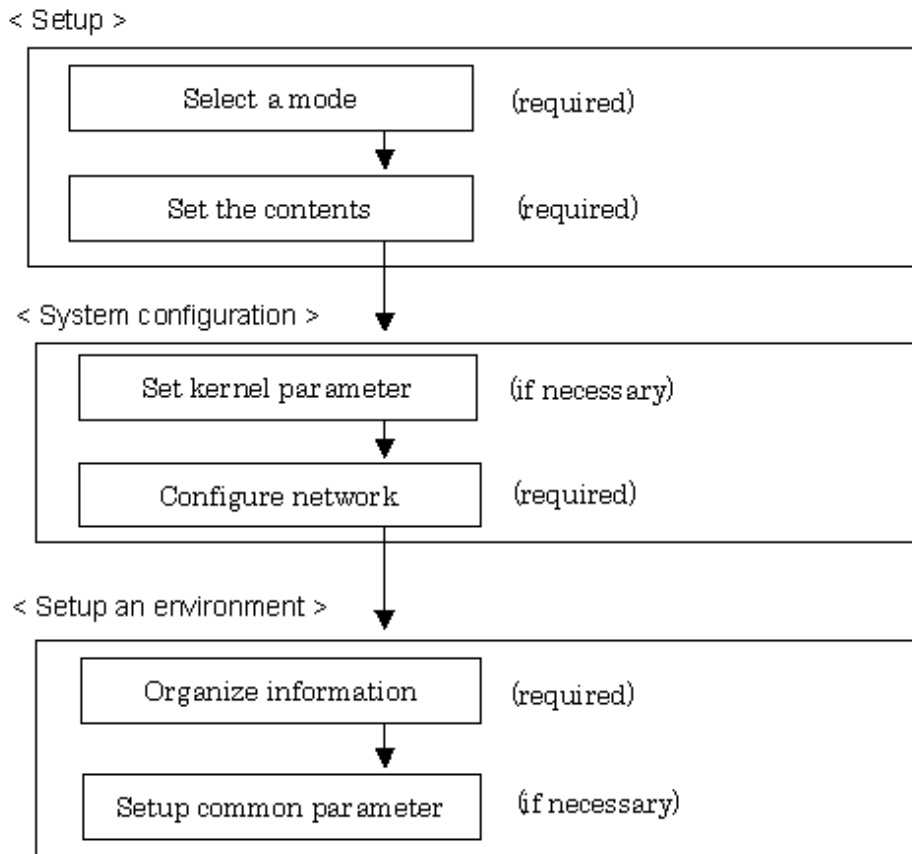
This chapter discusses how to set up and configure GLS.

3.1 Setup

Select a GLS mode and prepare for the environmental information such as interface names and IP addresses.

The following is the procedure of this configuration

Figure 3.1 Configuration to Setting up an environment



3.1.1 Selecting mode

Determine which mode to use. [Table 3.1 Selection of modes](#) indicates the selection of modes.

For selecting adequate mode, refer to "[1.1.2 Criteria for selecting redundant line control methods](#)".

Table 3.1 Selection of modes

| Mode | Selecting mode |
|----------------------|--|
| Fast switching mode | Select this mode if every one of the remote hosts is a Solaris server or Linux server. This mode can detect the abnormalities of the multiplexed transfer route immediately. When abnormalities are detected, communication can be immediately changed to a normal transfer route. |
| NIC switching mode | Select this mode, if a hot-standby router, a network load balancer, or servers and other various network devices from other manufacturers are used. This mode is usable for many configurations. |
| GS/SURE linkage mode | Select this mode if using GS and SURE SYSTEM exclusively. Other servers or any network device must not exist in the same network. |

It is possible to create multiple virtual interfaces in a single system to use several modes concurrently.

 **Note**

In order to use redundant mode on a single system, you must provide NIC for each mode. For example, when using hme0 and hme1 in Fast switching mode, the other modes such as NIC switching or GS/SURE linkage mode must use different NIC (such as hme2 and hme3).

Specify a mode using "hanetconfig create" command with -m option.

3.1.2 Selecting appropriate contents

Select appropriate contents for each mode.

3.1.2.1 Fast switching mode

When using Fast switching mode, determine the information required for configuration of the mode listed in the [Table 3.2 Configuration information of Fast switching mode](#).

Table 3.2 Configuration information of Fast switching mode

| Components | | |
|---|--|-------------------------|
| Virtual interface information (1) | Virtual interface name | |
| | Virtual IP address or host name | |
| | Subnet mask | |
| | Physical interface information (1) | Physical interface name |
| | | IP address or host name |
| | | Subnet mask |
| | Physical interface information (2) | Physical interface name |
| | | IP address or host name |
| | | Subnet mask |
| | (Repeat for the number of physical interfaces) | |
| (Repeat for the number of virtual interfaces) | | |

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name

Specify a name for a virtual interface, which will be assigned to the physical interface used for redundancy. Specify shaX (X represents a number) of this component using "hanetconfig create" command with -n option.

Virtual IP address or host name

Specify an IP address or host name to be assigned for the virtual interface. The network portion (IPv4) and a prefix (IPv6) of this IP address must be different from the IP address assigned for the physical interface. When using IPv4, use "hanetconfig create" command with -i option to specify the IP address to be allocated for the virtual interface. When using IPv6, configure these in /etc/inet/ndpd.conf file.

Subnet mask

When using IPv4 address, specify the sub network mask value applied to the virtual IP address. If subnet is not used, this configuration can be omitted. This component is written in /etc/inet/netmasks file. However, this configuration is not necessary if using IPv6 address.

<Physical interface information>

Setup the followings for the number of physical interfaces used for redundancy.

Physical interface name

Specify a name for the physical interface. This component can be set using "hanetconfig create" command with -t option (e.g. hme1, qfe2 etc).

Physical IP address or host name

If using IPv4 address, specify an IP address or host name to be assigned for the physical interface. The network portion of this IP address must be different from IP address of other physical and virtual interface. Set up this component as follows:

[Solaris 10]

Create "/etc/hostname.*physical interface name*" file and then assign the IP address (or host name) in the file.

[Solaris 11 or later]

Use the ipadm(1M) command.

Make sure this value is different from the other IP.

Subnet mask

If using IPv4 address, specify a sub network mask value applied to the physical IP address. If subnet is not used for allocation, this configuration can be omitted. This configuration is written in /etc/inet/netmasks file. Note that, this configuration is not necessary if using IPv6 address.

3.1.2.2 NIC switching mode

Table 3.3 Configuration information of NIC switching mode shows the information required to configure NIC switching mode:

Table 3.3 Configuration information of NIC switching mode

| Components | | |
|---|-------------------------------------|---|
| Virtual interface information (1) | Virtual interface name | |
| | Virtual IP address (or host name) | |
| | Subnet mask | |
| | Physical interface information (1) | Physical interface name |
| | | IP address or host name |
| | Physical interface information (2) | Physical interface name |
| | Standby interface information | Virtual interface name |
| | | Automatic switching back mode |
| | | Local MAC address configured in Standby interface |
| | Monitored remote system information | Primary Monitored remote system IP address or host name |
| Secondary Monitored remote system IP address or host name | | |
| HUB-to-HUB monitoring | | |
| (Repeat for the number of physical interfaces) | | |

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name

Name a virtual interface to be configured on a physical interface used for GLS. Specify the name using "hanetconfig create" command with -n option, in "shaX" (where X is a natural number) format.

Virtual IP address or host name

Specify an IP address or host name allocated to the virtual interface. The network portion (for IPv4) or prefix (for IPv6) of this IP address must be the same IP address assigned to the physical interface. This value is specified using "hanetconfig create" command with -i option.

Subnet mask

When using IPv4 address, specify the value of a sub network mask used for the virtual IP address. This configuration can be omitted if not allocating a subnet. Set a subnet mask in /etc/inet/netmasks file. When using IPv6 address, it is not required to configure this value.

<Physical interface information>

Setup the followings for the number of physical interfaces for redundancy.

Physical interface name

Specify a name of the physical interface. This can be specified using "hanetconfig create" command with -t option. (e.g. hme1,qfe2)

Physical IP address or host name

Specify an IP address or host name assigned to the physical interface. This IP address must be different from the IP address of the other physical and virtual interfaces. Set up this component as follows:

[Solaris 10]

Create "/etc/hostname.<physical interface name>" file and then assign an IP address (or host name) in the file.

[Solaris 11 or later]

Use the ipadm(1M) command.

<Standby patrol information>

When using Standby patrol function, setup the followings. Skip this process if Standby patrol function is not used.

Virtual interface name

Specify a name to a virtual interface for standby patrol function. Specify it using "hanetconfig create" command with -n option, in "shaX" (where X is a natural number) format.

Automatic switch back mode

Setting up the Standby patrol function enables the automatic switch back function when a transfer path recovers from a failure. Specify "q" to "hanetconfig create" command with -m option for using immediate switch-back after a transfer path recovery, or "p" for using standby interface capability.

Local MAC address configured in Standby interface

If the standby patrol function is used, specify a local MAC address to be allocated to the standby interface. A local MAC address is specified in the form of: "02:XX:XX:XX:XX:XX" (where X represents a hexadecimal digit between 0 and F). The leading value "02" indicates the local MAC address, and the rest of the values can be arbitrary. However, please make sure that each MAC address should be unique within a single network. If the same MAC address is used within a network, the standby patrol may not run properly. When multiplexing the virtual networks (vsw and vnet) in Oracle VM environments, specify 0:0:0:0:0:0 to the MAC address because the virtual MAC address generated by the operating system must be used as it is.

Also, automatic configuration (-a option is omitted) is done in the following cases, because setting of local MAC address is not allowed.

- When setting the standby patrol for a virtual interface bundling tagged VLAN interfaces with Solaris 11 or later
- When setting the standby patrol for a virtual interface in the exclusive-IP zone or Kernel Zones

A local MAC address is specified using "hanetconfig create" command with -a option.

<Monitored remote system information>

Setup the following for the number of virtual interfaces. This configuration cannot be omitted.

Primary Monitored remote system IP address or host name

Specify an IP address or host name of a HUB to be monitored while primary physical interface is being used. This IP address is assigned using "hanetpoll create" command with -p option.

Secondary Monitored remote system IP address or host name

Specify an IP address or host name of a HUB to be monitored while the secondary physical interface is being used. This IP address is specified using "hanetpoll create" command with -p option. This step can be omitted. In such case, the same value as primary remote end IP address or host name is applied.

HUB-to-HUB monitoring

Indicate whether the HUB-to-HUB monitoring function should monitor a transfer path between cascaded HUBs or not, when two HUBs are used:

- on: monitor between HUBs,
- off: do not monitor between HUBs.

The default value is "off". Specify the value using "hanetpoll create" command with -b option.

3.1.2.3 GS/SURE linkage mode

Table 3.4 Configuration information of GS/SURE linkage mode shows the information required to configure GS/SURE linkage mode.

Table 3.4 Configuration information of GS/SURE linkage mode

| Components | | | |
|---|--|---|---|
| Virtual interface information (1) | Virtual interface name | | |
| | Virtual IP address or host name | | |
| | Subnet mask | | |
| | Physical interface information (1) | Physical interface name | |
| | | IP address or host name | |
| | | Subnet mask | |
| | Physical interface information (2) | Physical interface name | |
| | | IP address or host name | |
| | | Subnet mask | |
| | (Repeat for the number of the physical interfaces) | | |
| Virtual gateway information | Virtual gateway IP address | | |
| (Repeat for the number of the virtual interfaces) | | | |
| Remote node information (1) | Remote node name | | |
| | Virtual IP information (1) | Virtual IP address | |
| | | Remote host physical IP address information | IP address or host name (1) |
| | | | IP address or host name (2) |
| | | | (Repeat for the number of IP addresses) |
| | Monitoring on/off | | |
| | Send RIP from remote host on/off | | |
| | Network information of relaying host | | |
| (Repeat for the number of virtual IP) | | | |
| (Repeat for the number of remote nodes) | | | |

Description of each component is as follows:

<Virtual interface information>

Setup the followings for the number of virtual interfaces.

Virtual interface name

A virtual interface name is specified via "hanetconfig create" command with -n option, in "shaX" (where X is a natural number) format.

Virtual IP address or host name

Specify an IPv4 address or host name to be assigned to the virtual interface. The network portion of this IP address must be different from the IP address assigned to the physical interface. Virtual IP address or host name is specified via "hanetconfig create" command with -i option.

Subnet mask

Specify a sub network mask value applied to the virtual IP address. This procedure can be omitted if not applying a subnet. Subnet mask is specified in /etc/inet/netmasks file. When applying subnet mask, apply the same mask value to the whole virtual and physical IP.

<Physical interface information>

Setup the followings for the number of physical interfaces for redundancy.

Physical interface name

Specify a name for the physical interface. Physical interface name is specified via "hanetconfig create" command with -t option.

Physical IP address or host name

Specify an IP address or host name to be assigned to the physical interface. The network portion of this IP address must be different from the IP address allocated to the other physical and virtual interfaces. The physical IP address (or host name) is specified via -i option while executing "hanetconfig create" command with -n option. Do not create "/etc/hostname.<physical interface name>" file.

Subnet mask

Specify a sub network value applied to the physical IP address. This procedure can be omitted if not applying a subnet. Subnet mask is specified in /etc/inet/netmasks file. If using subnet mask, apply the same mask value to a whole virtual and physical IP.

<Virtual gateway information>

Setup the following for the number of virtual interfaces.

Virtual gateway IP address

Specify the IP address of the remote virtual gateway. The network (subnet) portion of the IP address should be the same as the IP address assigned to the virtual interface. This item is specified via "hanetgw create" command with -g option.

<Remote node information>

Configure the following for the number of host nodes.

Remote host name

Specify an arbitrary name (within 16 one-bit characters) to identify the node of remote host. Remote host name is specified via "hanetobserv create" command with -n option.

<Virtual IP information>

Setup the followings for the number of virtual IP.

Virtual IP address or host name

Specify a virtual IP address or host name of the remote host. The virtual IP address or host name is specified via "hanetobserv create" command with -i option. Also, the host name and IP address must be defined in /etc/inet/hosts file.

Remote host physical IP address information

Specify a physical IP address or host name in the virtual IP of the remote host. List these physical IP addresses separated by ',' (commas). Remote host physical IP address information is specified via "hanetobserv create" command with -t option. The IP address and the host name specified here must be defined in /etc/inet/hosts file as well.

Monitoring on/off

Set whether or not to use monitoring function.

on: Turn on the monitoring function from the local host

off: Does not turn on the monitoring.

If monitoring is enabled from the remote host, monitoring the remote host can be omitted. Check the configuration of the remote host and decide whether or not to turn on the monitoring function.

If the remote host (GS) is setup as a hot standby server, then define this in either active node or standby node. This configuration can be specified via "hanetobserv create" command with -m option.

Send RIP from remote host on/off

For this component, specify whether or not to send RIP packets from a remote host.

on: Awaits notification from the remote host and sends notification of the node whether the node has switched or not. After receiving RIP packets from the remote host, it sends out the notification.

off: Does not wait for notification from the remote host. It sends out a notification to every path.

Initially, this is set to "on". If the global server (GS) is setup as a hot standby server, then define this in either operation node or standby node while setting up Monitored remote system information. This configuration is specified using "hanetobserv create" command with -r option.

Caution) If the remote system is setup as a hot standby server, because RIP determines whether operational node or standby is functioning, the parameter should be set as "on".

Network information of relaying host

Specify an IP address or host name of communicating remote network. This IP address and host name must be defined in /etc/inet/hosts file. This configuration is specified using "hanetobserv create" command with -c option.

3.1.2.4 Configuration of individual mode

Table 3.5 Configuration of redundancy mode shows description of parameters for each mode. These values apply to all modes and virtual interfaces on one server. You cannot change these values for each virtual interface or redundancy mode. This configuration is not necessary when using the default value.

Table 3.5 Configuration of redundancy mode

| Contents | Fast switching mode | NIC switching mode | GS/SURE linkage mode | Default |
|---|---------------------|--------------------|----------------------|---------|
| Transfer path monitoring interval | A | N | N | 5 sec |
| The number of constant monitoring prior to outputting message | A | N | N | 0 time |
| The number of constant monitoring prior to switching cluster | A | N | N | 5 sec |
| Switching cluster immediately after starting | A | N | N | none |
| Outputting message (monitoring the physical interface) | A | N | N | none |
| Standby patrol monitoring period | N | A | N | 15 sec |
| The number of constant standby monitoring prior to outputting message | N | A | N | 3 times |
| Deactivating the standby interface | N | A | N | plumb |
| Monitoring period | N | A | A | 5 sec |
| The number of monitoring | N | A | A | 5 times |
| Recovery monitoring period | N | N | A | 5 sec |
| Cluster switching | N | A | A | Yes |
| Link up waiting period | N | A | A | 60 sec |
| Link status monitoring function | N | A | N | Enabled |

[Meaning of the symbols] A: Available, N: Not available

The followings are description of each of the content.

Transfer path monitoring interval

Specify the transfer path monitoring interval in seconds. The range of the intervals that can be specified is from 0 to 300 sec. If "0" is specified, it will not monitor the transfer path. Initially, it is set to 5 seconds. The transfer path monitoring interval is set using "hanetparam" command with -w option. This feature is available for Fast switching mode.

The number of constant monitoring prior to message output

Specify the number of times for monitoring before outputting the message (No: 800 or 801) if the message needs to be output as a transfer path failure is detected. The effective range of the numbers which can be specified is from 0 to 100. If "0" is specified, it will not output a message. Initially it is set to 0 (does not output any message). using "hanetparam" command of -m option. Note that this feature is only available for Fast switching mode.

The number of constant monitoring prior to switching cluster

Specify whether or not to switch over the cluster if a failure occurs on a whole transfer path of the virtual interface. The effective range of the numbers is from 0 to 100. it will not switch the cluster. When configuring to switch the cluster, set how many times it repeatedly monitors. The range is from 1 to 100. Initially, it is set to 5, meaning that a cluster failover is triggered after continuously detecting the same failure 5 times. This feature is specified using "hanetparam" command with -i option. This feature is available only for Fast switching.

Switching cluster immediately after starting

Specify whether or not to switch the cluster immediately after the cluster starts up. Configure this if a failure occurs in entire transfer path of the virtual interface before the system starts up. The values which can be specified are either "on" or "off". If "on" is selected, cluster is switched immediately after the userApplication starts up. On the other hand, if "off" is selected, the cluster is not switched even after the userApplication starts up. As an initial value, it is set to "off". This setting is specified using "hanetparam" command with -c option. This is available for Fast switching.

Outputting message (monitoring the physical interface)

Configure whether or not to output a message when the status of the physical interface changes (detecting a failure in transfer path or transfer path recover) in the virtual interface. The values which can be specified are either "on" or "off". If "on" is selected, a message (message number: 990, 991, 992) is output. If "off" is selected, a message is not output. Initially, it is set to "off". This setting is specified via "hanetparam" command with -s option. This is available for Fast switching.

Standby patrol monitoring period

Specify the monitoring interval (in seconds) of operational NIC for standby patrol function. The values which can be specified are from 0 to 100. If "0" is specified, it will not run monitoring. Note if the user command function (using user command when standby patrol fails or detects recovery) is enabled, do not set the parameter to "0". If the parameter is set to "0", the user command function will not work. Initially, the parameter is set to 15 (seconds). This setting is specified via "hanetparam" command with -p option. This configuration is available for NIC switching mode with standby patrol function is enabled.

The number of constant standby monitoring prior to outputting message

When a failure is detected in a transfer path using the standby patrol function, a message will be output to inform the failure. In this section, specify how many times to monitor until the message (message number: 875) is output. The values which can be specified are from 0 to 100. If "0" is selected, it stops outputting a message and disables monitoring using the standby patrol function. Note if the user command function (using user command when standby patrol fails or detects recovery) is enabled, do not set the parameter to "0". If the parameter is set to "0", the user command function will not work. Initially, the parameter is set to 3 (times). This configuration is specified via "hanetparam" command with -o option. This is available in NIC switching mode, which uses the standby patrol function. Using this option, the number of monitoring times doubles immediately after the standby patrol starts.

Deactivating the standby interface

Specify how the standby interface is deactivated. The values which can be specified are either "plumb" or "unplumb". If "plumb" parameter is specified, the standby interface is deactivated and sets "0.0.0.0" for the IP address. Specify "unplumb" in value to inactivate and delete the standby interface. Initially, the parameter is set to "plumb".

Do not specify "unplumb" for the following situations:

- When configuring high-reliable networks of a shared-IP zone with the NIC switching mode
- When configuring high-reliable LinkAggregation which the LACP mode is active with the NIC switching mode

This configuration is specified by "hanetparam" command with -d option. This is available exclusively for NIC switching mode.

Monitoring period

Specify the monitoring period in seconds. The values which can be specified are from 1 to 300. The default value is 5 (seconds). This configuration is specified by "hanetpoll on" command with -s option. This feature is available for NIC switching and GS/SURE linkage mode.

The number of monitoring

Specify the number of monitoring times. The values which can be specified are from 1 to 300. The default value is 5 (times). This configuration is specified using "hanetpoll on" command with -c option. This feature is available for NIC switching and GS/SURE mode.

Recovery monitoring period

Specify the monitoring period when a failure is detected by monitoring the remote host by GS/SURE linkage mode. The values which can be specified are from 0 to 300. The default value is 5 (seconds). This configuration is assigned via "hanetpoll on" command with -b option. This feature is available for GS/SURE linkage mode.

Cluster switching

Specify whether or not to switch the node when a failure occurs to every transfer paths.

yes: Switch nodes when a failure occurs to a whole transfer paths.

no: Does not switch nodes when a failure occurs to a whole transfer path.

The default parameter is "yes". This configuration is specified by "hanetpoll on" command with -f. This feature is available for NIC switching and GS/SURE linkage mode operating as a cluster.

Link up waiting period

In NIC switching mode, specify the time period (in seconds) until the HUB links up after monitoring starts. The values which can be specified are from 1 to 300. If this option is not specified, then the default value is used. Initial value is set to 60 (seconds). If the value is less than the product of monitoring period and monitoring times ("monitoring period" multiplied by "monitoring times"), then the value is ignored and ends up using the value of the product of monitoring period and monitoring times. This configuration is specified by "hanetpoll on" command with -p option. This feature is available for NIC switching and GS/SURE linkage mode.

Link status monitoring function

Specify whether to monitor the link state of the NICs in the virtual interface bundles. The link state is monitored at intervals set by using the -s option of the hanetpoll on command, and GLS immediately performs NIC switching when NIC link down is detected. Also, to switch NICs by detecting an error by the transfer path monitoring, check the link status of the NIC which is the destination of switching beforehand. If NIC is in link down state and the state continues for over 5 seconds (when the standby patrol is set: over 2.5 seconds), switching will be restricted. Specify this monitoring with the -l option of the hanetpoll on command. This function is enabled in NIC switching mode.

3.1.2.5 Upper limit of configuration

The following describes the upper limit of configuration in each mode.

Upper limit of redundant line control methods

The following table lists the upper limit of configuration items set in the redundant line control methods.

| Configuration item | Upper limit |
|---|-------------|
| Total number of virtual interfaces and logical virtual interfaces | 64 |



See

.....
For information on how to set the upper limit, refer to "7.1 hanetconfig Command".
.....

Upper limit of GS/SURE linkage mode

The following table lists the upper limit of configuration items set for communication host monitoring for GS/SURE linkage mode.

| Configuration item | Upper limit |
|---|-------------|
| Maximum number of virtual IP addresses (Note 1) | 64 |
| Maximum number of physical IP addresses | 128 |
| Maximum number of nodes in which a single virtual IP address can be transferred | 4 |
| Maximum number of relay destination IP addresses for TCP relay function | 256 |

Note 1)

In the environment where GLS is used in a cluster configuration, you need to configure the following virtual IP addresses as monitoring targets:

- Virtual IP address of communication target
- Virtual IP address of GLS on the cluster standby node



For information on how to set the upper limit, refer to "7.5 hanetobserv Command".

3.2 System Setup

Setup the system according to the contents determined in "3.1 Setup".



If you want to output interface operation history for the redundant line control function as syslog messages, see "3.2.3 syslog setup".

3.2.1 Checking system resources

In Redundant Line Control function, the required capacity for the shared memory and the semaphore are shown below. If these parameters are insufficient in the whole system, extend these values. For modifying the parameter, refer to the Solaris manual.

Table 3.6 Required capacity for system resources

| Resource parameter name | Required capacity | Reference (Meaning of parameter) |
|-------------------------|-------------------|---|
| project.max-shm-memory | 5888 | Number of total bytes of shared memory. |
| project.max-shm-ids | 2 | Maximum number of shared memory ID. |
| project.max-sem-ids | 1 | Maximum number of shared semaphore ID. |

3.2.2 Network configuration

3.2.2.1 Setup common to modes

(1) Verification of the physical interface

Verify if the physical interface is inserted into the system using prtconf (1M) command.

```
# prtconf -D | grep "name of the physical interface"
```

For example, to use qfe, execute the command as below:

```
# prtconf -D | grep qfe
      SUNW,qfe, instance #0 (driver name: qfe)
```

```
SUNW,qfe, instance #1 (driver name: qfe)
SUNW,qfe, instance #2 (driver name: qfe)
SUNW,qfe, instance #3 (driver name: qfe)
```

In the above example, it is possible to use qfe0, qfe1, qfe2, and qfe3. For details regarding prtconf (1M) command, refer to the Solaris manual.

If the system has no NIC installed, install a NIC. After adding a new NIC on the system, run "boot -r" command at the ok prompt, and then verify the physical interface as above.

Information

When using Tagged VLAN, ensure that the NIC supports tagged VLAN functionality (IEEE802.1Q). Refer to the documents of individual ethernet driver for configuring tagged VLAN interface. In addition, in a Redundant Line Control function, the effective range of VLAN-ID which can be specified is from 1 to 4094.

(2) Checking the name service

When using name services such as DNS or NIS, define keywords such as hosts, netmasks, and ipnodes in /etc/nsswitch.conf file to first refer to the local file. This allows to solve the address even if the DNS, NIS or LDAP sever is unreachable. The following is an example of /etc/nsswitch.conf.

```
#
# /etc/nsswitch.files:
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

passwd:      files
group:       files
hosts:       files dns
ipnodes:     files
networks:    files
protocols:   files
rpc:         files
ethers:      files
netmasks:   files
bootparams:  files
```

Note

Even when using only IPv4 address in Redundant Line Control function, please define a host name as both /etc/inet/hosts file and /etc/inet/ipnodes file.

(3) Checking the network configuration files of the OS

When setting IP addresses using the network configuration files of the OS (/etc/hostname.interface file or /etc/hostname6.interface file), it is recommended to set up as follows for hardware failure such as NIC or SB (System Board).

Fast switching mode

[Solaris 10]

Create either or both of the following files as the network configuration files for both physical interfaces for redundancy:

- /etc/hostname.interface

- /etc/hostname6.interface

[Solaris 11 or later]

Set both physical interfaces for redundancy by using the `ipadm(1M)` command.

NIC switching mode

[Solaris 10]

Create either or both of the following files as the network configuration files for either of the physical interfaces for redundancy:

- /etc/hostname.interface

- /etc/hostname6.interface

[Solaris 11 or later]

Set either of the physical interfaces for redundancy by using the `ipadm(1M)` command.

GS/SURE linkage mode

It is not necessary to create any network configuration files of physical interfaces for redundancy.

Note

Services related to the network including Redundant Line Control function will not start if all IP addresses set by `hostname.interface` or the `ipadm` command cannot be allocated due to a hardware failure on system startup.

To activate Redundant Line Control function even in the case of a hardware failure, set interfaces as shown in the following figure:

- For Solaris 10

Create the `hostname.interface` file.

- For Solaris 11 or later

Set IP addresses by the `ipadm` command.

For NIC switching mode, it is recommended to create the network configuration files so that at least one physical interface is to be activated on system startup as shown in the following figure:

Figure 3.2 Setup example of the OS setting file in the NIC switching mode (For Solaris 10)

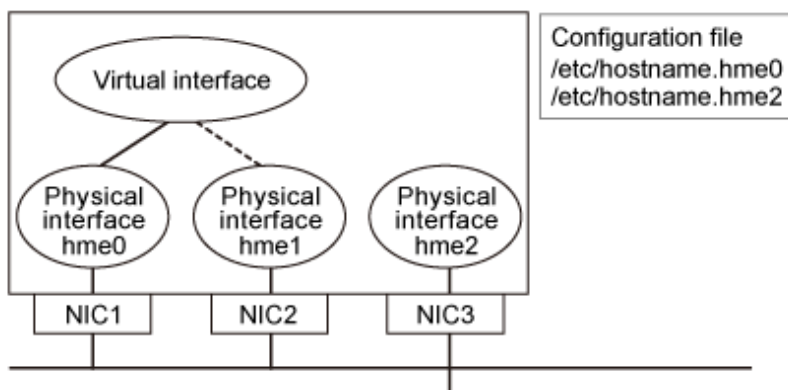
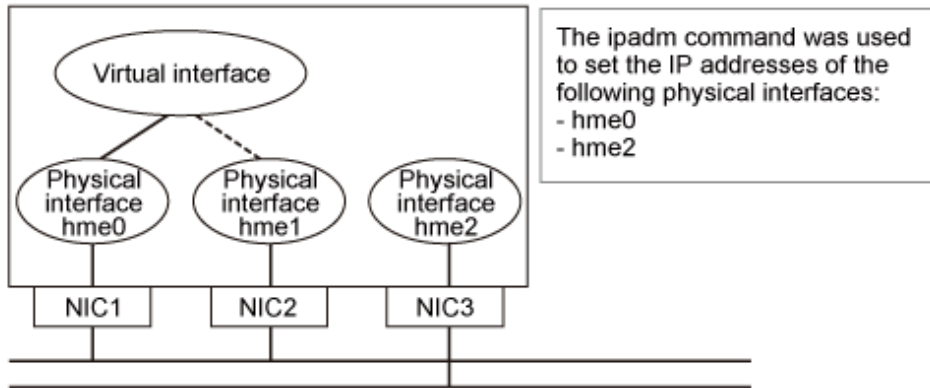


Figure 3.3 Setup example of the OS setting file in the NIC switching mode (For Solaris 11 or later)



When system boards are multiplexed or NICs with multiple ports are used, activation of the network service (svc:/network/physical) may fail because IP addresses cannot be assigned by rebooting the system while a failure occurs in the system board or the NIC. In this case, services related to the network including the service Redundant Line Control function (svc:/network/physical) will not start.

Therefore, if the a system board is multiplexed, it is recommended to set one or more physical interfaces to be activated on each system board so that at least one physical interface is to be activated on system startup as shown in the following figure.

For Solaris 10, set interfaces by creating the network configuration files.

For Solaris 11 or later, set interfaces by using the ipadm command.

If you cannot follow the procedures above due to reasons such as the small number of equipped NICs, check that the physical interface to be activated for the network configuration file has no failure before rebooting the system.

Figure 3.4 Setup example of the OS setting file in the environment with redundant system boards (For Solaris 10)

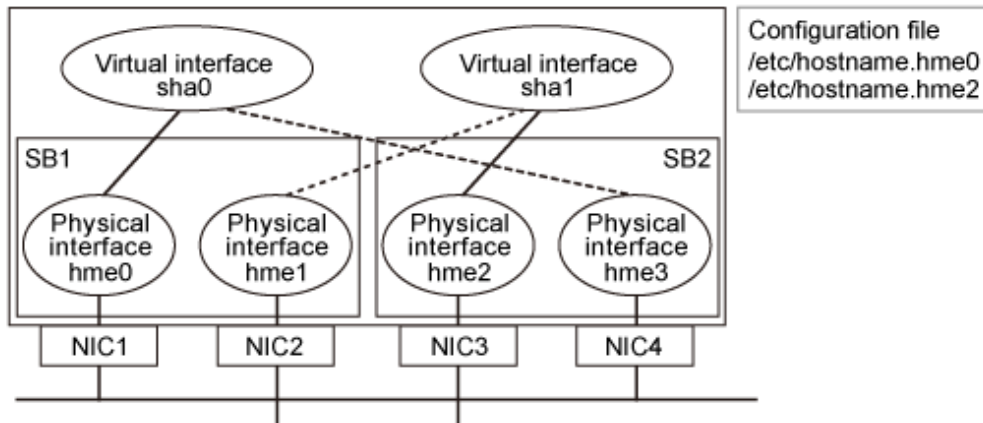
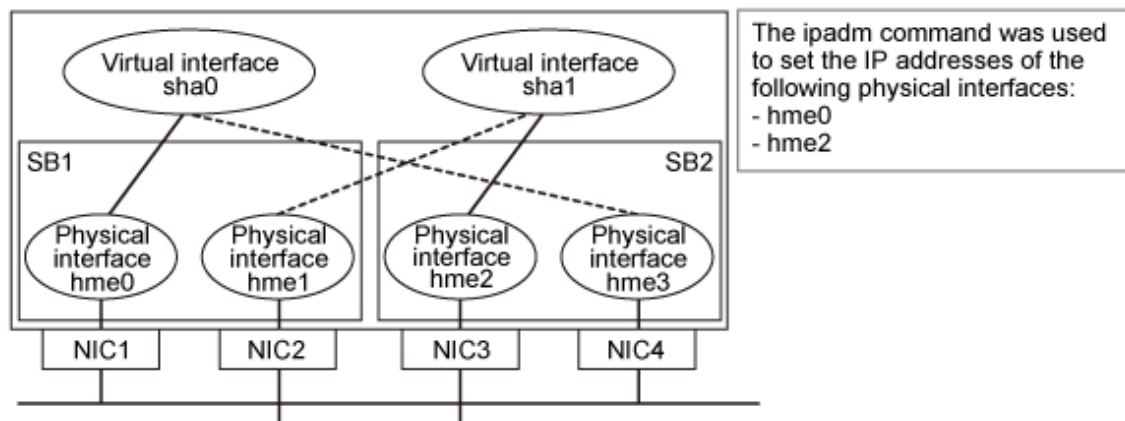


Figure 3.5 Setup example of the OS setting file in the environment with redundant system boards (For Solaris 11 or later)



In the NIC switching mode (physical IP takeover II), it is necessary to avoid IP duplication between nodes in the cluster. For Solaris 10, create an empty network configuration file to avoid IP addresses being set. When network configuration files are required, create network configuration files so that at least one physical interface other than the physical interface for redundancy is to be activated on system startup.

3.2.2.2 System setup in Fast switching mode

- When using an IPv4 address, define in the `/etc/inet/hosts` file the host names (host names to be attached to virtual IP, monitored host names to be specified in monitoring destination information, etc.) to be specified in environment definitions of Redundant Line Control function. These host names must be specified in the `/etc/inet/hosts` file even if no host names but IP addresses are directly specified in environment definitions.
- If an IPv6 address is used, define the IPv6 address and a host name in `/etc/inet/ipnodes` file.
- When using an IPv4 address, define a configured physical interface to use in IPv4 before defining a virtual interface.
[Solaris 10]
Check whether or not an `/etc/hostname.interface` file exists. If not, create it and reboot the system.
[Solaris 11 or later]
Create a physical interface by using the `ipadm(1M)` command and reboot the system.
- When using an IPv6 address, define a configured physical interface to use in IPv6 before defining a virtual interface.
[Solaris 10]
Check whether or not an `/etc/hostname6.interface` file exists. If not, create it and reboot the system. When creating a `/etc/hostname6.interface` file, make sure it is an empty file.
[Solaris 11 or later]
Create a physical interface by using the `ipadm(1M)` command and reboot the system.
- If IPv6 address is used, it is recommended to setup at least two Solaris servers running in Fast switching mode as IPv6 routers just in case an IPv6 router fails and communication cannot be achieved using a site local address. Note that if configuring IPv6 router for multiple servers, make sure these servers use the same prefix information for the virtual interface configured in `/etc/inet/ndpd.conf`. An example of setting a `/etc/inet/ndpd.conf` file when using a Solaris server as an IPv6 router is shown below. (See a Solaris manual for the detail of a `/etc/inet/ndpd.conf` file.)

```
ifdefault AdvSendAdvertisements true # Every interface sends a
router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends "Prefix
fec0:1::0/64".
```

3.2.2.3 System setup in NIC switching mode

When using IPv4 address:

- When using an IPv4 address, define in the `/etc/inet/hosts` file the host names (host names to be attached to virtual IP, monitored host names to be specified in monitoring destination information, etc.) to be specified in environment definitions of Redundant Line Control function. These host names must be specified in the `/etc/inet/hosts` file even if no host names but IP addresses are directly specified in environment definitions.
- When using an IPv4 address, define a configured primary physical interface to use in IPv4 before defining a virtual interface.
[Solaris 10]
Check whether or not an `/etc/hostname.interface` file exists. If not, create it and reboot the system.
[Solaris 11 or later]
Create a physical interface by using the `ipadm(1M)` command and reboot the system.
- For Redundant Line Control function, the path information must be initialized and the routing daemon must be restarted. If path information is statically specified, the static paths must be described in `/etc/gateways`.

When using IPv6 address:

- If an IPv6 address is used, define the IPv6 address and a host name in `/etc/inet/ipnodes` file.
- When using an IPv6 address, define a configured physical interface to use in IPv6 before defining a virtual interface.
[Solaris 10]

Check whether or not an /etc/hostname6.interface file exists. If not, create it and reboot the system. When creating a /etc/hostname6.interface file, make sure it is an empty file.

[Solaris 11 or later]

Create a physical interface by using the ipadm(1M) command and reboot the system.

- When using an IPv6 address, set an IPv6 router on a network to be connected without fail. Specify the same prefix and the same length of a prefix for an IPv6 address to be set in a Redundant Line Control function as those set in an IPv6 router.

In addition, when you use a Solaris server as an IPv6 router, please define two or more server as an IPv6 router. When abnormalities occur in an IPv6 router, it becomes impossible to perform communication which used a site local address. Therefore, it recommends defining two or more IPv6 routers. When you define an IPv6 router as two or more servers, the prefix information on the virtual interface defined as /etc/inet/ndpd.conf should define the same value in each server.

An example of setting a /etc/inet/ndpd.conf file when using a Solaris server as an IPv6 router is shown below. (See a Solaris manual for the detail of a /etc/inet/ndpd.conf file.)

```
ifdefault AdvSendAdvertisements true # Every interface sends a
router advertisement.
prefix fec0:1::0/64 hme0 # hme0 sends "Prefix
fec0:1::0/64".
prefix fec0:2::0/64 hme1 # hme1 sends "Prefix
fec0:2::0/64".
```

3.2.2.4 System setup in GS/SURE linkage mode

- When using an IPv4 address, define in the /etc/inet/hosts file the host names (host names to be attached to virtual IP, monitored host names to be specified in monitoring destination information, etc.) to be specified in environment definitions of Redundant Line Control function. These host names must be specified in the /etc/inet/hosts file even if no host names but IP addresses are directly specified in environment definitions.
- The physical interface to be specified must not be defined for normal use in TCP/IP. (Check whether or not an /etc/hostname.interface file exists. If it does, rename the file or delete it, and execute "/usr/sbin/ifconfig <interface> unplumb" command.)
- When you do not configure the virtual gateway in GS/SURE linkage mode, dynamic routing is required. When configuring dynamic routing, it is necessary to block leaks of routing information from the local system. Use the routeadm(1M) command to set up a routing daemon. The following show how to set up a routing daemon.

```
Routing daemon setup:
# routeadm -e ipv4-routing
# routeadm -s ipv4-routing-daemon="/usr/sbin/in.routed"
# routeadm -s ipv4-routing-daemon-args="-q"
# routeadm

Configuration      Current           Current
          Option   Configuration   System State
-----
IPv4 forwarding    disabled         disabled
IPv4 routing       enabled          disabled
IPv6 forwarding    disabled         disabled
IPv6 routing       disabled         disabled

IPv4 routing daemon "/usr/sbin/in.routed"
IPv4 routing daemon args "-q"
IPv4 routing daemon stop "kill -TERM `cat /var/tmp/
in.routed.pid`"
IPv6 routing daemon "/usr/lib/inet/in.ripngd"
IPv6 routing daemon args "-s"
IPv6 routing daemon stop "kill -TERM `cat /var/tmp/
in.ripngd.pid`"
# routeadm -u
```

or,

```

# routeadm -m route:default quiet_mode=true
# routeadm

```

| Configuration Option | Current Configuration | Current System State |
|----------------------|-------------------------------|----------------------|
| IPv4 routing | enabled | disabled |
| IPv6 routing | disabled | disabled |
| IPv4 forwarding | disabled | disabled |
| IPv6 forwarding | disabled | disabled |
| Routing services | "route:default ripng:default" | |

```

Routing daemons:

```

| STATE | FMRI |
|----------|--|
| disabled | svc:/network/routing/legacy-routing:ipv4 |
| disabled | svc:/network/routing/legacy-routing:ipv6 |
| online | svc:/network/routing/ndp:default |
| disabled | svc:/network/routing/rdisc:default |
| offline | svc:/network/routing/ripng:default |
| disabled | svc:/network/routing/ripng:quagga |
| online | svc:/network/routing/route:default |
| disabled | svc:/network/routing/zebra:quagga |
| disabled | svc:/network/routing/rip:quagga |
| disabled | svc:/network/routing/ospf:quagga |
| disabled | svc:/network/routing/ospf6:quagga |
| disabled | svc:/network/routing/bgp:quagga |

```

# routeadm -u

```

3.2.3 syslog setup

Set the following to output the interface up/down operation history through the redundant line control as syslog messages.

[Setting file]

/etc/syslog.conf

[Settings]

When enabling message output

Add "*.info" information to the setting file. In this setting, messages are output to the /var/adm/messages file.

```

# #ident "@(#)syslog.conf 1.4 96/10/11 SMI" /* SunOS 5.0
*/
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
#
*.err;kern.notice;auth.notice /dev/console
*.err;kern.debug;daemon.notice;mail.crit;*.info /var/adm/messages

```

When disabling message output

Delete "*.info" information from the setting file.

```

# #ident "@(#)syslog.conf 1.4 96/10/11 SMI" /* SunOS 5.0
*/
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#

```

```
# syslog configuration file.
#
#
*.err;kern.notice;auth.notice      /dev/console
*.err;kern.debug;daemon.notice;mail.crit  /var/adm/messages
```

[Setting notification]

After changing the setting file (/etc/syslog.conf), obtain the super-user rights and then issue a reread notification of the definition file to the syslog daemon (syslogd) as shown below:

(1) Example of acquiring the process ID of the syslog daemon

In the following case, 234 becomes the process ID.

```
# ps -ef | grep syslogd
root    234      1  0 17:19:04 ?        0:00 /usr/sbin/syslogd
```

(2) SIGHUP transmission

Send SIGHUP to the process (process ID=234 in the above example) obtained in (1).

```
# kill -HUP 234
```

[Others]

For details about how to set the system log, see the system online manuals. Because error messages of transfer path monitoring are output to the log at the ERROR level, there is no need to make any special settings.



Information

Messages that users need are displayed in err (system log priority), even if the message type is WARNING or INFO. Shown below are examples of messages displayed in err. For details on messages, see "[Appendix A Messages and corrective actions](#)".

```
WARNING: 87500: standby interface failed.
INFO: 88500: standby interface recovered.
INFO: 88600: recover from route error is noticed.
INFO: 88700: recover from route error is detected.
INFO: 89600: path to standby interface is established.
INFO: 89700: immediate exchange to primary interface is canceled.
WARNING: 89900: route to polling address is inconsistent.
WARNING: 92400: physical interface is not running.
WARNING: 92500: exchange interface is canceled.
```

3.3 Additional system setup

This section describes additional setup procedure for setting up the system.



Note

The configuration command of a Redundant Line Control function can be executed only when the system is operating in multi-user mode.

3.3.1 Fast switching mode

The following shows the procedure for adding configuration information for Fast switching mode. When sharing NIC used in a virtual interface of the already defined Fast switching mode and adding the configuration information, use the same procedure:

1. Create a virtual interface using "hanetconfig create" command. If NICs are shared amongst several virtual interfaces, the same pair of physical interfaces should be specified to create each of the virtual interfaces with "hanetconfig create" command. For information, see Section "[7.1 hanetconfig Command](#)".

When a shared-IP zone is used

If you want to use a virtual interface of fast switching in a shared-IP zone, it is necessary to add the configuration as follows:

1. Create a virtual interface using "hanetconfig create" command.
2. After creating the configuration information, activate the concerned virtual interface using the "strhanet" command.
3. Create a non-global zone. For information on how to create a zone, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".
4. Start the non-global zone. The logical virtual interface (sha0:X) will be added to the virtual interface (sha0) by starting the non-global zone. The IP address specified during creation of the non-global zone will be allocated.

3.3.2 NIC switching mode

The procedure to add the configuration information using NIC unused in the other virtual interfaces is as follows:

1. Set up a virtual interface using the "hanetconfig create" command. For information, see Section "[7.1 hanetconfig Command](#)".
2. Set up the standby patrol function using the "hanetconfig create" command (only if the standby patrol function is used). For information, see Section "[7.1 hanetconfig Command](#)".
3. Set up the HUB monitoring function using the "hanetpoll create" command. For information, see Section "[7.7 hanetpoll Command](#)".

The procedure to share NIC used in a virtual interface of the already defined NIC switching mode and to add the configuration information is as follows (when using an NIC sharing function):

1. Set a virtual interface with "hanetconfig copy" command. See "[7.1 hanetconfig Command](#)" for the detail.
2. Set standby patrol with "hanetconfig create" command. (Only when using a standby patrol function.) It is not necessary to set if a standby patrol function is already set in a virtual interface that already shares NIC. See "[7.1 hanetconfig Command](#)" for the detail.
3. Set the HUB monitoring function with "hanetpoll copy" command. See "[7.7 hanetpoll Command](#)" for the detail.

When a shared-IP zone is used

If you want to use a redundant physical interface of NIC switching in a shared-IP zone, it is necessary to add the configuration as follows:

1. Set up a virtual interface using the "hanetconfig create" command.
2. Set up the standby patrol function using the "hanetconfig create" command (only if the standby patrol function is used). It is not necessary to set if a standby patrol function is already set in a virtual interface that already shares NIC.
3. Set up the HUB monitoring function using the "hanetpoll create" command.
4. Specify "plumb" to deactivate a standby interface using the "hanetparam -d" command.
5. After creating the configuration information, activate the concerned virtual interface using the "strhanet" command.
6. Start the HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
7. Create a non-global zone. For information on how to create a zone, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".
8. Start the non-global zone. The logical virtual interface (hme0:X) will be added to the primary interface (hme0) from the redundant physical interface (sha0) by starting the non-global zone. The IP address specified during creation of the non-global zone will be allocated.



Note

- In NIC switching mode, physical interfaces are activated or deactivated when switching over the transfer path. However, these changes are not recorded to a log file by default. For recording logs of these processes, refer to "[3.2.3 syslog setup](#)".

- In NIC switching mode with tagged VLAN interfaces, configure the standby patrol function on only one of virtual interfaces, if multiple virtual interfaces exist on the same pair of physical interfaces, and do not configure the standby patrol function on the other virtual interfaces. Note that, in general, the standby patrol function is not need to be configured on every single virtual interface.
- You cannot build an environment in which only one NIC is shared on multiplex physical interface on NIC switching mode using tagged VLAN interface.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.
- In cluster environments other than the physical IP takeover II, do the following. For details on a cluster environment of the physical IP takeover II, see "[B.4.10 Example of the Cluster system in Physical IP address takeover function II.](#)"
[Solaris 10]
Ensure to specify the same IP address configured in "/etc/hostname.interface" when specifying physical IP addresses by "hanetconfig" command using '-i' or '-e' option.
[Solaris 11 or later]
Ensure to specify the same IP address configured with the ipadm(1M) command when specifying physical IP addresses by "hanetconfig" command using '-i' or '-e' option.
When setting a cluster environment of the physical IP takeover II on Solaris 10, create "/etc/hostname.interface" as an empty file.
- If your HUB is using STP (Spanning Tree Protocol), NIC switching occurs while a failure does not occur on a transmission route. In such a case, it is necessary to tune a monitoring parameter of the HUB monitoring function. See "[7.7 hanetpoll Command](#)" or "[G.3.3.1 Switching takes place in NIC switching mode regardless of failure at the monitoring end](#)".
- If you specify a physical interface of NIC switching for the network setting of a shared-IP zone, it is necessary to set the method of deactivating a standby interface to "plumb" using the "hanetparam -d" command (however for 4.5A00 or later, default setting is "plumb"). For details, see "[7.6 hanetparam Command](#)".

3.3.3 GS/SURE linkage mode

The following shows the procedure for adding configuration information for GS/SURE linkage mode:

1. Set up a virtual interface using the "hanetconfig create" command. For information, see Section "[7.1 hanetconfig Command](#)".
2. Set up the remote party monitoring function using the "hanetobserv create" command. For information, see Section "[7.5 hanetobserv Command](#)".
To change the monitoring period or number of monitoring times of this remote party, use "hanetpoll on" command. Refer to "[7.7 hanetpoll Command](#)" for details.
3. Configure the virtual gateway information by using the hanetgw create command. For details, see "[7.16 hanetgw Command](#)".

3.3.4 Setting parameter for individual mode

See the following procedure for using a value different from the default value indicated in section "[3.1.2.4 Configuration of individual mode](#)".

1. Use "hanetparam" command and "hanetpoll on" command for setting up the parameter.
For detailed description regarding these commands, see "[7.6 hanetparam Command](#)" or "[7.7 hanetpoll Command](#)".
2. Reboot the system.

3.4 Changing system setup

This section explains a procedure of modifying the system setup.



Note

- The configuration command of a Redundant Line Control function can be executed only when the system is operating in multi-user mode.

- Once the setup is completed for Redundant Line Control function, the information regarding the host name (host name information over host database such as /etc/inet/hosts file) cannot be changed. To modify the information on host database, remove Redundant Line Control function configuration, and modify the information on the host database, then reconfigure the system.

 **Information**

Once configuration is completed, "resethanet -s" command allows you to reflect the settings without rebooting the system. For details on this command refer to "[7.15 resethanet Command](#)".

3.4.1 Fast switching mode

The following shows the procedure for changing configuration information for Fast switching mode:

1. Inactivate the concerned virtual interface using the "stphanet" command. For information, see Section "[7.3 stphanet Command](#)".
2. Change the configuration information.
3. After changing the configuration information, activate the concerned virtual interface using the "strhanet" command. For information, see Section "[7.2 strhanet Command](#)".

The procedure to change the information of a monitoring function is as follows:

1. Change the information of a monitoring function using a "hanetparam" command. See "[7.6 hanetparam Command](#)" for the detail. In this case, it is not necessary to reactivate a virtual interface. The information becomes valid immediately after changed.
2. Reboot the system after applying changes.

The following lists the information that can be changed for Fast switching mode. No information can be changed besides the information listed below. Delete the concerned definition and add it again.

- Configuration definition information
Use the "hanetconfig" command to change the following information. For information, see Section "[7.1 hanetconfig Command](#)".
 - Host name or IP address to be attached to a virtual interface or a logical virtual interface
 - Interface names to be bundled by a virtual interface
- Monitoring function information
Use the "hanetparam" command to change the following information. For information, see Section "[7.6 hanetparam Command](#)".
 - Transfer path monitoring interval
 - The number of constant monitoring prior to outputting message
 - The number of constant monitoring prior to switching cluster
 - Timing of activating the virtual interface
 - Outputting message (monitoring the physical interface)
 - Switching cluster immediately after starting RMS

When a shared-IP zone is used

If you want to use a virtual interface of fast switching in a shared-IP zone, it is necessary to add the configuration as follows;

1. Stop the non-global zone.
2. Inactivate the concerned virtual interface using the "stphanet" command.
3. Change the configuration information.
4. Change the network settings of a non-global zone. For information on how to change the zone network settings such as virtual IP address, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".
5. After changing the configuration information, activate the concerned virtual interface using the "strhanet" command.

6. Start the non-global zone.

3.4.2 NIC switching mode

The procedure to change the configuration information, and the configuration information and the other information at the same time is as follows:

1. Stop the HUB monitoring function using "hanetpoll off" command. See "[7.7 hanetpoll Command](#)" for the detail.
2. Deactivate a virtual interface to change using a "stphanet" command. See "[7.3 stphanet Command](#)" for the detail.
3. Change the setup information and parameter. (This can be done when executing "hanetpoll on" command for changing the monitoring period, the number of monitoring times, the recovery monitoring period, the waiting time for cluster switching and a link-up.) See "[7.7 hanetpoll Command](#)" for the detail.
4. Reactivate the virtual interface that was deactivated in step 2 by using a "strhanet" command. See "[7.2 strhanet Command](#)" for the detail.
5. Start the HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
(Changes made to the monitoring period, the number of monitoring times, the monitoring recovery period, the waiting time for a cluster failover, and the waiting time for a link up are reflected when "hanetpoll on" command is executed.) See "[7.7 hanetpoll Command](#)" for the detail.

The procedure for enabling a change made on the monitoring information is as follows:

1. Stop the HUB monitoring function using "hanetpoll off" command. See "[7.7 hanetpoll Command](#)" for the detail.
2. Start the HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
(Changes made to the monitoring period, the number of monitoring times, the waiting time for a cluster failover, and the waiting time for a link up are reflected when "hanetpoll on" command is executed. For more information, refer to "changing configuration and additional information at the same time".) See "[7.7 hanetpoll Command](#)" for the detail.

The following lists the information that can be changed for NIC switching mode. No information can be changed besides the information listed below. Delete the concerned definition and add it again.

- Configuration definition information
Use the "hanetconfig" command to change the following information. For information, see Section "[7.1 hanetconfig Command](#)".
 - Host name or IP address to be attached to a virtual interface or a logical virtual interface
 - A physical interface name for the virtual interface
 - An IP address or host name of the physical interface
- Standby patrol information
Use the "hanetconfig" command to change the following information. For information, see Section "[7.1 hanetconfig Command](#)".
 - Local MAC address to be allocated to a standby NIC
 - Interface names to be bundled by a virtual interface
- Information of monitored remote system and parameters
Use the "hanetpoll" command to change the following information. For information, see Section "[7.7 hanetpoll Command](#)".
 - Information on monitored remote system (primary monitored remote system IP address and secondary monitored remote system IP address)
 - HUB-to-HUB monitoring
 - Monitoring interval
 - The number of monitoring times
 - Cluster switching
 - Link up waiting time
 - Link status monitoring function

Use the "hanetparam" command to change the following information. For information, see Section "[7.6 hanetparam Command](#)".

- Standby patrol monitoring interval
- The number of constant standby monitoring prior to outputting message

When a shared-IP zone is used

If you want to use a redundant physical interface of NIC switching in a shared-IP zone, it is necessary to add the configuration as follows:

1. Stop the non-global zone.
2. Stop the HUB monitoring function using "hanetpoll off" command.
3. Deactivate a virtual interface to change using a "stphanet" command.
4. Change the setup information and parameter. (This can be done when executing "hanetpoll on" command for changing the monitoring period, the number of monitoring times, the recovery monitoring period, the waiting time for cluster switching and a link-up.)
5. Change the network settings of a non-global zone. For information on how to change the zone network settings such as virtual IP address, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".
6. Reactivate the virtual interface that was deactivated in step 3 using "strhanet" command.
7. Start the HUB monitoring function to monitor the routers/hubs using "hanetpoll on" command.
(Changes made to the monitoring period, the number of monitoring times, the monitoring recovery period, the waiting time for a cluster failover, and the waiting time for a link up are reflected when "hanetpoll on" command is executed.)
8. Start the non-global zone.



Note

- In cluster environments other than the physical IP takeover II, do the following. For details on a cluster environment of the physical IP takeover II, see "[B.4.10 Example of the Cluster system in Physical IP address takeover function II](#)".
[Solaris 10]
Ensure to specify the same IP address configured in "/etc/hostname.interface" when specifying physical IP addresses by "hanetconfig" command using '-i' or '-e' option.
[Solaris 11 or later]
Ensure to specify the same IP address configured with the ipadm(1M) command when specifying physical IP addresses by "hanetconfig" command using '-i' or '-e' option.
When setting a cluster environment of the physical IP takeover II on Solaris 10, create "/etc/hostname.interface" as an empty file.
- For NIC sharing and tagged VLAN (synchronous switching), in a configuration in which several virtual interfaces share a single physical line, physical interfaces are also inactivated when the last virtual interface is inactivated using the stphanet command.

3.4.3 GS/SURE linkage mode

The following shows the procedure for changing configuration information for GS/SURE linkage mode:

1. Inactivate the concerned virtual interface using the "stphanet" command. For detail, see Section "[7.3 stphanet Command](#)".
2. Change the configuration information.
3. Reboot the system.
(Note: restarting the HUB monitoring function with "hanetpoll off/on" enables a change made on the monitoring interval, the number of times for monitoring, the monitoring recovery interval, the waiting time for a link up, or the waiting time for cluster switching.)

The following is a list of the information that can be changed for GS/SURE linkage mode. No information can be changed besides the information listed below. Delete the concerned definition and add it again.

- Configuration definition information
Use the "hanetconfig" command to change the following information. For information, see Section "[7.1 hanetconfig Command](#)".
 - Host name or IP address to be attached to a virtual interface or a logical virtual interface
 - Host name or IP address to be attached to a physical interface

- Interface names to be bundled by a virtual interface
- Parameters
 - Use the "hanetpoll" command to change the following information. For information, see Section "[7.7 hanetpoll Command](#)".
 - Monitoring interval
 - The number of monitoring times
 - Recovery monitoring period
 - Cluster switching
 - Link up waiting period
- Remote node information
 - Use the "hanetobserv" command to change the following information. For information, see Section "[7.5 hanetobserv Command](#)".
 - Remote node name
 - Virtual IP information (Virtual IP address, Remote physical IP address, Monitoring on/off, Send RIP from remote host on/off, Network information of relaying host)
- Virtual gateway
 - Use the "hanetgw" command to change the following information. For information, see Section "[7.16 hanetgw Command](#)".
 - Virtual gateway IP address

3.4.4 Note on changing configuration information

The following shows a note on changing configuration information.

- It is not possible to change the configuration information of a virtual interface registered to a cluster resource. It is necessary to delete the cluster resource to which the target virtual interface has been registered, and reregister the virtual interface to a cluster resource after changing the configuration information.

3.5 Deleting configuration information

This section explains procedures of deleting various definitions information such as virtual interfaces and monitoring function to be used for Redundant Line Control function.



Note

The configuration command of a Redundant Line Control function can be executed only when the system is operating in multi-user mode.



Information

Use the "resethanet" command to delete the entire configured values of the virtual interface for Redundant Line Control function. For details on "resethanet" command, refer to "[7.15 resethanet Command](#)".

3.5.1 Fast switching mode

The following shows the procedure for deleting configuration information:

1. Inactivate the concerned virtual interface using the "stphanet" command. For information, see Section "[7.3 stphanet Command](#)".
2. Delete the configuration information of the concerned virtual interface. For information, see Section "[7.1 hanetconfig Command](#)".
3. Delete the following settings and files:

When using IPv4 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname.interface` file, and then delete host names defined in the `/etc/inet/hosts` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/hosts`.

When using IPv6 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname6.interface` file, and then delete host names defined in the `/etc/inet/ipnodes` file. Moreover, delete a router public-relations setup from the virtual interface defined in the `/etc/inet/ndpd.conf` file. When only a router public-relations setup from a virtual interface exists in a `/etc/inet/ndpd.conf` file, delete the `/etc/inet/ndpd.conf` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/ipnodes` file. Moreover, delete a router public-relations setup from the virtual interface defined in the `/etc/inet/ndpd.conf` file. When only a router public-relations setup from a virtual interface exists in a `/etc/inet/ndpd.conf` file, delete the `/etc/inet/ndpd.conf` file.

When a shared-IP zone is used

If a virtual interface of fast switching has been used in a shared-IP zone, it is necessary to delete the configuration as follows;

1. Stop the non-global zone.
2. Inactivate the concerned virtual interface using the "stphanet" command.
3. Delete the configuration information of the concerned virtual interface.
4. Delete the following settings and files:

When using IPv4 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname.interface` file, and then delete host names defined in the `/etc/inet/hosts` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/hosts`.

When using IPv6 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname6.interface` file, and then delete host names defined in the `/etc/inet/ipnodes` file. Moreover, delete a router public-relations setup from the virtual interface defined in the `/etc/inet/ndpd.conf` file. When only a router public-relations setup from a virtual interface exists in a `/etc/inet/ndpd.conf` file, delete the `/etc/inet/ndpd.conf` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/ipnodes` file. Moreover, delete a router public-relations setup from the virtual interface defined in the `/etc/inet/ndpd.conf` file. When only a router public-relations setup from a virtual interface exists in a `/etc/inet/ndpd.conf` file, delete the `/etc/inet/ndpd.conf` file.

5. Delete the zone or change the zone network settings. For information on how to change the zone network settings or delete the zone, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".

3.5.2 NIC switching mode

The following shows the procedure for deleting configuration information:

1. Use the "hanetpoll off" command with '-n' option to stop the HUB polling feature of the virtual interface targeted for deletion. This command, "hanetpoll off" with '-n' option allows you to stop the virtual interface by specifying them individually. For information, see Section "[7.7 hanetpoll Command](#)".
2. Inactivate the virtual interface of the concerned NIC switching mode using the "stphanet" command. To delete the operated definition in a cluster system, deactivate a virtual interface of the standby patrol using the "stpctl" command (only when using a standby patrol function). For information, see Section "[7.3 stphanet Command](#)" and Section "[7.11 stpctl Command](#)".
3. Delete the concerned monitoring destination information. For information, see Section "[7.7 hanetpoll Command](#)".

4. Delete the configuration information of the concerned virtual interface. For information, see Section "[7.1 hanetconfig Command](#)".
5. Delete the following settings and files:

When using IPv4 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname.interface` file, and then delete host names defined in the `/etc/inet/hosts` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/hosts`.

When using IPv6 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname6.interface` file, and then delete host names defined in the `/etc/inet/ipnodes` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/ipnodes` file.

When a shared-IP zone is used

If a redundant physical interface of NIC switching has been used in a shared-IP zone, it is necessary to delete the configuration as follows;

1. Stop the non-global zone.
2. Use the "hanetpoll off" command with '-n' option to stop the HUB polling feature of the virtual interface targeted for deletion. This command, "hanetpoll off" with '-n' option allows you to stop the virtual interface by specifying them individually.
3. Inactivate the virtual interface of the concerned NIC switching mode using the "stphanet" command.
If the logical IP address takeover function is set, disable a virtual interface of standby patrol using the "stpctl" command. (only for standby patrol)
4. Delete the concerned monitoring destination information.
5. Delete the configuration information of the concerned virtual interface.
6. Delete the following settings and files:

When using IPv4 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname.interface` file, and then delete host names defined in the `/etc/inet/hosts` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/hosts`.

When using IPv6 addresses

[Solaris 10]

Delete the corresponding `/etc/hostname6.interface` file, and then delete host names defined in the `/etc/inet/ipnodes` file.

[Solaris 11 or later]

Delete the settings by using the `ipadm(1M)` command, and then delete host names defined in the `/etc/inet/ipnodes` file.

7. Change the network settings of non-global zones or delete non-global zones. For information on how to change delete non-global zones, see "[C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones](#)".

3.5.3 GS/SURE linkage mode

The following shows the procedure for deleting configuration information:

1. Inactivate the concerned virtual interface using the "stphanet" command. For information, see Section "[7.3 stphanet Command](#)".
2. Delete virtual gateway information. For information, see "[7.16 hanetgw Command](#)".

3. Delete the monitoring destination information of the concerned communication parties. For information, see Section "[7.5 hanetobserv Command](#)".
4. Delete the configuration information of the concerned virtual interface. For information, see Section "[7.1 hanetconfig Command](#)".
5. Delete the host name defined as the /etc/inet/hosts file.
6. Reboot the system.

3.5.4 Note on deleting configuration information

The following shows a note on deleting configuration information.

- "hanetconfig delete" command cannot delete a virtual interface that has been used to create a take over IP address resource via "hanethvrsc create" command. In order to delete the virtual interface, use "hanethvrsc delete" command first to delete the take over IP address resource that is created with the target virtual interface, and then issue "hanetconfig delete" command to delete the virtual interface. Refer to "[7.14 hanethvrsc Command](#)" for the deletion method of a resource for a virtual interface.
- If deleting all configuration information at once, use the "resethanet" command. See "[7.15 resethanet Command](#)" for detail.

3.6 Setting Option Function

3.6.1 Configuring multiple virtual interfaces

Use the "hanetconfig" command to set the multiple virtual interfaces setting function. For details about this command, see "[7.1 hanetconfig Command](#)".

3.6.2 Switching cluster when all the transfer paths fails

In Fast switching mode, execute "hanetparam" command to switch the cluster when failure occurs in the whole transfer path, See "[7.6 hanetparam Command](#)" for detail.

Additionally, if failure occurs in the whole transfer path in NIC switching and GS/SURE linkage modes, use the "hanetpoll" command to switch the cluster. See "[7.7 hanetpoll Command](#)" for detail.

3.6.3 Sharing physical interface

Use the "hanetconfig" command to set the physical interface sharing function. For details about this command, see the execution examples in Section "[7.1 hanetconfig Command](#)".

3.6.4 Multiple logical virtual interface definition

Use the "hanetconfig" command to set the multiple logical virtual interface definition function. For details about this command, see the execution examples in Section "[7.1 hanetconfig Command](#)".

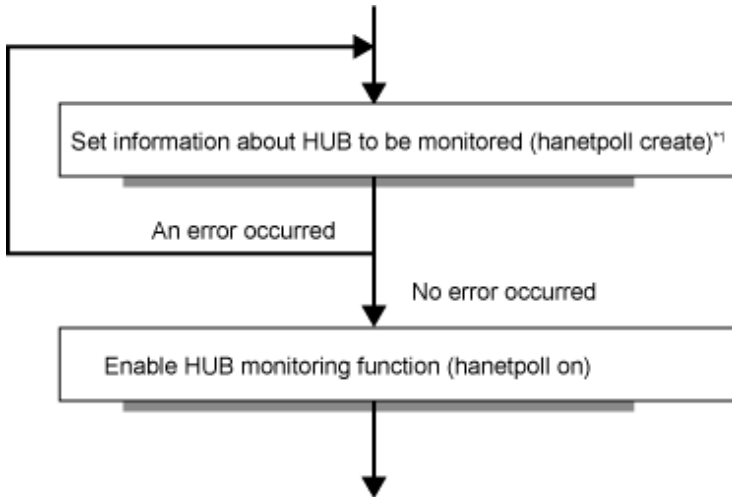
3.6.5 Single physical interface definition

Use the "hanetconfig" command to set the single physical interface definition function. For details about this command, see the execution examples in Section "[7.1 hanetconfig Command](#)".

3.6.6 HUB monitoring function

Set the HUB monitoring function for the operation in NIC switching mode. Set the HUB monitoring function in accordance with the following procedure:

Figure 3.6 Setting procedure of the HUB monitoring function



*1: If multiple virtual interfaces for NIC switching mode exist, be sure to configure the remote host information on each virtual interface.

3.6.6.1 Creating monitoring information

Create the monitoring information of the HUB monitoring function. Use the "hanetpoll" command for this setting. For details about this command, see Section "7.7 hanetpoll Command".

3.6.6.2 Enabling HUB monitoring function

Enable the HUB monitoring function.

Use the "hanetpoll on" command to set up this function. If the "hanetpoll on" command is executed, the ping command is executed on the HUB.

Note

In NIC switching mode, no line failure is assumed even if the ping command fails until the link up wait time (IDLE (seconds) in [Figure 3.7 Basic sequence of HUB monitoring](#)) passes. This is because monitoring starts after a physical interface is activated. Time required for link up depends on the HUB type to be connected. If the line monitoring fails although the HUB is not faulty, extend the wait time as required, using the -p parameter of the "hanetpoll on" command.

If the "hanetpoll on" command is executed while the virtual interface with monitoring destination information specified is activated, the monitoring function is immediately enabled.

If the "hanetpoll" command is executed while the virtual interface with monitoring destination information specified is not activated, the HUB monitoring function is not enabled.

If, after the HUB monitoring function is enabled, the virtual interface with monitoring destination information specified is activated, the HUB monitoring function is not enabled. In this case, disable the HUB monitoring function, activate the virtual interface, and enable the HUB monitoring function again. For more information, see Section "7.7 hanetpoll Command".

Figure 3.7 Basic sequence of HUB monitoring

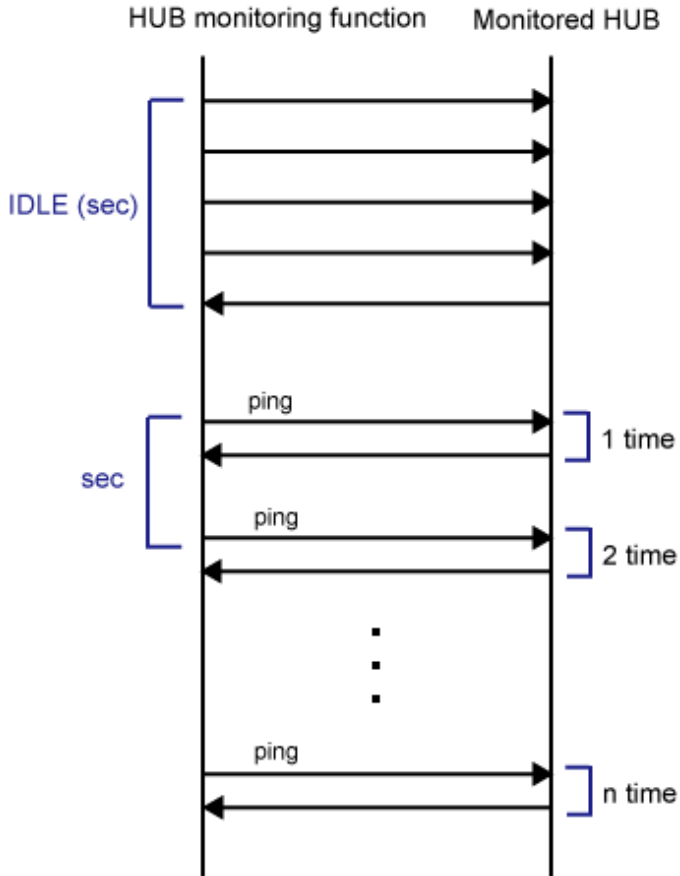
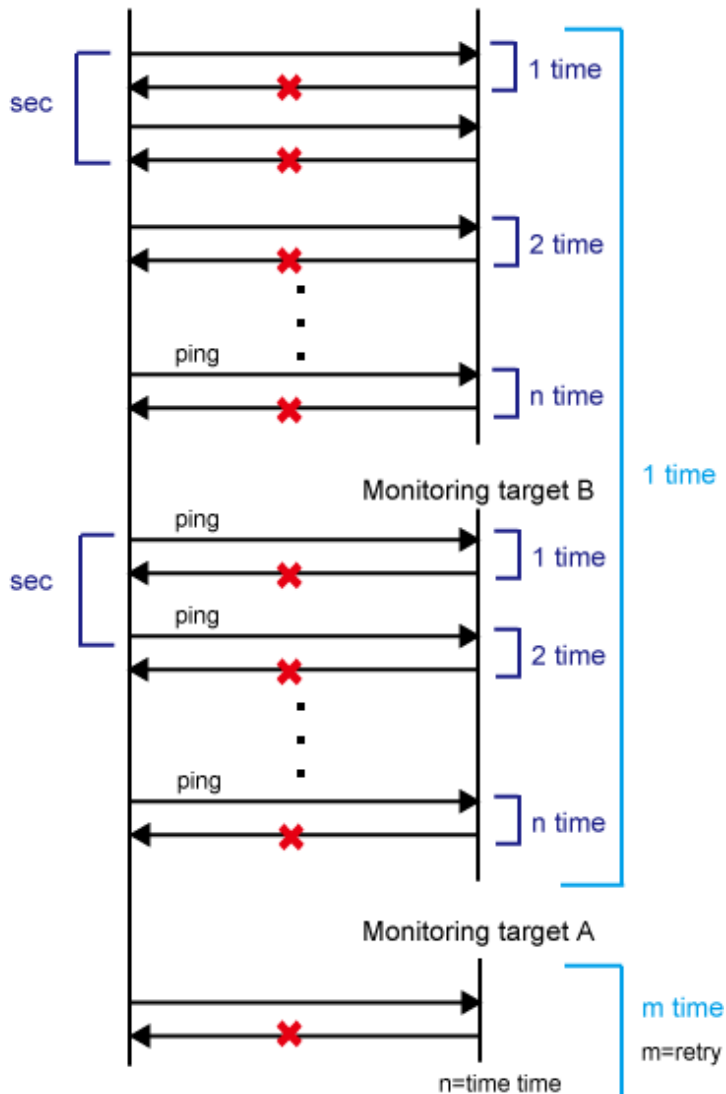


Figure 3.8 HUB monitoring sequence after detect line fault
HUB monitoring function Monitoring target A



3.6.6.3 Transfer route error detection time for NIC switching mode

This section describes on transfer route error detection sequence of HUB monitoring feature on NIC switching mode.

The followings are examples of the case of one monitoring target and two monitoring targets. There is only one monitoring destination when the HUB-to-HUB monitoring is disabled on the dual NIC configuration, or when a single HUB monitoring destination is set on a single NIC configuration. There are two monitoring destinations when the HUB-to-HUB monitoring is enabled, or when two monitoring destinations are set on a single NIC configuration.

One monitoring destination:

$$\text{Error detection time} = \text{monitoring interval (in seconds)} \times (\text{monitoring frequency} - 1) + \text{ping time out period (*1)}$$

*1: If the monitoring interval is 1 second, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

The default value would look like the following.

$$5 \text{ sec} \times (5 \text{ times} - 1) + 2 \text{ sec} = 22 \text{ sec}$$

Two monitoring destinations:

Error detection time = monitoring interval (in seconds) x (monitoring frequency - 1) + ping time out period (*2)
x 2

*2: If the monitoring interval is 2 seconds, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

The default value would be like the following.

$$5 \text{ sec} \times (5 \text{ times} - 1) + 2 \text{ sec} \times 2 = 24 \text{ sec}$$

Figure 3.9 Transfer path error detection sequence (one monitoring destination)

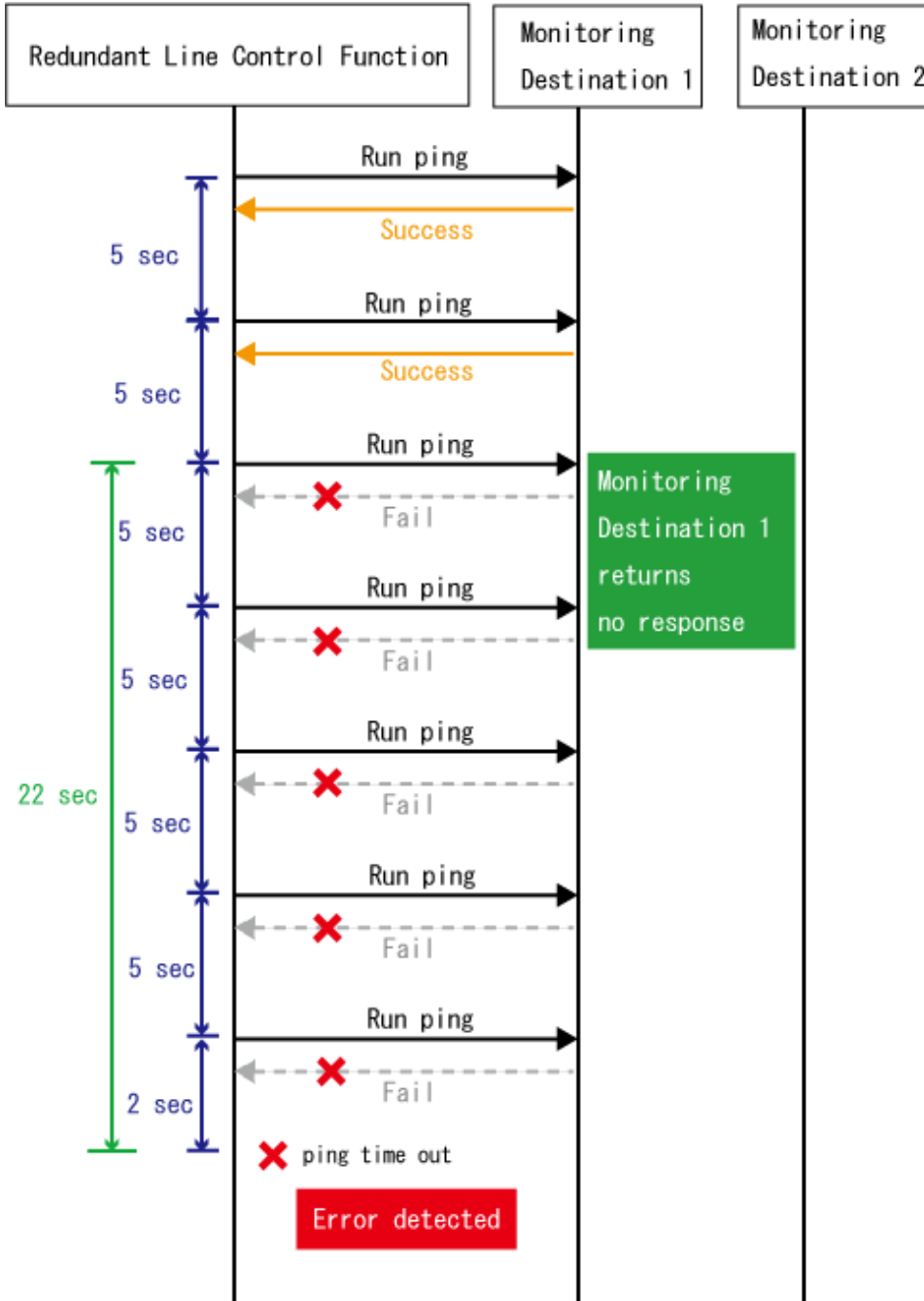
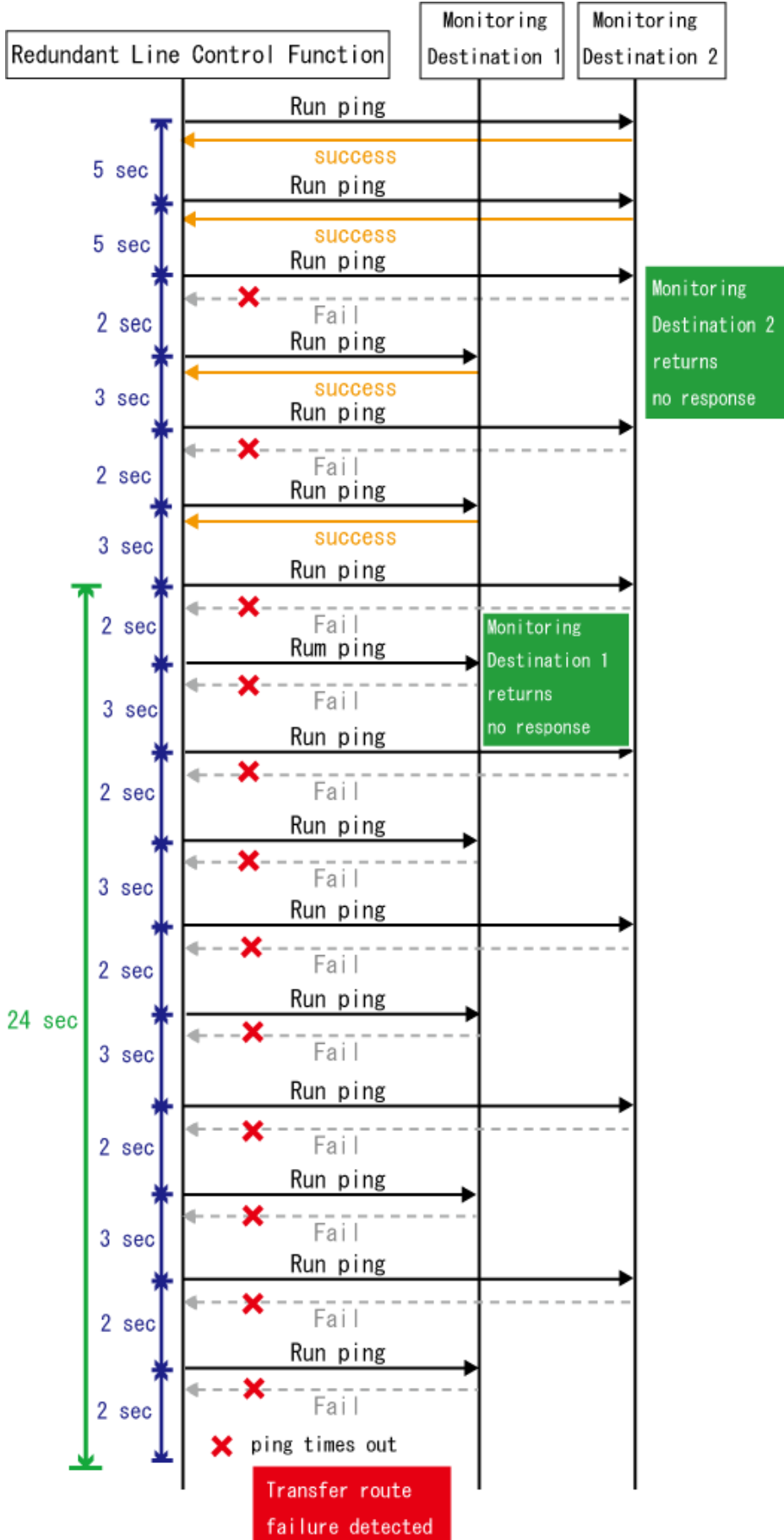


Figure 3.10 Transfer path error detection sequence (two monitoring destination)



If the link status monitoring function is enabled, the link state is checked immediately after a ping failure to the primary monitoring destination (monitoring destination 1). If the link is down, the link status monitoring function determines that the transfer route failed.

One monitoring destination:

$$\text{Error detection time} = \text{ping time out period}(*3) + (0 \text{ to monitoring interval (in seconds)})$$

*3: If the monitoring interval is 1 second, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

The default value would look like the following.

$$2 \text{ sec} + 0 \text{ to } 5 \text{ sec} = 2 \text{ to } 7 \text{ sec}$$

Two monitoring destinations:

$$\text{Error detection time} = \text{ping time out period}(*4) \times 2 (0 \text{ to monitoring interval (in seconds)})$$

*4: If the monitoring interval is 2 seconds, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

The default value would be like the following.

$$2 \text{ sec} \times 2 \text{ time} + 0 \text{ to } 5 \text{ sec} = 4 \text{ to } 9 \text{ sec}$$

Figure 3.11 Transfer path error detection sequence with link down (one monitoring destination)

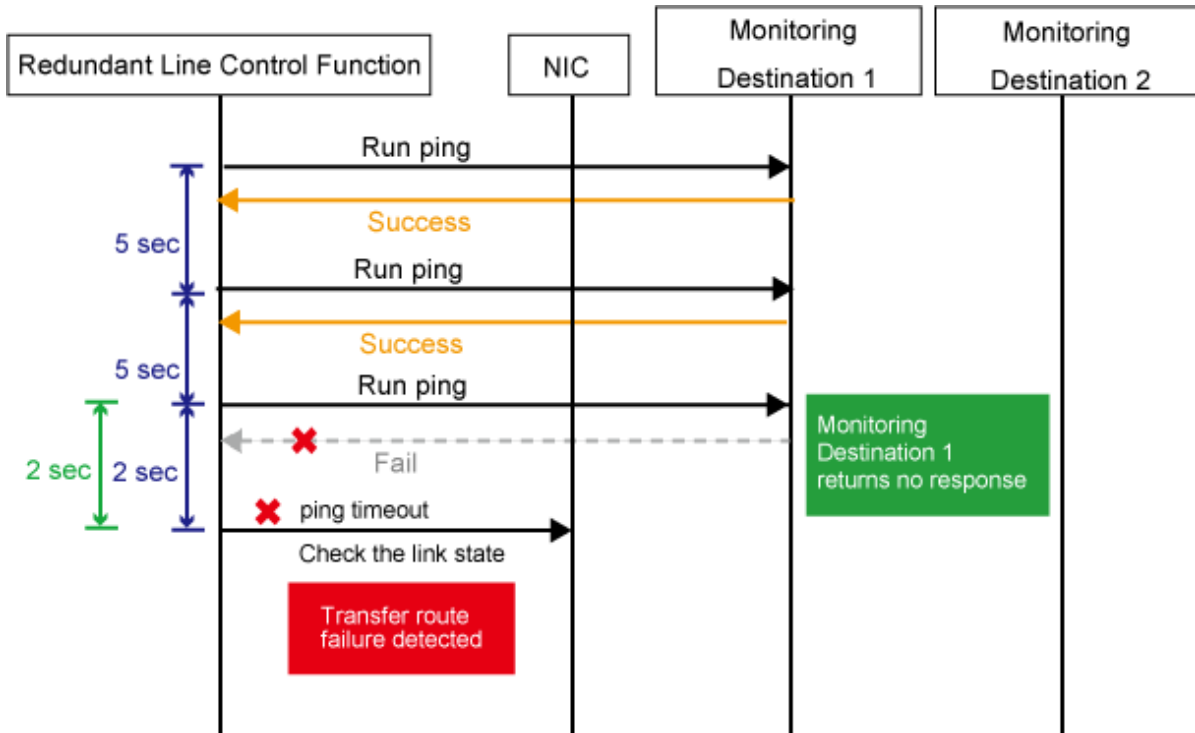
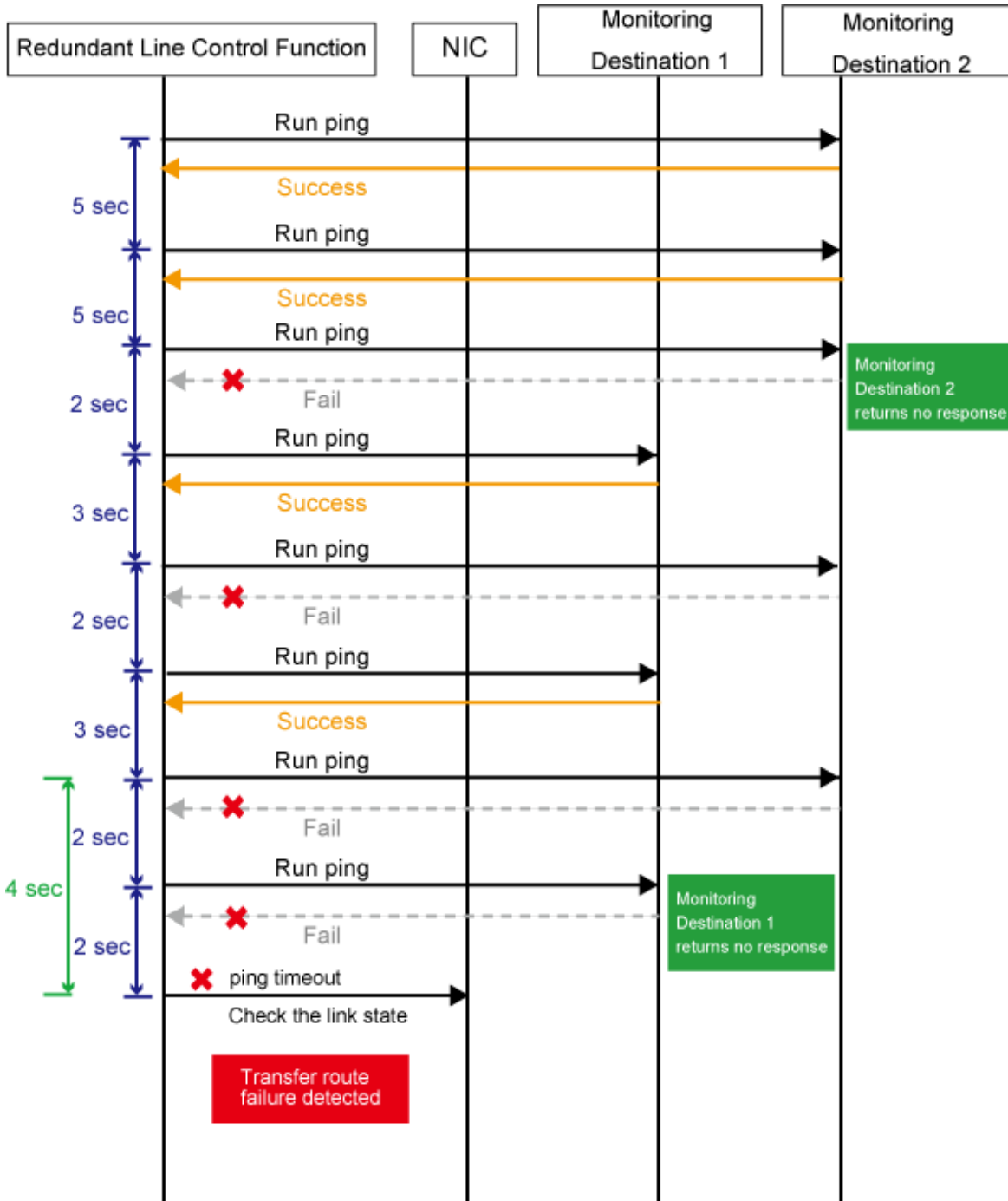


Figure 3.12 Transfer path error detection sequence with link down (two monitoring destinations)



Information

- Since ping monitoring is performed at regular intervals (in seconds), the maximum interval of time is required between the time the monitoring destination fails and the time the next ping is sent. Therefore, it takes at least 22 seconds and up to 27 seconds to detect the failure after a failure has occurred. In addition, if the transfer route failure due to NIC link down is detected, it takes at least 2 seconds and up to 7 seconds for GLS to detect the transfer route failure after notification (to the system log, etc) that the NIC link is down message was sent.
- Just after starting error monitoring for transfer routes, e.g. just after activation of virtual interfaces or NIC switching, error detection will be suspended until the waiting time for linkup elapses.

- In an Oracle VM environment, the NIC link down cannot be detected by the link status monitoring function. This is because the link down is not notified to a physical interface bundled by GLS and connected via a virtual switch, even if the NIC link down of the host domain is detected by the link status monitoring function. Therefore, the line will be switched after an error is detected by the HUB monitoring function instead of by the link status monitoring function. However, when setting (setting phys-state to linkprop option) to propagate the link down of physical NIC, link down can still be detected even in the Oracle VM environment for the virtual network device (vnet).
- If vnic is bundled by the NIC switching mode, the link down of a physical NIC cannot be detected with the link status monitoring function. This is because the link status of a physical NIC does not propagate to the vnic interface. Therefore, switching of transfer paths is not executed by the link status monitoring function, but is executed after detecting an error at HUB monitoring function.



Note

If no response after the ping command run for 30 seconds, the hang-up will be detected and it will be determined that an error has occurred on the transfer route before running the command again.

3.6.7 Monitoring the remote host

Sets a function to monitor if or not possible to communicate with a GS/SURE system (the other end of communication), that becomes the other end of communication when operating GS/SURE linkage mode. To set monitor-to, use the "hanetobserv" command. See "[7.5 hanetobserv Command](#)" as to how to set it. To set an interval to monitor, use the "hanetpoll" command. See "[7.7 hanetpoll Command](#)" as to how to set it.



Note

It is necessary to set GS/SURE linkage mode (the operation mode is "c") before executing this setting.

If the local system is running on a clustered system, it switches a node when GS/SURE system (remote host) stops. During this process, if no response is returned from any of the defined monitored remote system by executing "hanetobserv" command, it is recognized as a local NIC failure and it switches the node. Moreover, even though all the GS/SURE system (remote host) stops operating, all monitored remote system does not return responses, and there occurred an unnecessary switching. To avoid this, it is possible to interoperate operational node and standby node to monitor network failures. So that if all the remote system stops operating, it does not mistakenly switch the node.

If operating the cluster, use the "hanetobserv" command to monitor from both operational node and standby command. Keep in mind that since it is necessary to identify the remote node from both operational and standby node, a take over IP address must be used for a virtual IP address.

3.6.7.1 Transfer route error detection time in GS/SURE linkage mode

This section describes the transfer route error detection sequence.

In GS/SURE linkage mode, issue the ping command for the real IP address of a target that you set with the remote host monitoring function and for the IP addresses of other nodes in the cluster. The time it takes for an error to be detected is as follows:

Error detection time:

```
Error detection time = monitoring interval (in seconds) x (monitoring frequency - 1) +
ping time out period (*1)
```

*1: If the monitoring interval is 1 second, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

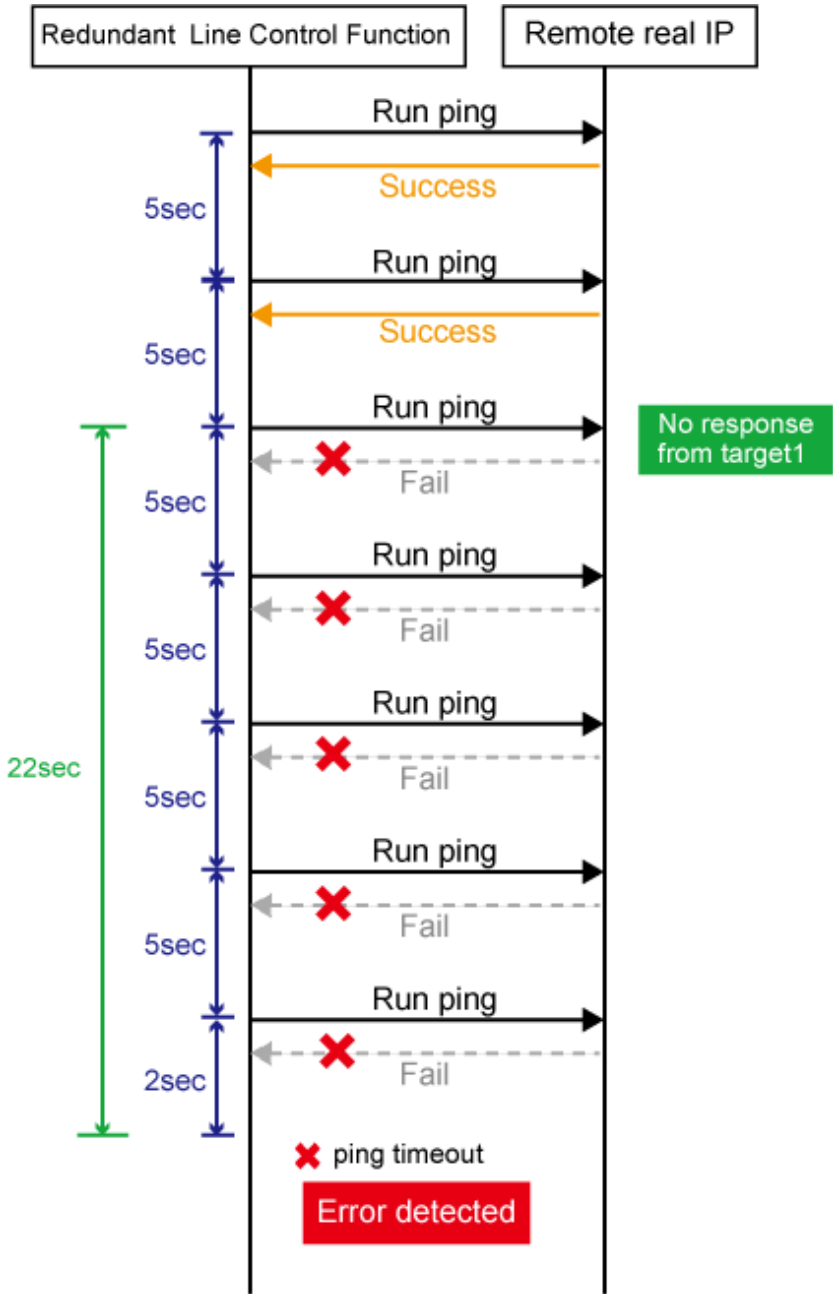
The default value would look like the following:

5 sec x (5 times - 1) + 2 sec = 22 sec

Note that if the target detects an error first, it will determine that an error has occurred on the transfer route without waiting for the error detection by ping monitoring.

The settings for the error detection time can be changed by using the "hanetpoll" command. For more details on how to make settings, see "7.7 hanetpoll Command".

Figure 3.13 Transfer path error detection sequence



Information

- Ping monitoring is performed at regular intervals (in seconds). The maximum interval of time required between the time the monitoring destination fails and the time the next ping is sent. Therefore, it takes up to 27 seconds (22 seconds + 5 seconds by default) to detect the failure after a failure has occurred.

- If applications monitor the network, configure the monitoring time so that an error should not be detected while Redundant Line Control function is switching the transfer route.

 **Note**

If no response after the ping command run for 30 seconds, the hang-up will be detected and it will be determined that an error has occurred on the transfer route before running the command again.

3.6.7.2 Transfer route recovery detection time in GS/SURE linkage mode

This section describes the transfer route recovery detection sequence.

In GS/SURE linkage mode, issue the ping command for the real IP address of the target that you set with the remote host monitoring function. After the transfer route error has been detected, Redundant Line Control function performs recovery monitoring by ping to monitor the state of the recovery of transfer route. The time it takes for recovery to be detected is as follows:

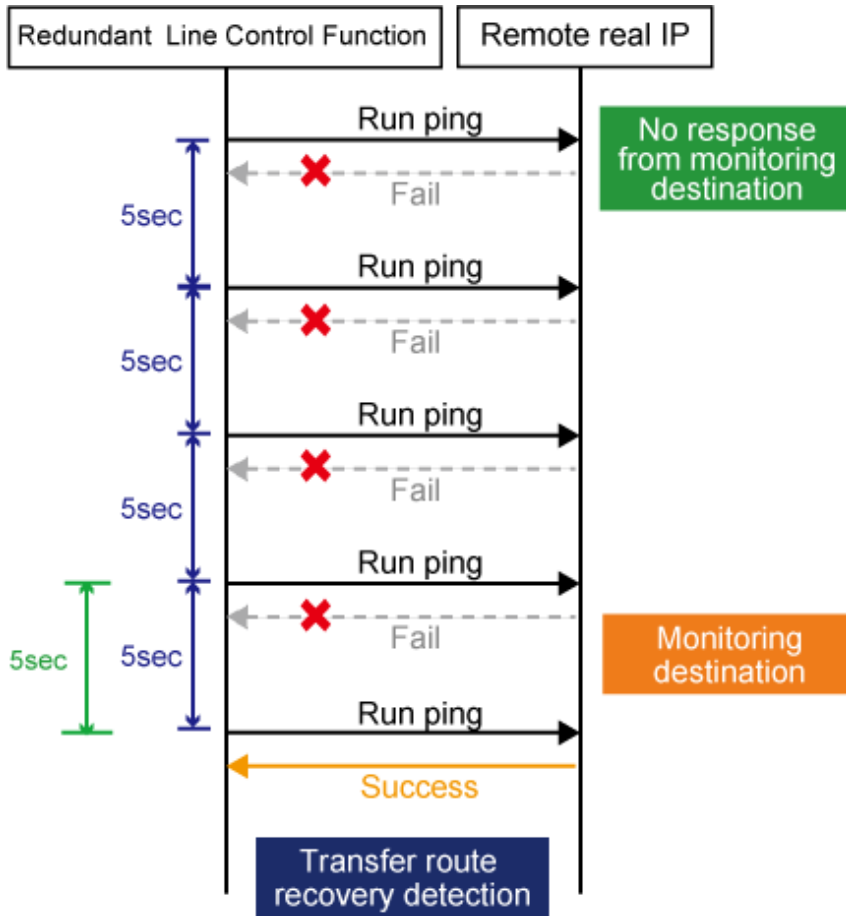
Recovery detection time:

| |
|---|
| Recovery detection time = recovery monitoring interval (in seconds) |
|---|

Note that if the target detects the recovery first, it will determine that the transfer route has recovered without waiting for the recovery detection by ping monitoring.

The settings for the error detection time can be changed by using the "hanetpoll" command. For more details on how to make settings, see "[7.7 hanetpoll Command](#)".

Figure 3.14 Transfer path recovery detection sequence



3.6.8 Standby patrol function

3.6.8.1 Setting what to be monitored

It is possible to set a function to monitor the state of a standby interface in non-activated condition when operating NIC switching mode. It is also possible to set an Automatic failback function when a primary interface recovered using a standby patrol function. Use the "hanetconfig" command to set it. See Section "7.1 hanetconfig Command" as to how to set it.



Note

It is necessary to set a virtual interface of NIC switching mode (an operation mode is either "d" or "e") before this setting.

3.6.8.2 Setting monitoring interval

Set the monitoring interval for the standby NIC. Use the "hanetparam" command for this setting. For details about this command, see Section "7.6 hanetparam Command".

3.6.8.3 Setting error monitoring interval

Set the monitoring failure count for the standby NIC before a message is output. Use the "hanetparam" command for this setting. For details about this command, see Section "7.6 hanetparam Command".

3.6.9 Setting dynamic addition/deletion/switching function of physical interfaces

3.6.9.1 Dynamic addition of physical interfaces

In Fast switching mode and GS/SURE linkage mode, it is possible to add an actual interface to be redundant while keeping a virtual interface activated. This is called "Dynamic addition of an actual interface". To add dynamically, use the "hanetnic add" command. See "[7.9 hanetnic Command](#)" as to how to set.

3.6.9.2 Dynamic deletion of physical interfaces

In Fast switching mode and GS/SURE linkage mode, it is possible to delete a redundant actual interface while keeping a virtual interface activated. This is called "Dynamic deletion of an actual interface". To delete dynamically, use the "hanetnic delete" command. See "[7.9 hanetnic Command](#)" as to how to set.

3.6.9.3 Dynamic switching of physical interfaces

In NIC switching mode, it is possible to switch a using actual interface from an operation system to a standby system while keeping the operation state. This is called "dynamic switching of an actual interface". To change dynamically, use the "hanetnic change" command. See "[7.9 hanetnic Command](#)" as to how to set.

3.6.10 Setting User command execution function

A user-defined command can be executed at a specific timing. For information on execution timing, see "[2.2.11 User command execution function](#)". In NIC switching mode, this function can be used to flush an ARP table, change the interface status, and change the MTU length, etc. In GS/SURE linkage mode, this function can be used to send a signal to a specific process, etc. The following settings must be made to use this function. See the sample files for information on creating a script file appropriate for a user's environment.

Sample file for NIC switching mode

- /etc/opt/FJSVhanet/script/interface/sha.interface.sam (When activating or deactivating an IP address)
- /etc/opt/FJSVhanet/script/failover/sha.failover.sam (When detected an error in a transfer route)
- /etc/opt/FJSVhanet/script/patrol/sha.patrol.sam (When detected a standby patrol error or recovery)

Sample file for GS/SURE linkage mode

- /etc/opt/FJSVhanet/script/host/host.sam

Sample file of the service for Redundant Line Control function

- /etc/opt/FJSVhanet/script/service.sh.sam (When the service is started)
- /etc/opt/FJSVhanet/script/system/monitor.sam (When an error is detected by the self-checking function)

[Setup files]

The storage destination and file name of a setup file varies depending on the type and name of a virtual interface.

Setup file for NIC switching mode

- /etc/opt/FJSVhanet/script/interface/shaX (When activating or deactivating an IP address)
- /etc/opt/FJSVhanet/script/failover/shaX (When detected an error in a transfer route)
- /etc/opt/FJSVhanet/script/patrol/shaY (When detected a standby patrol error or recovery)
- * shaX is the created virtual interface name for NIC switching mode.
- * shaY is the created virtual interface name of the standby patrol for NIC switching mode.

Setup file for GS/SURE linkage mode

- /etc/opt/FJSVhanet/script/host/hostIP

* hostIP is the host name or IP address of the virtual interface of the communication target.

However, pay attention to the following point when using the host name:

If the same IP address is defined to two or more host names in the /etc/inet/hosts file, use the host name which is defined in the beginning of the hosts file.

Setup file of the service for Redundant Line Control function

- /etc/opt/FJSVhanet/script/service.sh (When the service is started)

- /etc/opt/FJSVhanet/script/system/monitor (When an error is detected by the self-checking function)

Note

- Do not call the operational command for redundancy line control function in the script file.
- The commands executed in the script file do not output messages to the standard output. When checking for the contents of the output messages, use the "logger(1)" command of the operating system to output the messages to syslog.
- In a clustered system, the script for NIC switching mode of activating or deactivating IP addresses is executed only by active node. It will not run for standby node.

Information

GLS is unaffected by the exit code of the script file because GLS does not refer the exit code.

3.6.10.1 Settings for NIC switching mode

The following shows the script file call format and the definition file sample for the operation in NIC switching mode.

(1) When activated or deactivated an IP address

[Script file call format]

```
/bin/sh shaX param1 param2 param3 param4
```

param1

activate: Activation of a take over IP address

inactivate: Inactivation of a take over IP address

create: Activation of a physical NIC (logical IP takeover only)

delete: Inactivation of a physical NIC (logical IP takeover only)

param2

before: Before activation or deactivation

after: After activation or deactivation

param3

ifname: Physical interface name

param4

inet6: Address family (IPv6 only)

* No param4 for IPv4.

[Definition file sample]

```
#!/bin/sh
#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2011
#
```

```

#ident "%W% %G% %U% - FUJITSU"
#
#
# Control interface for HA-Net
#
#
# Params
#
# $1 activate or inactivate or create or delete
# $2 before or after
# $3 physical interface name
# $4 address family (IPv6 only)
#
#
# Set Params
#
INTERFACE=$3
#IP_ADDR1="xx.xx.xx.xx"
#IP_ADDR2="yy.yy.yy.yy"
#MAC_ADDR1="xx:xx:xx:xx:xx:xx"
#MAC_ADDR2="yy:yy:yy:yy:yy:yy"
#
#
# cace $# in
# 3)
# ADDRESS_FAMILY="inet"
# ;;
# 4)
# if [ $4 = "inet6" ]
# then
# ADDRESS_FAMILY="inet6"
# else
# ADDRESS_FAMILY="unknown"
# fi
# ;;
# *)
# ADDRESS_FAMILY="unknown"
# ;;
# esac
#
# if [ $ADDRESS_FAMILY = "inet" ]
# then
#
# case "$1" in
# 'activate')
#
# #
# # Activate interface
# #
#
# case "$2" in
# 'before')
#
# #
# # script before activate interface
# #
#
# # logger -p daemon.notice "execute script before activate interface on"
# $INTERFACE
# #if [ ! $INTERFACE = "hmeX" ]
# #then

```

```

#   ifconfig $INTERFACE ether $MAC_ADDR1
#else
#   ifconfig $INTERFACE ether $MAC_ADDR2
#fi
;;

'after')
#
# script after activate interface
#

# logger -p daemon.notice "execute script after activate interface on"
$INTERFACE

#if [ ! $INTERFACE = "hmeX" ]
#then
#   arp -d $IP_ADDR1
#   ping $IP_ADDR2 2
#else
#   arp -d $IP_ADDR2
#   ping $IP_ADDR1 2
#fi

;;

*)
    ;;
esac

;;

'inactivate')
#
# inactivate interface
#

case "$2" in
'before')
#
# script before inactivate interface
#

# logger -p daemon.notice "execute script before inactivate interface on"
$INTERFACE
;;

'after')
#
# script after inactivate interface
#

# logger -p daemon.notice "execute script after inactivate interface on"
$INTERFACE

;;

*)
    ;;
esac

;;

'create')

```



```

#
# create physical interface (logical IP takeover only)
#

case "$2" in
'before')
#
# script before create interface
#

# logger -p daemon.notice "execute script before create interface on"
$INTERFACE
;;

'after')
#
# script after create interface
#

# logger -p daemon.notice "execute script after create interface on" $INTERFACE
;;

*)
    ;;
esac

;;

'delete')
#
# delete physical interface (logical IP takeover only)
#

case "$2" in
'before')
#
# script before delete interface
#

# logger -p daemon.notice "execute script before delete interface on"
$INTERFACE
;;

'after')
#
# script after delete interface
#

# logger -p daemon.notice "execute script after delete interface on" $INTERFACE
;;

*)
    ;;
esac

;;

*)
    ;;
esac

fi

```

```

if [ $ADDRESS_FAMILY = "inet6" ]
then

case "$1" in
'activate')

#
# Activate interface
#

case "$2" in
'before')
#
# script before activate interface
#

# logger -p daemon.notice "execute script before activate interface on"
$INTERFACE

;;

'after')
#
# script after activate interface
#

# logger -p daemon.notice "execute script after activate interface on"
$INTERFACE

;;

*)
    ;;
esac

;;

'inactivate')
#
# inactivate interface
#

case "$2" in
'before')
#
# script before inactivate interface
#

# logger -p daemon.notice "execute script before inactivate interface on"
$INTERFACE

;;

'after')
#
# script after inactivate interface
#

# logger -p daemon.notice "execute script after inactivate interface on"
$INTERFACE

;;

```

```

*)
    ;;

esac

;;

'create')
#
# create physical interface (logical IP takeover only)
#

case "$2" in
'before')
#
# script before create interface
#

# logger -p daemon.notice "execute script before create interface on"
$INTERFACE
;;

'after')
#
# script after create interface
#

# logger -p daemon.notice "execute script after create interface on" $INTERFACE
;;

*)
    ;;

esac

;;

'delete')
#
# delete physical interface (logical IP takeover only)
#

case "$2" in
'before')
#
# script before delete interface
#

# logger -p daemon.notice "execute script before delete interface on"
$INTERFACE
;;

'after')
#
# script after delete interface
#

# logger -p daemon.notice "execute script after delete interface on" $INTERFACE
;;

*)
    ;;

esac

```

```

;;

*)
    ;;

esac

fi

exit 0

```

(2) When detected an error in a transfer route

[Script file call format]

```
/bin/sh shaX param1 param2
```

param1

primary: Error in a Primary interface
secondary: Error in a Secondary interface
all: Error in both Primary/Secondary interfaces

param2

retryout: Retry out of the ping command
linkdown: Link-down of the interface
pinghang: Hang-up of the ping command

[Definition file sample]

```

#!/bin/sh
#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2016
#
#ident "%W% %G% %U% - FUJITSU"
#
#
# Control interface for HA-Net
#
#
# Params
#
# $1 communication line state primary/secondary/all
# $2 event exit code retryout/linkdown/pinghang
#
#
# Set Params
#
#STATE=$1
#EXIT_CODE=$2
#PROC="process_name"
#kill -15 `usr/bin/ps -e | /usr/bin/sed -n \
# -e '/'$PROC'$/s/[^0-9 \t].*//p' \
# ` > /dev/null 2>/dev/null
#
#if [ $STATE = "primary" ]
#then
# if [ $EXIT_CODE = "retryout" ]
# then

```

```

# echo "execute script Polling failover : primary retryout" > /dev/console
# elif [ $EXIT_CODE = "linkdown" ]
# then
# echo "execute script Polling failover : primary linkdown" > /dev/console
# elif [ $EXIT_CODE = "pinghang" ]
# then
# echo "execute script Polling failover : primary pinghang" > /dev/console
# fi
#fi

#if [ $STATE = "secondary" ]
#then
# if [ $EXIT_CODE = "retryout" ]
# then
# echo "execute script Polling failover : secondary retryout" > /dev/console
# elif [ $EXIT_CODE = "linkdown" ]
# then
# echo "execute script Polling failover : secondary linkdown" > /dev/console
# elif [ $EXIT_CODE = "pinghang" ]
# then
# echo "execute script Polling failover : secondary pinghang" > /dev/console
# fi
#fi

#if [ $STATE = "all" ]
#then
# if [ $EXIT_CODE = "retryout" ]
# then
# echo "execute script Polling failover : all retryout" > /dev/console
# elif [ $EXIT_CODE = "linkdown" ]
# then
# echo "execute script Polling failover : all linkdown" > /dev/console
# elif [ $EXIT_CODE = "pinghang" ]
# then
# echo "execute script Polling failover : all pinghang" > /dev/console
# fi
#fi

```

(3) When detected a standby patrol error or recovery

[Script file call format]

/bin/sh shaX param1 param2

param1

establish: Standby patrol established
recover: Standby NIC monitoring recovered
fail: Standby NIC error

param2

Physical interface name of standby NIC: Physical interface name such as hmeX
unknown: Standby NIC undecided

[Definition file sample]

```

#!/bin/sh
#
#       All Rights Reserved, Copyright (c) FUJITSU LIMITED 2011
#
#ident  "%W% %G% %U% - FUJITSU"
#
# Control interface for HA-Net
#

```

```

#
# Params
#
# $1 standby NIC state   establish/recovery/fail
# $2 standby NIC name   hmeX
#
#
# Set Params
#
#STATE=$1
#NIC=$2
#if [ $STATE = "fail" ]
#then
# logger -p daemon.notice "execute script Patrol fail ($NIC)"
#fi
#if [ $STATE = "establish" ]
#then
# logger -p daemon.notice "execute script Patrol establish ($NIC)"
#fi
#if [ $STATE = "recover" ]
#then
# logger -p daemon.notice "execute script Patrol recover ($NIC)"
#fi

```

3.6.10.2 Settings for GS/SURE linkage mode

The following shows the script file call format and the definition file sample for the operation in GS/SURE linkage mode.

[Script file call format]

```
/bin/sh hostIP
```

[Definition file sample]

```

#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2011
#
#ident "%W% %G% %U% - FUJITSU"
#
#
# Control interface for HA-Net
#
#
# Set Params
#
#PROC="process_name"
#
# Procedure
#
#
#kill -15 `usr/bin/ps -e | /usr/bin/sed -n \
# -e '/'$PROC'$/s/[^0-9 \t].*/p' \
# ` > /dev/null 2>/dev/null
#

```

3.6.10.3 Settings of the service for Redundant Line Control function

The following shows the script file call format and a setting example when configuring the service for Redundant Line Control function.

(1) When the service is started

The following shows the script file call format and the definition file sample when the service is started.

[Script file call format]

```
/bin/sh service.sh param1
```

param1

fjsvhanet: Startup of the service for Redundant Line Control function

fjsvhanet-poll: Startup of the transfer path monitoring service for Redundant Line Control function

[Definition file sample]

```
#!/bin/sh
#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2011
#
#ident "%W% %G% %U% - FUJITSU"
#
# custom initialize script for fjsvhanet and fjsvhanet-poll service
#
# Params
#
# $1 Started service name fjsvhanet or fjsvhanet-poll
#

case "$1" in

'fjsvhanet')
#
# add procedure for fjsvhanet service
#
# logger -p daemon.notice "execute script for fjsvhanet service"
#
# svcadm restart svc:/network/xxxxxxx
#
;;

'fjsvhanet-poll')
#
# add procedure for fjsvhanet-poll service
#
# logger -p daemon.notice "execute script for fjsvhanet-poll service"
#
# svcadm restart svc:/network/xxxxxxx
#
;;

*)
;;

esac

exit 0
```

(2) When an error is detected by the self-checking function

The following shows the script file call format and the definition file sample for the self-checking function.

[Script file call format]

```
/bin/sh monitor param1 param2
```

param1

driver: GLS driver
daemon: GLS daemon

param2

hungup: A driver or daemon hang detected.
error: A driver or daemon error detected.
process: The abnormal end of the daemon detected.

[Definition file sample]

```
#!/bin/sh
#
#       All Rights Reserved, Copyright (c) FUJITSU LIMITED 2011
#
#ident   "%W% %G% %U% - FUJITSU"
#
#
# Control interface for HA-Net
#
#
#       Params
#
#       $1       driver   ... sha driver
#                daemon   ... hanetctld
#       $2       hungup   ... hanetctld or driver hungup has been detected.
#                error    ... hanetctld or driver i/o error has been detected.
#                process   ... hanetctld process does not exist.
#
#
COMPO=$1
ERRKIND=$2

case $COMPO
in
driver)
#
# script when a driver error is detected.
#

;;

daemon)
#
# script when a daemon error is detected.
#

;;
esac

exit 0
```


3.7 Configuring other functions

3.7.1 Outputting message when transfer paths fails

To configure the system to output a message when a failure occurs in a transfer path, use the "hanetparam" command or "hanetpoll" command. For details, refer to "7.6 hanetparam Command" or "7.7 hanetpoll Command".

3.7.2 Setting Dynamic Reconfiguration (DR)

This section explains the settings when using the Dynamic Reconfiguration function.



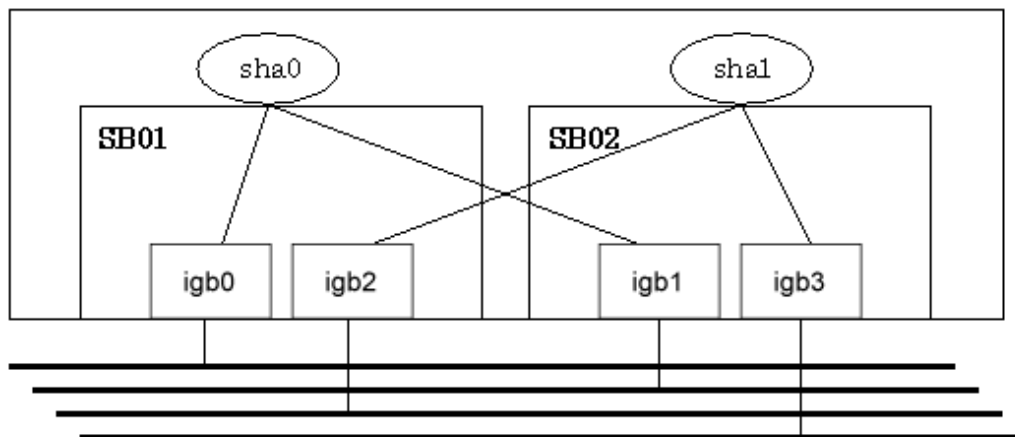
See

For products provided with the DR function, see "2.3.2 DR (Dynamic Reconfiguration) function".

3.7.2.1 Configure environment

When building LAN environment for redundancy system using Redundant Line Control function, in order to replace or add the hardware without stopping the communication using Dynamic Reconfiguration, it is recommended to build the environment shown in "Figure 3.15 Recommended LAN configuration".

Figure 3.15 Recommended LAN configuration



Addition and deletion of hardware resource by a DR function are executed in an SB (System Board) unit. To continue communication when a DR command cuts off a system board, necessary to bundle actual interfaces on several different system boards as shown in a recommended configuration.

When using Redundant Line Control function other than GS/SURE linkage mode on Solaris 10, create one or more network configuration files on each system board. If the network configuration files are created only for one system board, services related to the network including Redundant Line Control function will not start in the case of the system board failure.

For details, see "(3) Checking the network configuration files of the operating system" of "3.2.2.1 Setup common to modes."

3.7.2.2 When using DR linkage function of ESF

Redundant Line Control function uses DR function to manage NIC device name, which allows dynamic replacement or expansion, on a single configuration file (/opt/FJSVhanet/etc/dr.d/hanet_dr_dev). Ensure the NIC device name is defined in the configuration file. If the NIC device name is not defined in the configuration file, DR function cannot be used for dynamic replacement or expansion. In such case, use the text editor to define the NIC device name in the configuration file to allow dynamic replacement or expansion.

The following shows the verification procedure of the configuration file (/opt/FJSVhanet/etc/dr.d/hanet_dr_dev).

```
# cat /opt/FJSVhanet/etc/dr.d/hanet_dr_dev
hme
qfe
eri
vge
ge
fjge
fjgx
fjqe
fjgi
ce
ibdl
bge
e1000g
nxge
fjxge
```

For driver names which are not listed in the setting file (/opt/FJSVhanet/etc/dr.d/hanet_dr_dev), add driver names to the end of the setting file.

```
hme
qfe
eri
vge
ge
fjge
fjgx
fjqe
fjgi
ce
ibdl
bge
e1000g
nxge
fjxge
newdev      <- Added
```

3.7.3 Transfer route multiplexing with Tagged VLAN interface

This section describes on transfer route multiplexing using tagged VLAN interfaces.



Transfer route multiplexing with tagged VLAN is not available in GS/SURE modes.

3.7.3.1 Operating VLAN interface on Fast switching mode

When bundling a tagged VLAN interface on Fast switching mode, specify the tagged VLAN interface instead of the physical interface. [Figure 3.16 Fast switching mode with tagged VLAN interface](#) illustrates bundled tagged VLAN architecture.



- You cannot create a virtual interface by bundling two tagged VLAN interfaces emerged from a single physical interface. Please be sure to specify the tagged VLAN interfaces on disparate physical interfaces when creating a virtual interface for Fast switching mode.
- You cannot mix tagged and untagged VLANs. VLANs can only contain tagged or untagged ports.

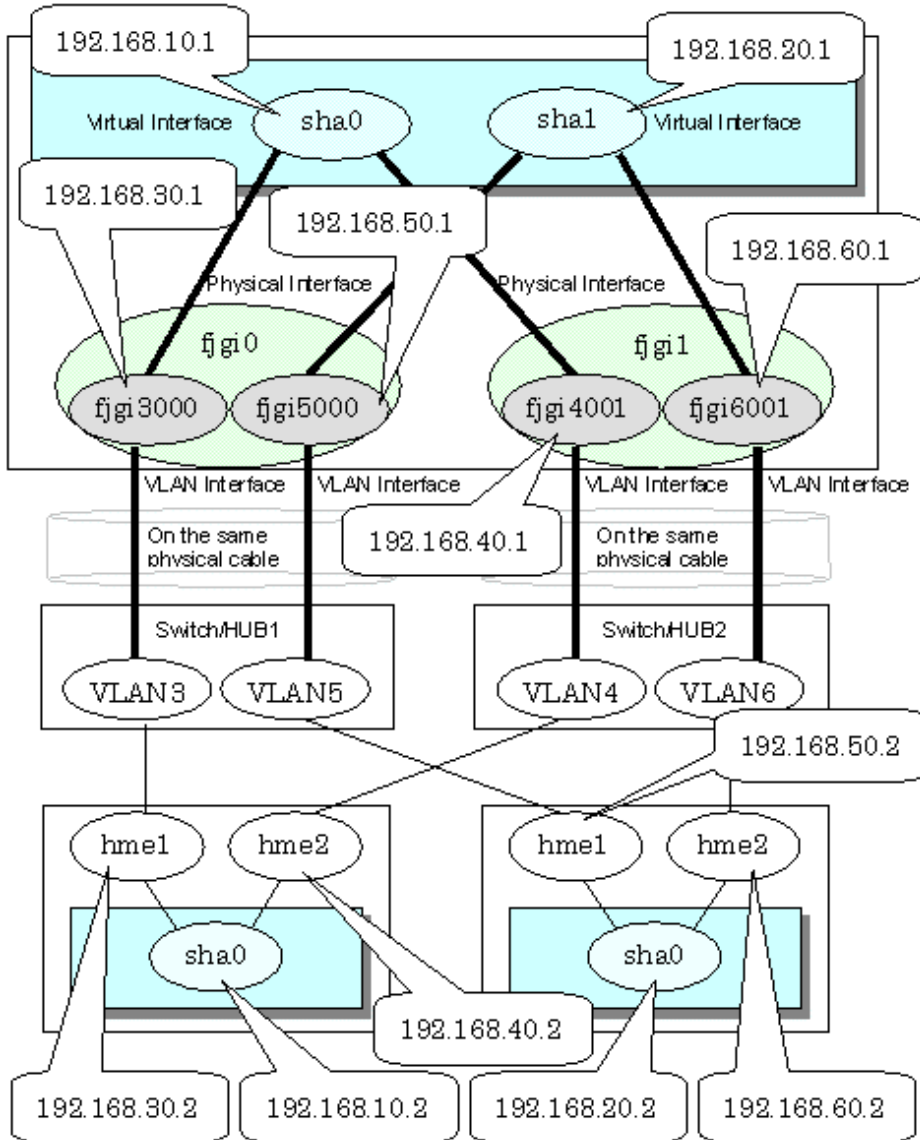


See

Refer to "7.1 hanetconfig Command" for configuring an interface bundled with Fast switching mode.

Figure 3.16 Fast switching mode with tagged VLAN interface illustrates an example of using tagged VLAN interface on Fast switching mode.

Figure 3.16 Fast switching mode with tagged VLAN interface



3.7.3.2 Operating VLAN interface on NIC switching mode

When using a tagged VLAN interface on NIC switching mode, specify the tagged VLAN interface instead of a physical interface at configuration.

In addition, when tagged VLAN interfaces on the same physical network cable is made redundant by two or more virtual interfaces, the mode to "synchronized switching" or "asynchronous switching" operation is defined. Below, operation of "synchronized switching" and "asynchronous switching" is explained.



See

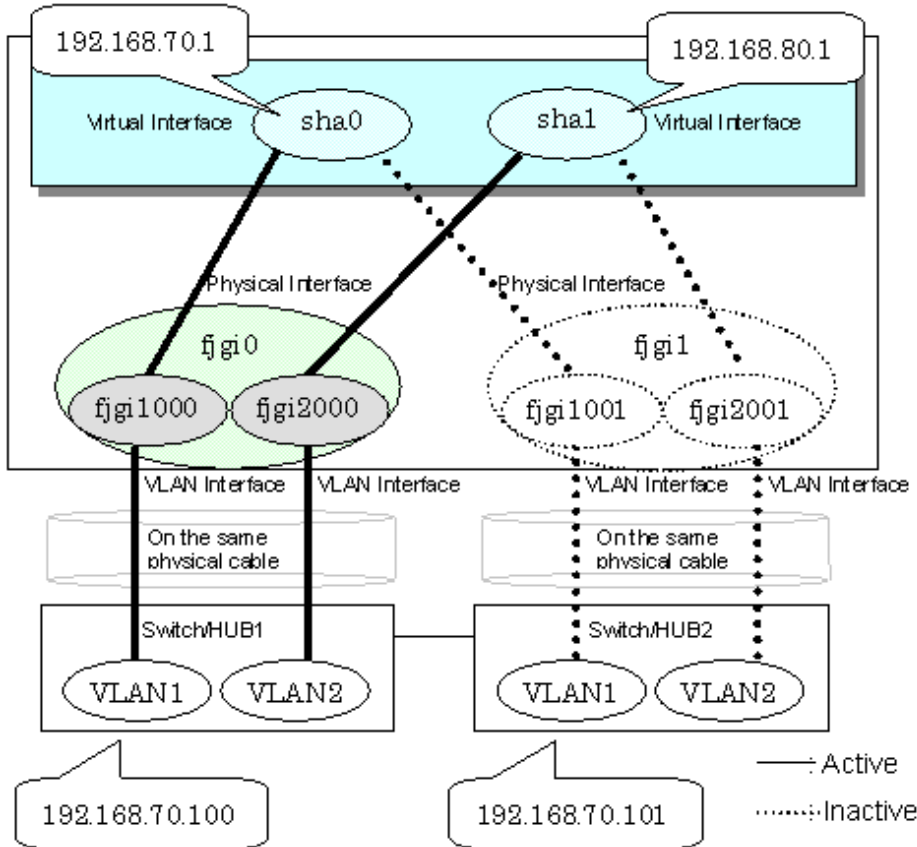
For configuration of monitoring target, refer to "7.7 hanetpoll Command".

Synchronized switching of virtual interfaces

In Two or more virtual interfaces which bundle multiple tagged VLAN interfaces redundantly, by defining the same monitoring target IP address, all virtual interfaces are synchronous switching, when failure occurs in monitoring of transfer path. When the IP address for management can define only one as switch/HUB of a monitoring target, "synchronous switching" of a virtual interface is chosen.

Figure 3.17 NIC switching mode with tagged VLAN interface (synchronized switching) illustrates of synchronous switching architecture.

Figure 3.17 NIC switching mode with tagged VLAN interface (synchronized switching)



Asynchronous switching of virtual interfaces

Contrary to a synchronous switching, two or more virtual interfaces which bundle multiple tagged VLAN interfaces, can be switched asynchronously. In this case, the monitoring target IP address from which it differs for every virtual interface is defined as monitoring target information.

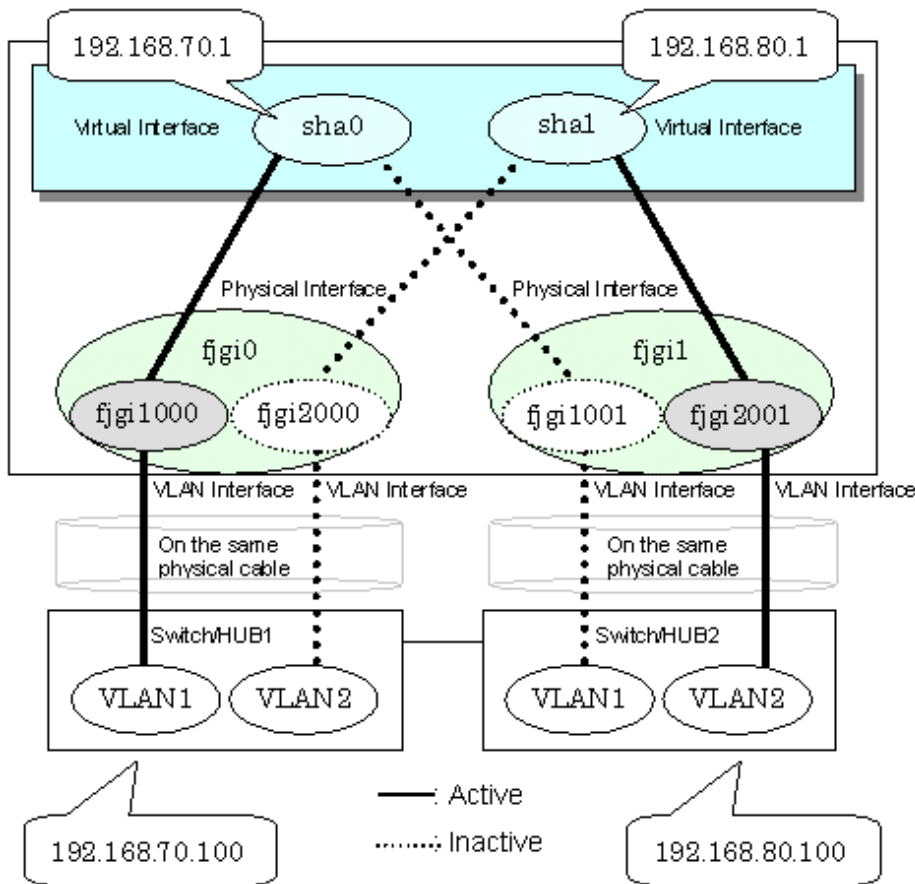
When two or more definitions of the IP address for management are possible to switch/HUB used as a monitoring target, the asynchronous switching of the virtual interfaces is chosen to use Standby NIC effectively.

Point

When the IP address for management can set only one as switch/HUB used as a monitoring target, in order to perform the asynchronous switching of the virtual interfaces, please define the IP address for management of switch/HUB as one certain virtual interface, and define other connection equipment or remote hosts as a monitoring target about other virtual interfaces.

Figure 3.18 NIC switching mode with tagged VLAN interface (asynchronous switching) illustrates of asynchronous switching architecture.

Figure 3.18 NIC switching mode with tagged VLAN interface (asynchronous switching)



Note

- On NIC switching mode, if several tagged VLAN interfaces exist on two physical interfaces, and at least two virtual interfaces are created on pairs of those tagged VLAN interfaces, please ensure that you configure the standby patrol function exclusively on a single virtual interface. For example, say virtual interface (sha0) is created on two tagged VLAN interfaces "fjgi1000" and "fjgi1001", and similarly, another virtual interface (sha1) is created on "fjgi2001" and "fjgi2002", the standby patrol function must be configured on either one of the virtual interfaces (sha0 or sha1).
- On NIC switching mode, tagged VLAN interfaces on a pair of physical interfaces should be used to create multiple virtual interfaces, if tagged VLAN networks are used. For example, you cannot have an environment where a virtual interface is created on a pair of VLAN interfaces "fjgi1000" and "fjgi1001", and another virtual interface is created on a pair of VLAN interfaces "fjgi2001" and "fjgi2002" because the physical interface "fjgi1" is the only shared physical interface here.
- When using synchronized switching mode with tagged VLAN interfaces, only one virtual interface is selected to switch/HUB monitoring. Its interface address is the nearest to monitoring target.
- If you specify two monitoring targets with synchronized switching mode, please specify two network addresses which belong to the same network. If their network addresses are different, switch/HUB monitoring cannot operate normally, because they are assigned to only one virtual interface.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.
- When the physical IP address takeover function of the NIC switching mode is used, a virtual interface cannot be synchronized switched.
- When sharing a physical interface between a virtual interface without tag and a virtual interface with tagged VLAN in NIC switching mode, configure the standby patrol for both virtual interfaces. In this case, specify 0:0:0:0:0:0 to the MAC address.

Chapter 4 Operation

This chapter explains how to operate the redundant line control function.

Redundant Line Control function is operated with commands.

Table 4.1 Redundant Line Control function operation commands below lists the Redundant Line Control function operation commands.

Table 4.1 Redundant Line Control function operation commands

| Type | Command | Function | Authority |
|---|--|--|--------------|
| Activating and deactivating a virtual interface | /opt/FJSVhanet/usr/sbin/strhanet | Activating a virtual interface | Super user |
| | /opt/FJSVhanet/usr/sbin/stphanet | Deactivating a virtual interface | Super user |
| Changing operation | /opt/FJSVhanet/usr/sbin/hanetconfig modify | Changing configuration information | Super user |
| | /opt/FJSVhanet/usr/sbin/hanetpoll on | Enabling the HUB polling function | Super user |
| | /opt/FJSVhanet/usr/sbin/hanetpoll off | Disabling the HUB polling function | Super user |
| Displaying the operation status | /opt/FJSVhanet/usr/sbin/dsphanet | Displaying the operation status of a virtual interface | General user |
| Displaying the polling status | /opt/FJSVhanet/usr/sbin/dsppoll | Displaying the polling status of a HUB | General user |
| Backing up and restoring an configuration file | /opt/FJSVhanet/usr/sbin/hanetbackup | Backing up an configuration file | Super user |
| | /opt/FJSVhanet/usr/sbin/hanetrestore | Restoring an configuration file | Super user |

4.1 Starting and Stopping Redundant Line Control function

This section explains how to start and stop Redundant Line Control function.

4.1.1 Starting Redundant Line Control function

Redundant Line Control function starts automatically when the system starts up.

Then, the preset virtual and logical virtual interfaces are also automatically activated. (However, virtual interfaces in cluster operation mode are activated according to the userApplication status.)

4.1.2 Stopping Redundant Line Control function

Redundant Line Control function stops automatically when the system is shut down.

Then, the preset virtual and logical virtual interfaces are also automatically inactivated. (However, virtual interfaces in cluster operation mode are activated according to the userApplication status.)

4.2 Activating and Inactivating Virtual Interfaces

This section explains how to activate and inactivate virtual interfaces.

The method explained here is valid in single-system operation mode but not in cluster-system operation mode. In cluster-system operation mode, virtual interfaces are activated or inactivated by the start or stop of the userApplication where the virtual interfaces belong.

4.2.1 Activating virtual interfaces

If the configuration has been completed, virtual interfaces are automatically activated at system start. To activate virtual interfaces without a system restart after installing Redundant Line Control function, setting configuration information, and specifying an operation mode, use the `strhanet` command.

For details about this command, see Section "[7.2 strhanet Command](#)".



- Be sure to use a `strhanet` command to activate a virtual interface. Do not use an `ifconfig` command to do the operation.
- Do not operate physical interfaces that a virtual interface bundles with an `ifconfig` command while activating a virtual interface.
- A virtual interface for the shared-IP zone must be activated prior to zone startup. Normally, the virtual interface is activated during system startup. When the virtual interface is added during system startup, however, it is necessary to activate the virtual interface manually before starting the zone.

4.2.2 Inactivating virtual interfaces

Virtual interfaces are automatically inactivated at system shutdown. To inactivate virtual interfaces without a system restart, use the `sphanet` command.

For details about this command, see Section "[7.3 sphanet Command](#)".



- Be sure to use a `sphanet` command to deactivate a virtual interface. Do not use an `ifconfig` command to do the operation.
- If the shared-IP zone is using the virtual interface, you cannot deactivate it. First, stop the zone then deactivate the virtual interface.

4.3 Displaying Operation Status

Use the `dsphanet` command to display the operation status of virtual interfaces.

Specifying options enables the display of the operation status of specific virtual interfaces, the operation status of communication parties in Fast switching mode, and the number of connections to be assigned in GS/SURE linkage mode. For details about this command, see Section "[7.4 dsphanet Command](#)".

4.4 Displaying Monitoring Status

Use the `dsppoll` command to display the monitoring statuses of the HUB function and the communication target monitoring function.

For information on this command, see Section "[7.8 dsppoll Command](#)".

4.5 Dynamic operation (Replacement / Expansion)

In Redundant Line Control function, it is possible to replace or add redundant NIC (PCI card) by linking with Dynamic Reconfiguration (DR) and PCI Hot Plug (PHP).

The following table shows the available functions for replacing or adding NICs (PCI cards), and their support statuses.

| Dynamic operation | Compatible system |
|------------------------------|--|
| DR (Dynamic Reconfiguration) | SPARC M12-2S/M10-4S, SPARC Enterprise M4000/M5000/M8000/M9000 |
| PHP (PCI Hot Plug) | SPARC M12/ M10, SPARC Enterprise M4000/M5000/M8000/M9000 |

4.5.1 Executing DR command of ESF

(1) Disconnecting a system board

When using a DR command (drc -disconnect), an actual interface on the corresponding system board is automatically cut off from a virtual interface according to a DR connection script of a Redundant Line Control function.

It is not possible to disconnect a system board if a virtual interface (sha0 etc) and a physical interface have been configured on it. A DR connection script outputs a message and ends abnormally.

In this case, deactivate a virtual interface configured by a physical interface on a system board to be cut off, and execute a DR command (drc -disconnect) after deleted a definition.

(2) Connecting a system board

When connected using a DR command (drc -connect), an actual interface on the corresponding system board is automatically incorporated into a virtual interface according to a description of the configuration information file in a DR connection script of a Redundant Line Control function.

(3) Cancellation

In case the system commands to stop executing DR process due to a certain reason, or if the user requests to stop it while a DR command is executed, the system cancels execution of the DR command.

Through the DR connection script of GLS, the disconnection process can be stopped, and the environment is restored to the original state.

[Notes]

- While exchanging a system board containing a physical interface that has been used to configure a virtual interface in NIC switching mode, HUB monitoring function halts temporarily since it is not possible to switch NICs even if an error occurs in a transfer route.
- After replacing a system board containing a physical interface used to configure a virtual interface in NIC switching mode, line monitoring will start normally.
- The connection script does not support the disconnecting/embedding of an NIC under a redundant virtual interface comprised of an IPv6 virtual interface and a tagged VLAN interface. If disconnecting the system board using the DR command, first disconnect the NIC built into the system board from the multiplex configuration according to the following procedure. Also, after performing the system board embedding, perform embedding to the multiplex configuration.
 - For virtual interfaces of dual stack
Delete physical NICs of IPv6 by using the ifconfig command. If the target NIC for DR is the primary interface and the active interface, switch the NIC by using the hanetnic change command beforehand.
 - For virtual interfaces of IPv6 native or tagged VLAN interfaces
Disconnect NICs by using the same procedure as for the XSCF DR.

4.5.2 Replacing the system board using the DR of XSCF

4.5.2.1 Replacing the system board using the DR of XSCF (SPARC M12-2S/ M10-4S)

1) Checking the system configuration

Check the NIC built into the system board to be replaced according to the following procedure.

1-1) Execute the showbbstatus(8) command to check that XSCF of the system board to be replaced is not the master XSCF.

If it operates as the master XSCF, you need to change its status from Active to Standby.

For details, see "Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide."

1-2) Check the status of the system board to be replaced.

```
XSCF> showboards -p 0
PSB  PPAR-ID(LSB) Assignment  Pwr  Conn Conf Test   Fault
-----
```


| | | | | | | | |
|------|--------|----------|---|---|---|--------|--------|
| 00-0 | 00(00) | Assigned | y | y | y | Passed | Normal |
| 01-0 | 00(01) | Assigned | y | y | y | Passed | Normal |

1-3) Check the NIC built into the system board to be replaced.

For details, see "Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide."

2) Disconnecting from the multiplex configuration

In order to disconnect the NIC to be replaced from the multiplex configuration, specify the interface name confirmed in step 1), and execute the following commands. When the active path is disconnected from the redundant configuration of the active-standby mode, the standby side will be automatically switched over to be active.

The interface names described in the following procedure vary depending on the environment.

If using fast-switching mode

- For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i igb1 <Return>
# /usr/sbin/ifconfig igb1 unplumb <Return>
# /usr/sbin/ifconfig igb1 inet6 unplumb <Return>
```

- For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i net1 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

Note

Since the IP address and the netmask of the interface to be disconnected will be used in the step 6), take notes for them in advance by executing some commands (such as ifconfig).

```
# /usr/sbin/ifconfig net1 <Return>
```

If using NIC switching mode

The following procedure is required depending on the status of a NIC built into the target system board for replacement.

- If OS is Solaris 11 or later and NIC is the primary interface:
Settings of the IP address must be deleted before replacing the system board.
- If NIC is the operation NIC, NIC switch is required manually before replacing the system board.

1. Checking the primary interface name and the operation NIC

Check the primary interface name. The primary interface name is displayed at the beginning of "Interface List" field. In this example, it is "net1."

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol]

Name          Hostname          Mode MAC Adder/Phys ip Interface List
+-----+-----+-----+-----+-----+
sha0          192.168.70.1      d   192.168.70.2     net1,net2
sha1          -                 p   00:00:00:00:00:00 sha0

[IPv6]

Name          Hostname/prefix          Mode Interface List
+-----+-----+-----+-----+-----+

```

Check the operation NIC name, in this example, it is "net1."

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL  Device
-----+-----+-----+-----+-----+
sha0      Active  d    ON   net1(ON),net2(OFF)
sha1      Active  p    OFF  sha0(ON)
[IPv6]
Name      Status   Mode CL  Device
-----+-----+-----+-----+-----+
```

2. Stopping the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off <Return>
# /opt/FJSVhanet/usr/sbin/stpctl -n sha1 <Return>
```

3. Switching the physical interfaces

To execute this command, the NIC for replacement must be the operation NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

4. Deleting IP address settings

To execute this command, OS must be Solaris 11 or later and NIC for replacement must be the primary interface.

```
# /usr/sbin/ifconfig net2 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

 **Note**

To return to the multiplex configuration, the IP address and the netmask of the interface specified by the ipadm delete-ip command must be set.

Note the output result of the ifconfig command.

If using GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i sha2 <Return>
```

3) Deleting the I/O device of the system board to be replaced from the logical domain

Delete the I/O device of the system board to be replaced from the logical domain before replacing the system board.

For details, see "Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide."

4) Replacing the system board

Replace the system board.

4-1) Delete the system board.

Delete the system board with the deleteboard(8) command.

```
XSCF> deleteboard -c disconnect 01-0
```

Execute the showresult(8) command to check that the exit status of the deleteboard(8) command is 0.

```
XSCF> showresult
0
```

4-2) Check the status of the system board.

Use the showboards(8) command to display the system board information and check the status.

```
XSCF> showboards -p 0
PSB  PPAR-ID(LSB)  Assignment  Pwr  Conn  Conf  Test   Fault
-----
00-0  00(00)         Assigned   y    y    y    Passed Normal
01-0  00(01)         Assigned   n    n    n    Passed Normal
```

4-3) Physically replace the system board.

Execute the replacefru(8) command. Follow the displayed directions, and replace the board with the hot swap procedure. For details on hot swap, see the service manual for the service being used.

```
XSCF> replacefru
```

4-4) Check the status of the replaced system board.

Use the showboards(8) command to display the system board information. Then, check the status of all applicable system boards.

```
XSCF> showboards -p 0
PSB  PPAR-ID(LSB)  Assignment  Pwr  Conn  Conf  Test   Fault
-----
00-0  00(00)         Assigned   y    y    y    Passed Normal
01-0  00(01)         Assigned   n    n    n    Passed Normal
```

4-5) Add the replaced system board to the physical partition.

```
XSCF> addboard -c configure -p 0 01-0
```

Execute the showresult(8) command to check that the exit status of the addboard(8) command is 0.

```
XSCF> showresult
0
```

4-6) Check the status of the system board.

Check the status of the replaced system board with the showboards(8) command.

```
XSCF> showboards -p 0
PSB  PPAR-ID(LSB)  Assignment  Pwr  Conn  Conf  Test   Fault
-----
00-0  00(00)         Assigned   y    y    y    Passed Normal
01-0  00(01)         Assigned   y    y    y    Passed Normal
```

5) Checking the operating status of the logical domain

Check that the operating status of the logical domain has not been changed.

For details, see "Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide."

6) Connecting the logical domain to the I/O device for the replaced system board

Connect the logical domain to the I/O device for the replaced system board.

For details, see "Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Domain Configuration Guide."

7) Embedding to the multiplex configuration

In order to embed the NIC built in the replaced system board into the multiplex configuration, specify the interface name confirmed in step 1) and execute the following command.

The interface names described in the following procedure vary depending on the environment.

If using fast-switching mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i igb1 <Return>
```

When setting configuration for fast-switching mode, execute the following commands to activate the added interfaces in advance:

- When using IPv4 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igb1 plumb <Return>
# /usr/sbin/ifconfig igb1 ipaddress netmask + broadcast + -trailers up
<Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4 <Return>
```

- When using IPv6 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igb1 inet6 plumb up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
```

If using NIC switching mode

The following procedure is required depending on the status of a NIC built into the replaced system board.

- If OS is Solaris 11 or later and NIC is the primary interface:

After replacing the system board, switch the NIC manually, and reset the IP address.

1. Switching the physical interface and resetting the IP address

To execute this command, OS must be Solaris 11 or later and a NIC built into the replaced system board must be the primary interface. Otherwise, move to Step 2.

- If the IPv4 address is used

```
# /usr/bin/touch /var/opt/FJSVhanet/tmp/disable_watchif <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4
<Return>
# /usr/bin/rm -f /var/opt/FJSVhanet/tmp/disable_watchif <Return>
```

- If the IPv6 address is used

```
# /usr/bin/touch /var/opt/FJSVhanet/tmp/disable_watchif <Return>
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

```
# /usr/sbin/ipadm delete-ip net1 <Return>
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
# /usr/bin/rm -f /var/opt/FJSVhanet/tmp/disable_watchif <Return>
```

2. Starting the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1 <Return>
# /opt/FJSVhanet/usr/sbin/hanetpoll on <Return>
```

3. Switching the physical interfaces

Switch the physical interfaces as necessary.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i sha2 <Return>
```

If using GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i sha2 <Return>
```

8) Reverting the active path (only if necessary)

If changing the active path through the hot swap, perform a reversion of the active path as necessary.

4.5.2.2 Replacing the system board using the DR of XSCF (SPARC Enterprise M4000/M5000/M8000/M9000)

1) Checking the system configuration

Check the NIC built into the system board to be replaced according to the following procedure.

1-1) Check the domain status.

Using the showdcl(8) command, display the domain information and confirm the domain status.

```
XSCF> showdcl -d 0
DID  LSB  XSB  Status
00
    00  00-0
    01  01-0
```

1-2) Check the status of the system board to be replaced.

Using the showboards(8) command, display the system board information and confirm the status of the system board to be deleted.

```
XSCF> showboards 01-0 <Return>
XSB DID(LSB) Assignment Pwr Conn Conf Test Fault
-----
01-0 00(01)  Assigned    y    y    y    Passed Normal
```

1-3) Check the NIC built into the system board to be replaced.

Using the showdevices(8) command, check the NIC interface name built into the system board to be replaced.

```
XSCF> showdevices 01-0
CPU:
----
DID XSB id state    speed  ecache
00  01-0 0  on-line  2048    4
00  01-0 1  on-line  2048    4
```

```

Memory:
-----
          board  perm   base                domain  target  deleted  remaining
DID XSB  mem MB   mem MB   address            mem MB   XSB     mem MB   mem MB
00 01-0  8192    2048    0x000003c000000000  65536

IO Devices:
-----
DID XSB  device resource                usage
00 01-0  sd0      /dev/dsk/c0t0d0s0  mounted filesystem "/"
00 01-0  sd0      /dev/dsk/c0t0d0s1  swap area
00 01-0  sd0      /dev/dsk/c0t0d0s1  dump device (swap)
00 01-0  bge0     SUNW_network/bge0 bge0 hosts IP addresses:10.1.1.1
00 01-0  bge2     SUNW_network/bge2 bge2 hosts IP addresses:10.1.2.1

```

2) Disconnecting from the multiplex configuration

In order to disconnect the NIC to be replaced from the multiplex configuration, specify the interface name confirmed in step 1), and execute the following commands. When the active path is disconnected from the redundant configuration of the active-standby mode, the standby side will be automatically switched over to be active.

The interface names described in the following procedure vary depending on the environment.

If using fast-switching mode

- For Solaris 10

```

# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i igb1 <Return>
# /usr/sbin/ifconfig igb1 unplumb <Return>
# /usr/sbin/ifconfig igb1 inet6 unplumb <Return>

```

- For Solaris 11 or later

```

# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i net1 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>

```

Note

For changing back to the multiplex configuration, an IP address of the interface specified by the hanetnic delete command and a netmask need to be set.

Note them using the ifconfig command and so on, in advance.

```

# /usr/sbin/ifconfig net1 <Return>

```

If using NIC switching mode

The following procedure is required depending on the status of a NIC built into the target system board for replacement.

- If OS is Solaris 11 or later and NIC is the primary interface:
Settings of the IP address must be deleted before replacing the system board.
- If NIC is the operation NIC, NIC switch is required manually before replacing the system board.

1. Checking the primary interface name

Check the primary interface name. The primary interface name is displayed at the beginning of "Interface List" field. In this example, it is "net1."

```

# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol]

```

| Name | Hostname | Mode | MAC Adder/Phys ip | Interface List |
|------|--------------|------|-------------------|----------------|
| sha0 | 192.168.70.1 | d | 192.168.70.2 | net1,net2 |
| sha1 | - | p | 00:00:00:00:00:00 | sha0 |

[IPv6]

| Name | Hostname/prefix | Mode | Interface List |
|------|-----------------|------|----------------|
|------|-----------------|------|----------------|

Check the operation NIC name. In this example, it is "net1."

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL  Device
-----+-----+----+---+-----+
sha0     Active   d    ON   net1(ON),net2(OFF)
sha1     Active   p    OFF  sha0(ON)
[IPv6]
Name      Status   Mode CL  Device
-----+-----+----+---+-----+
```

2. Stopping the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off <Return>
# /opt/FJSVhanet/usr/sbin/stpctl -n sha1 <Return>
```

3. Switching the physical interfaces

To execute this command, the NIC for replacement must be the operation NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

4. Deleting IP address setting

To execute this command, OS must be Solaris 11 or later and NIC for replacement must be the primary interface.

```
# /usr/sbin/ifconfig net2 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

 Note

To return to the multiplex configuration, the IP address and the netmask of the interface specified by the ipadm delete-ip command must be set.

Note the output result of the ifconfig command.

If using GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i sha2 <Return>
```

3) Replacing the system board

Replace the system board.

3-1) Delete the system board.

Using the deleteboard(8) command, delete the system board.

```
XSCF> deleteboard -c disconnect 01-0
```

3-2) Check the status of the system board.

Using the showboards(8) command, display the system board information and confirm the status of the system boards.

```
XSCF> showboards 01-0
XSB DID(LSB) Assignment Pwr Conn Conf Test Fault
-----
01-0 00(01) Assigned y n n Passed Normal
```

3-3) Physically replace the system board.

Execute the replacefru(8) command. Follow the displayed directions, and replace the board with the hot swap procedure. For details on hot swap, refer to the service manual for the server being used.

```
XSCF> replacefru
```

3-4) Check the status of the replaced system board.

Using the showboards(8) command, display the system board information and confirm such items as the status of all applicable system boards and the registration status to the DCL.

```
XSCF> showboards 01-0
XSB DID(LSB) Assignment Pwr Conn Conf Test Fault
-----
01-0 00(01) Assigned y n n Passed Normal
```

3-5) Check the domain status.

```
XSCF> showdcl -d 0
DID  LSB  XSB  Status
00           Running
      00  00-0
      01  01-0
```

3-6) Add the replaced system board to the domain.

```
XSCF> addboard -c configure -d 0 01-0
```

3-7) Check the statuses for the domain and the system boards.

Using the showdcl(8) command, confirm the domain status.

```
XSCF> showdcl -d 0
DID  LSB  XSB  Status
00           Running
      00  00-0
      01  01-0
```

Using the showboards(8) command, confirm the status of the replaced system boards.

```
XSCF> showboards 01-0
XSB DID(LSB) Assignment Pwr Conn Conf Test Fault
-----
01-0 00(01) Assigned y y y Passed Normal
```


4) Embedding to the multiplex configuration

In order to embed the NIC built in the replaced system board into the multiplex configuration, specify the interface name confirmed in step 1) and execute the following command.

The interface names described in the following procedure vary depending on the environment.

If using fast-switching mode

```
# /opt/FJShanet/usr/sbin/hanetnic add -n sha0 -i igbl <Return>
```

When setting configuration for fast-switching mode, execute the following commands to activate the added interfaces in advance:

- When using IPv4 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igbl plumb <Return>
# /usr/sbin/ifconfig igbl ipaddress netmask + broadcast + -trailers up
<Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4 <Return>
```

- When using IPv6 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igbl inet6 plumb up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
```

If using NIC switching mode

The following procedure is required depending on the status of a NIC built into the replaced system board.

- If OS is Solaris 11 or later and a NIC is the primary interface:

After replacing the system board, switch the NIC manually, and reset the IP address.

1. Switching the physical interface and resetting the IP address

To execute this command, OS must be Solaris 11 or later and a NIC built into the replaced system board must be the primary interface. Otherwise, move to Step 2.

- If the IPv4 address is used

```
# /usr/bin/touch /var/opt/FJShanet/tmp/disable_watchif <Return>
# /opt/FJShanet/usr/sbin/hanetnic change -n sha0 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4
<Return>
# /usr/bin/rm -f /var/opt/FJShanet/tmp/disable_watchif <Return>
```

- If the IPv6 address is used

```
# /usr/bin/touch /var/opt/FJShanet/tmp/disable_watchif <Return>
# /opt/FJShanet/usr/sbin/hanetnic change -n sha0 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
# /usr/bin/rm -f /var/opt/FJSSVhanet/tmp/disable_watchif <Return>
```

2. Starting the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSSVhanet/usr/sbin/strptl -n sha1 <Return>
# /opt/FJSSVhanet/usr/sbin/hanetpoll on <Return>
```

3. Switching the physical interfaces

Switch the physical interfaces as necessary.

```
# /opt/FJSSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

If using GS/SURE linkage mode

```
# /opt/FJSSVhanet/usr/sbin/hanetnic add -n sha2 -i sha0 <Return>
```

5) Reverting the active path (only if necessary)

If changing the active path through the hot swap, perform a reversion of the active path as necessary.

4.5.3 Replacement/Expansion PHP (PCI Hot Plug)

This section explains a procedure of replacing or adding a PCI card for GLS in a PCI Hot Plug (PHP) environment.

Compatibility of PHP with each mode is shown in the table below.

Table 4.2 Compatibility of PHP with each mode

| PHP(PCI Hot Plug) operation | Fast switching mode | NIC switching mode | GS/SURE linkage mode |
|----------------------------------|---------------------|--------------------|----------------------|
| Replacement (Redundant system) | A | A | A |
| Extension (Non-redundant system) | A | A | A |
| Extension (Redundant system) | A | X | A |

[PHP Support] A: Supported X: Not supported

Note

Replacement and expansion of PHP (PCI Hot Plug) is allowed only when the system is running in a multiple user mode.

4.5.3.1 Replacement of PCI card on redundant system

In Fast Switching and NIC Switching mode, it is possible to replace the redundant NIC without stopping network communication.

Note

For NIC Switching mode, it is required to stop the transfer path monitoring function and standby patrol function.
For GS/SURE linkage mode, it is required to deactivate the virtual interface.

The following is a procedure of replacing redundant system.

1) Specify the replacing PCI card

An interface on the PCI card to be replaced can be identified from the warning messages output to the console (eg. igb1).

Note

In Solaris 11 or later, Solaris 10 9/10 or later releases, or in the environment where 142909-17 or later patch is applied in Solaris 10

When using PHP, execute the following command to enable the hotplug service. For details, refer to "Service Manual" according to your server.

```
# svcadm enable hotplug
```

2) Disconnect from redundant system

In order to remove the PCI card from the redundant system for replacement, please execute the following command with the interface name obtained in the procedure "1) Specify the replacing PCI card". On the redundant system of standby mode, when an online communication path is disconnected, a standby communication path will be online communication path automatically.

Fast switching mode

- For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetnic delete -n sha0 -i igb1 <Return>
# /usr/sbin/ifconfig igb1 unplumb <Return>
# /usr/sbin/ifconfig igb1 inet6 unplumb <Return>
```

- For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetnic delete -n sha0 -i net1 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

Note

For changing back to the multiplex configuration, an IP address of the interface specified by the hanetnic delete command and a netmask need to be set.

Note them using the ifconfig command and so on, in advance.

```
# /usr/sbin/ifconfig net1 <Return>
```

NIC switching mode

The following procedure is required depending on the status of a NIC (PCI card) built into the target system board for replacement.

- If OS is Solaris 11 or later and a NIC is the primary interface:
Settings of the IP address must be deleted before replacing the system board. If a NIC is the operation NIC, the NIC switching is required manually before replacing the system board.

1. Checking the primary interface name

Check the primary interface name. The primary interface name is displayed at the beginning of "Interface List" field. In this example, it is "net1."

```
# /opt/FJShanet/usr/sbin/hanetconfig print
[IPv4,Patrol]

Name          Hostname          Mode MAC Adder/Phys ip Interface List
+-----+-----+-----+-----+-----+-----+
sha0          192.168.70.1      d   192.168.70.2    net1,net2
sha1          -                 p   00:00:00:00:00:00 sha0
```

| [IPv6] | | | |
|---------------------------|-----------------|------|----------------|
| Name | Hostname/prefix | Mode | Interface List |
| +-----+-----+-----+-----+ | | | |

Check the operation NIC name. In this example, it is "net1."

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[ IPv4,Patrol]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
sha0      Active  d    ON   net1(ON),net2(OFF)
shal      Active  p    OFF  sha0(ON)
[ IPv6 ]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
```

2. Stopping the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off <Return>
# /opt/FJSVhanet/usr/sbin/stpctl -n sha1 <Return>
```

3. Switching the physical interfaces

To execute this command, a NIC for replacement must be the operation NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

4. Deleting IP address setting

To execute this command, OS must be Solaris 11 or later and NIC for replacement must be the primary interface.

```
# /usr/sbin/ifconfig net2 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
```

 Note

To return to the multiplex configuration, the IP address and the netmask of the interface specified by the ipadm delete-ip command must be set.

Note the output result of the ifconfig command.

GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i sha2 <Return>
```

3) Disconnect the PCI card

Specify the interface name (eg, igb1) identified in the procedure "1) Specify the replacing PCI card." to "inst2comp" command to obtain the PCI bus slot "Ap_Id".

Specify the "Ap_Id" obtained above as an argument to "cfgadm"(1M) command, and confirm that the slot status of the PCI card to be disconnected is "connected configured".

```
# cfgadm BB#0-PCI#0
```

| Ap_Id | Type | Receptacle | Occupant | Condition |
|------------|------------|------------------|-------------------|-----------|
| BB#0-PCI#0 | etherne/hp | <u>connected</u> | <u>configured</u> | ok |

Execute the `uncfgadm(1M)` command with specifying `unconfigure` to cancel the configuration of the PCI card at `Ap_Id`. After that, execute the `cfgadm(1M)` command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c unconfigure BB#0-PCI#0 <Return>
# cfgadm BB#0-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#0-PCI#0           unknown      connected   unconfigured unknown
```

Execute the `uncfgadm(1M)` command with specifying `disconnect` to disconnect the PCI card from `Ap_Id`.

After that, execute the `cfgadm(1M)` command to check if the slot status is changed to "disconnected unconfigured".

```
# cfgadm -c disconnect BB#0-PCI#0 <Return>
# cfgadm BB#0-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#0-PCI#0           unknown      disconnected unconfigured unknown
```

To indicate the slot position for replacement, specify the obtained "Ap_Id" to "cfgadm" command and blink the ATTENTION LED.

```
# cfgadm -x led=attn,mode=blink BB#0-PCI#0 <Return>
```

4) Replace the PCI card

The PCI card disconnected in the procedure "3) Disconnect the PCI card" is replaced with a new one. Our customer support staff does this for you.

5) Connect the PCI card

Execute the `cfgadm(1M)` command with specifying `connect` to connect the new PCI card to `Ap_Id`.

After that, execute the `cfgadm(1M)` command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c connect BB#0-PCI#0 <Return>
# cfgadm BB#0-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#0-PCI#0           unknown      connected   unconfigured unknown
```

Execute the `cfgadm(1M)` command with specifying `connect` to connect the new PCI card to `Ap_Id`.

After that, execute the `cfgadm(1M)` command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c configure BB#0-PCI#0 <Return>
# cfgadm BB#0-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#0-PCI#0           etherne/hp   connected   configured   ok
```

6) Connect to redundant system

In order to connect the new PCI card to a redundant system, please execute the following commands with the interface name identified in the procedure "1) Specify the replacing PCI card".

The interface names described in the following procedure vary depending on the environment.

For Solaris 11 or later, the default interface name is `netX` (X means the instance number).

Fast switching mode

- For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i igb1 <Return>
```

- For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetnic add -n sha0 -i net1 <Return>
```

When setting configuration for fast-switching mode, execute the following commands to activate the added interfaces in advance:

- When using IPv4 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igbl plumb <Return>
# /usr/sbin/ifconfig igbl ipaddress netmask + broadcast + -trailers up
<Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4 <Return>
```

- When using IPv6 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igbl inet6 plumb up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
```

NIC switching mode

The following procedure is required depending on the status of a NIC (PCI card) built into the target system board for replacement.

- If OS is Solaris 11 or later and NIC is the primary interface:

Settings of the IP address must be deleted before replacing the system board. After replacing the system board, switch the NIC manually, and reset the IP address.

1. Switching the physical interface and resetting the IP address

To execute this command, OS must be Solaris 11 or later and a NIC built into the replaced system board must be the primary interface. Otherwise, move to Step 2.

- If the IPv4 address is used

```
# /usr/bin/touch /var/opt/FJShanet/tmp/disable_watchif <Return>
# /opt/FJShanet/usr/sbin/hanetnic change -n sha0 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4
<Return>
# /usr/bin/rm -f /var/opt/FJShanet/tmp/disable_watchif <Return>
```

- If the IPv6 address is used

```
# /usr/bin/touch /var/opt/FJShanet/tmp/disable_watchif <Return>
# /opt/FJShanet/usr/sbin/hanetnic change -n sha0 <Return>
# /usr/sbin/ipadm delete-ip net1 <Return>
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
# /usr/bin/rm -f /var/opt/FJShanet/tmp/disable_watchif <Return>
```

2. Starting the HUB monitoring function and the patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1 <Return>
# /opt/FJSVhanet/usr/sbin/hanetpoll on <Return>
```

3. Switching the physical interfaces

Switch the physical interfaces as necessary.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 <Return>
```

GS/SURE linkage mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i sha2 <Return>
```

7) Switch back the redundant path

Please switch back an online communication path if needed.

4.5.3.2 Extension of PCI cards with new redundant system

By adding a new PCI card to a non-redundant system, it is possible to create a redundant system.

The following is the procedure of adding a new PCI card to a non-redundant system.



In Solaris 11 or later, Solaris 10 9/10 or later releases, or in the environment where 142909-17 or later patch is applied in Solaris 10

When using PHP, execute the following command to enable the hotplug service. For details, refer to "Service Manual" according to your server.

```
# svcadm enable hotplug
```

1) Add PCI cards

a.

Before adding a PCI card, please save the output of "prtpci"(1M) command.

```
# prtpci -v > /tmp/prtpci.pre <Return>
```

b.

Check the status of the slot.

An example of adding a PCI card to BB#1-PCI#0 is shown in this section.

Please confirm that the status of the PCI slot where a PCI card is added is "empty unconfigured" by using "cfgadm" (1M) command.

```
# cfgadm BB#1-PCI#0 <Return>
Ap_Id          Type          Receptacle  Occupant    Condition
BB#1-PCI#0    unknown      empty       unconfigured unknown
```

c.

To indicate the slot position for expansion, specify the "Ap_Id" identified in the procedure 1)b to "cfgadm" command and blink the ATTENTION LED.

```
# cfgadm -x led=attn,mode=blink BB#1-PCI#0 <Return>
```

d.

Add a PCI card after the POWER LED of the target PCI bus slot has turned off.
This operation is performed by our customer support.

e.

Please confirm that the PCI slot status which extended PCI cards is "disconnected unconfigured" by using cfgadm (1M) command.

```
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#1-PCI#0          unknown      disconnected unconfigured unknown
```

2) Connect PCI cards

Execute the cfgadm(1M) command with specifying connect to connect the new PCI card to Ap_Id.
After that, execute the cfgadm(1M) command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c connect BB#1-PCI#0 <Return>
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#1-PCI#0          unknown      connected    unconfigured unknown
```

Execute the cfgadm(1M) command with specifying connect to connect the added PCI card to Ap_Id.
After that, execute the cfgadm(1M) command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c configure BB#1-PCI#0 <Return>
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type          Receptacle  Occupant    Condition
BB#1-PCI#0          etherne/hp    connected    configured    ok
```

3) Connect equipment to PCI cards

The extended PCI card is connected with network equipment by the cable.

4) Setup driver

The driver configuration is added by following operations.

a.

The interface name is investigated in order to configure drivers and high layer products.

Please save the result of the prtcli (1M) command, and obtain the difference information between current result and the result taken at "1) a." Then, the driver instance number for the extended PCI card is obtained.

In the following example, since the instance number is 1, it can be determined that the interface name of the extended PCI card is "igb1."

```
# prtcli -v > /tmp/prtcli.post <Return>
# diff /tmp/prtcli.pre /tmp/prtcli.post | more <Return>
:
> :devfs-path      /pci@8900/pci@4/pci@0/pci@0/network@0
> :driver-name     igb
> :binding-name    pciex8086,1521
> :bus-addr        0
> :instance        1
> :_class          network
> :name            network
:
```

b.

Confirm that the interface name that is obtained from the above operation matches the one that has been added to the PCI bus slot.

c.

The configuration of each driver is added.
Please refer to each driver manual for details.

5) Setup redundant system

Activate the virtual interface after configuring Fast Switching, NIC Switching, or GS/SURE linkage mode. System reboot is not required after configuring each mode.

When configuring Fast Switching mode, the added interface "igb1(net1)" must be activated preliminary by the following command.

The interface names described in the following procedure vary depending on the environment.

For Solaris 11 or later, the default interface name is netX (X means the instance number).

- For IPv4 address
 - For Solaris 10

```
# /usr/sbin/ifconfig igb1 plumb <Return>
# /usr/sbin/ifconfig igb1 ipaddress netmask + broadcast + -trailers up
<Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net1/v4
<Return>
```

- For IPv6 address
 - For Solaris 10

```
# /usr/sbin/ifconfig igb1 inet6 plumb up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net1 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net1/v6 <Return>
```



[For Solaris 10 environment]

For Fast switching mode (IPv4), the IP address specified in this section must also be defined in /etc/inet/hosts and /etc/hostname.igb1.

For Fast switching mode (IPv6), create /etc/hostname6.igb1 as an empty file.

Unless these are configured, when the system reboots, the virtual interface for Fast Switching mode cannot be activated.

4.5.3.3 Extension of PCI cards to redundant system

It is possible to extend a PCI card to the redundant system.



- In NIC Switching mode, it is not possible to add a new interface to a redundant system.
Also, when adding a new interface in GS/SURE linkage mode, it is first required to deactivate the virtual interface for GS/SURE linkage mode and then add a new interface.

- When using PHP in Solaris 11 or later, Solaris 10 9/10 or later releases, or in the environment where 142909-17 or later patch is applied in Solaris 10, execute the following command to enable the hotplug service. For details, refer to "Service Manual" according to your server.

```
# svcadm enable hotplug
```

The following is the procedure of extending PCI card to the redundant system.

1) Add PCI cards

a.

Before extending the PCI card, please save the result (current configuration information) of the prtpticl (1M) command.

```
# prtpticl -v > /tmp/prtpticl.pre <Return>
```

b.

Check the status of the slot.

An example of adding a PCI card to BB#1-PCI#0 is shown in this section. Please confirm that the status of the PCI slot where a PCI card is added is "empty unconfigured" by using "cfgadm" (1M) command.

```
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type      Receptacle  Occupant    Condition
BB#1-PCI#0           unknown  empty       unconfigured unknown
```

c.

To indicate the slot position for expansion, specify the "Ap_Id" identified in the procedure 1) b to "cfgadm" command and blink the ATTENTION LED.

```
# cfgadm -x led=attn,mode=blink BB#1-PCI#0 <Return>
```

d.

Add a PCI card after the POWER LED of the target PCI bus slot has turned off. This operation is performed by our customer support.

e.

Please confirm that the PCI slot status which extended PCI cards is "disconnected unconfigured" by using cfgadm (1M) command.

```
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type      Receptacle  Occupant    Condition
BB#1-PCI#0           unknown  disconnected unconfigured unknown
```

2) Connect PCI cards

Execute the cfgadm(1M) command with specifying connect to connect the new PCI card to Ap_Id.

After that, execute the cfgadm(1M) command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c connect BB#1-PCI#0 <Return>
# cfgadm BB#1-PCI#0 <Return>
Ap_Id                Type      Receptacle  Occupant    Condition
BB#1-PCI#0           unknown  connected   unconfigured unknown
```

Execute the cfgadm(1M) command with specifying connect to connect the added PCI card to Ap_Id.

After that, execute the cfgadm(1M) command to check if the slot status is changed to "connected unconfigured".

```
# cfgadm -c configure BB#1-PCI#0 <Return>
# cfgadm BB#1-PCI#0 <Return>
```

| Ap_Id | Type | Receptacle | Occupant | Condition |
|------------|------------|------------------|-------------------|-----------|
| BB#1-PCI#0 | etherne/hp | <u>connected</u> | <u>configured</u> | ok |

3) Connect equipment to PCI cards

The extended PCI card is connected with network equipment by the cable.

4) Setup driver

The driver configuration is added by following operations.

a.

The interface name is investigated in order to configure drivers and high layer products.

Please save the result of the prtcl (1M) command, and obtain the difference information between current result and the result taken at 1)

a. Then, the driver instance number for the extended PCI card is obtained.

In the following example, since the instance number is 2, it can be determined that the interface name of the extended PCI card is "igb2."

```
# prtcl -v > /tmp/prtcl.post <Return>
# diff /tmp/prtcl.pre /tmp/prtcl.post | more <Return>
:
> :devfs-path      /pci@8900/pci@4/pci@0/pci@0/network@0
> :driver-name     igb
> :binding-name    pciex8086,1521
> :bus-addr        0
> :instance        2
> :_class          network
> :name            network
:
```

b.

Confirm that the interface name that is obtained from the above operation matches the one that has been added to the PCI bus slot.

c.

The configuration of each driver is added.

Please refer to each driver manual for details.

5) Connect to redundant system

Please execute following commands in order to connect the extended PCI card to the existing redundant configuration system.

The interface names described in the following procedure vary depending on the environment. For Solaris 11 or later, the default interface name is netX (X means the instance number).

Fast switching mode

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i igb2 -f <Return>
```

When setting environment configuration for fast-switching mode, execute the following commands to activate the added interfaces in advance.

- When using IPv4 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igb2 plumb <Return>
# /usr/sbin/ifconfig igb2 ipaddress netmask + broadcast + -trailers
up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net2 <Return>
# /usr/sbin/ipadm create-addr -T static -a ipaddress/netmask net2/v4
<Return>
```

- When using IPv6 address:

- For Solaris 10

```
# /usr/sbin/ifconfig igb2 inet6 plumb up <Return>
```

- For Solaris 11 or later

```
# /usr/sbin/ipadm create-ip net2 <Return>
# /usr/sbin/ipadm create-addr -T addrconf net2/v6 <Return>
```



Note

[For Solaris 10 environment]

For Fast switching mode (IPv4), the IP address specified in this section must also be set to /etc/inet/hosts and /etc/hostname.igb2.

For Fast switching mode (IPv6), create /etc/hostname6.hme1igb1 as an empty file.

Unless these are configured, when the system reboots, the virtual interface for Fast Switching mode cannot be activated.

GS/SURE linkage mode

```
# /opt/FJSSVhanet/usr/sbin/stphanet -n sha0 <Return>
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha4 -m n -i IP_address -t igb2 <Return>
# /opt/FJSSVhanet/usr/sbin/hanetconfig modify -n sha0 -t sha2,sha3,sha4 <Return>
# /opt/FJSSVhanet/usr/sbin/strhanet -n sha0 <Return>
```

6) Switch the redundant path

Please switch an online communication path for extended communication path if needed.

4.6 Recovery Procedure from Line Failure

This section explains the recovery procedure in various modes after a line failure has occurred.

4.6.1 Recovery procedure from line failure in Fast switching mode

No special operation is required because recovery is automatically made after a line failure has occurred.

However, some applications may need to be restarted.

4.6.2 Recovery procedure from line failure in NIC switching mode

The following shows the recovery procedure from a line failure in NIC switching mode.

Some applications may need to be restarted after the recovery procedure on Redundant Line Control function.

[One-system (currently active NIC) failure]

After line recovery, execute the following command:

```
# /opt/FJSSVhanet/usr/sbin/hanetnic change -n shaX
```

* shaX is the virtual interface name for NIC switching mode.

[Both-system (currently active and standby NICs) failure]

After line recovery, execute the following command:

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

4.6.3 Recovery procedure from line failure in GS/SURE linkage mode

No special operation is required because recovery is automatically made after a line failure has occurred.

However, some applications may need to be restarted.

4.6.4 How to recover when an error occurred in a transfer route at the execution of DR

Described in this section is the recovery procedure from a transfer route error occurred during DR operation to replace a system board. After the recovery, execute "drc -connect" command and finish the DR operation.

[Fast switching mode]

See "[4.6.1 Recovery procedure from line failure in Fast switching mode](#)" as to how to recover when an error occurred in a transfer route in Fast switching mode.

[NIC switching mode]

Regarding DR execution in NIC switching mode, because HUB monitoring function and standby patrol function stop while replacing a system board, network communication is suspended if a failure is detected in a transfer path. After recovering the transfer path, communication will be restored thus recovery process is not necessary.

Some applications may require reactivating the application.

[GS/SURE linkage mode]

See "[4.6.3 Recovery procedure from line failure in GS/SURE linkage mode](#)" as to how to recover when an error occurred in a transfer route in GS/SURE linkage mode.

4.6.5 How to recover when an error occurred in a transfer route at the execution of PHP

The following describes the recovery procedures from a failure occurred during NIC (PCI card) replacement operation with PHP.

[Fast switching mode]

See "[4.6.1 Recovery procedure from line failure in Fast switching mode](#)" as to how to recover when an error occurred in a transfer route in Fast switching mode.

[NIC switching mode]

While executing PHP, because HUB monitoring function and standby interface monitoring function stops while exchanging the NIC (PCI card), if a failure is detected in a transfer path, it suspends the network communication. After the transfer path recovers, the communication recovers as well, so no further recovery work is required. However, some application requires restarting the application.

[GS/SURE linkage mode]

See "[4.6.3 Recovery procedure from line failure in GS/SURE linkage mode](#)" as to how to recover when an error occurred in a transfer route in GS/SURE linkage mode.

4.7 Backing up and Restoring Configuration Files

This section explains how to back up and restore configuration files of Redundant Line Control function.

4.7.1 Backing up Configuration Files

Use the `hanetbackup` command to back up configuration files.

For details about this command, see Section "[7.12 hanetbackup Command](#)".

4.7.2 Restoring Configuration Files

Use the `hanetrestore` command to restore configuration files.

For details about this command, see Section "[7.13 hanetrestore Command](#)".

After executing this command, restart the system immediately. The system will not operate as defined in the configuration file, unless you reboot the system.

Chapter 5 GLS operation on cluster systems

This chapter explains how to operate the redundant line control on a cluster system.

5.1 Outline of Cluster System Support

In cluster system, Redundant Line Control function supports the following operation modes:

- Active standby system (1:1 and N:1)
- Mutual standby system
- Cascade system
- Priority transfer system

How cluster failover is dealt with in each mode is shown below.

Table 5.1 List of the cluster system compatible function

| Mode | Active Standby System (1:1) | Active Standby System (N:1) | Mutual standby System | Cascade System | Priority transfer system | Duplicate transfer path for SIS |
|----------------------|-----------------------------|-----------------------------|-----------------------|----------------|--------------------------|---------------------------------|
| Fast switching mode | A | A | A | A | A | X |
| NIC switching mode | A | A | A | A | A | A |
| GS/SURE linkage mode | A | X | X | X | X | X |

[Meaning of the symbols] A: Supported X: Not supported

Virtual IP addresses allocated to virtual interfaces are taken over if a cluster switching event occurs. GLS does not provide any function to support MAC address takeover and system node name takeover. A physical interface used for GLS cannot be used to configure a cluster resource (Take over IP address and Take over MAC address). [Table 5.2 Supported cluster take over information](#) indicates the support status of each takeover function.

Table 5.2 Supported cluster take over information

| Cluster Operation mode | IP address | MAC address | IP address + MAC address | IP address + System node name | IP address + MAC address + System node name |
|------------------------|------------|-------------|--------------------------|-------------------------------|---|
| 1:1 Active standby | A | X | X | X | X |
| N:1 Active standby | A | X | X | X | X |
| Mutual standby | A | X | X | X | X |
| Cascade | A | X | X | X | X |
| Priority transfer | A | X | X | X | X |

[Meaning of the symbols] A: Supported X: Not supported B: No match

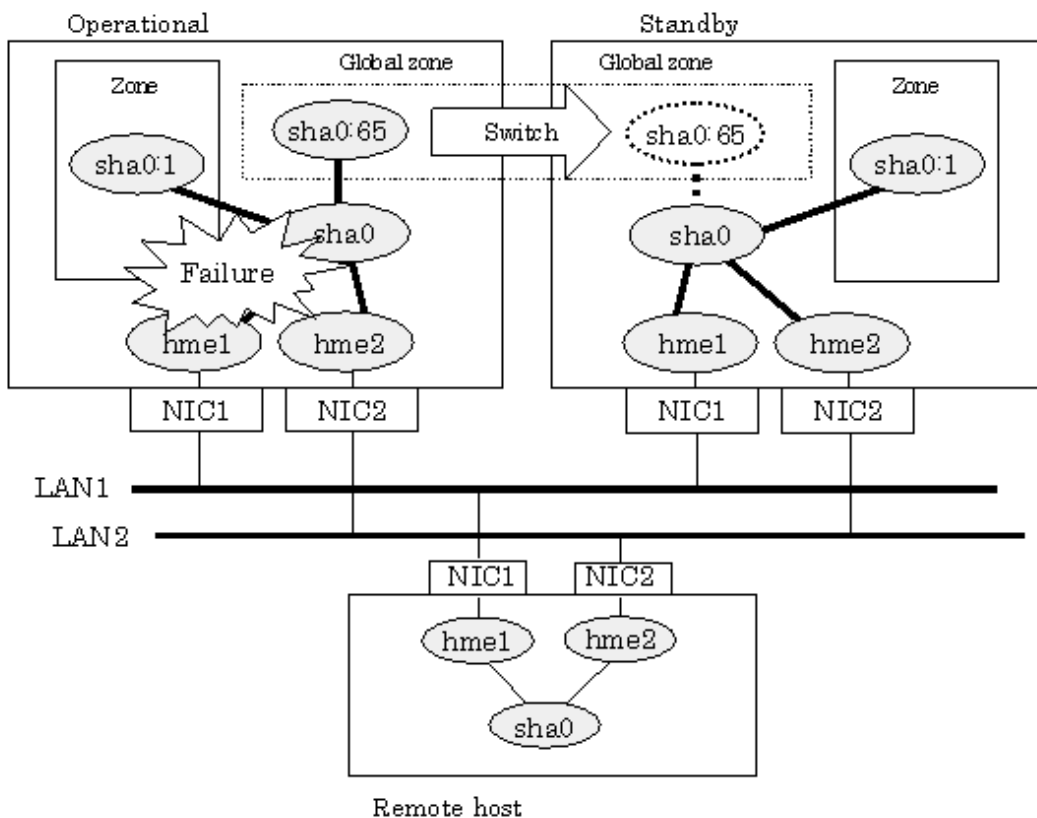
Note

- Configuring GLS as Priority transfer, one of the cluster operation, follows the same procedure for configuring Cascade operation.
- When using Fast switching mode, you need a host running Fast switching mode as an associate host other than a node configuring a Cluster system. Failover of GLS resource may fail if there is only one Cluster system configuring nodes due to simultaneous detection of transfer route failure on operation node and standby node.

- When switching the node in both Fast Switching and NIC switching mode, do not use IPv6 address as a take over virtual interface if immediate communication is required. If IPv6 address is used, it takes approximately 30 seconds to restore communication after switching the node. For detail, see "G.3 Troubleshooting".
- The logical virtual interface and IP address allocated in the Solaris Zones cannot be taken over along with cluster switching. If a failure occurs on all the transmission routes of the operating node, a communication session between the Solaris Zones and global zone fails.
- For GS/SURE linkage mode, the virtual interface on standby node side is inactive and its monitoring function stops. Therefore, it cannot monitor the GLS resource on the standby node. Unlike other modes, GS/SURE linkage mode does not require to specify "StandbyTransition" attribute because it does not run the resource monitoring.
- For cluster operation of virtual NIC mode, use one of the following configurations:
 - NIC switching mode (Virtual NIC)
 - NIC non-redundant of NIC switching mode will be built for virtual NIC.
 - For details, see "B.4.13 Example of the Cluster system (Virtual NIC)" in this manual.
 - Creating takeover network resources
 - Takeover network resources of cluster application will be created for virtual NIC.
 - For details, see "Creating Takeover Network Resources" in the manual "PRIIMECLUSTER Installation and Administration Guide."

Figure 5.1 Cluster Switching for the virtual interface shows an example of cluster switching for the virtual interface.

Figure 5.1 Cluster Switching for the virtual interface



The logical unit number for the virtual interface for cluster switching is 65 or later. (sha0:65, sha0:66)

5.1.1 Active Standby

5.1.1.1 Starting

5.1.1.1.1 Fast switching mode

With userApplication startup, the takeover virtual interface (sha0:65) over operating node will be activated, enabling communication using the takeover virtual IP address.

When operating, Fast switching mode uses the Redundant Line Control function to communicate with the remote system.

Note that the virtual interface (such as sha0) is inactive just after GLS starts up. The virtual interface will be active after the first startup of userApplication. Once it becomes active, regardless of stopping or restarting userApplication, it remains to be active until the system stops.



Note

When communicating with the other network using the virtual interface of Fast switching mode, or activating the virtual interface prior to userApplication startup, use hanetparam command to set the activation timing.

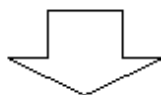
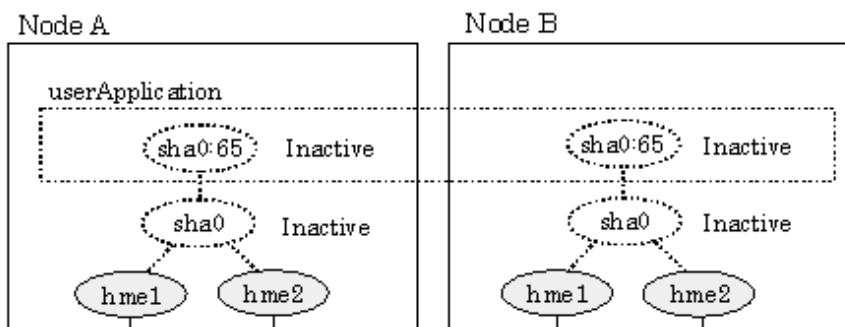
For detail, refer to "7.6 hanetparam Command".

For description of setup, refer to "G.1 Changing Methods of Activating and Inactivating Interface".

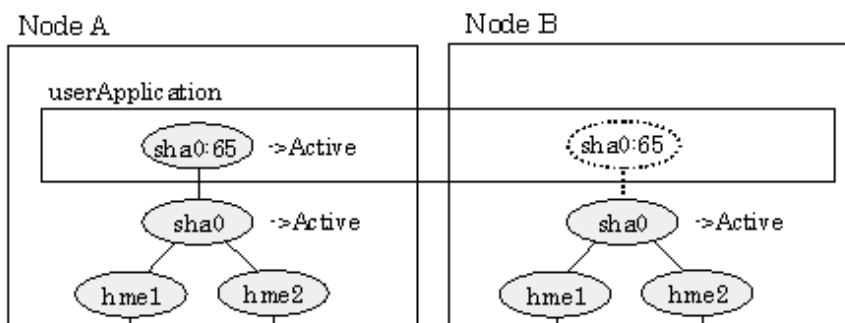
Figure 5.2 Startup behavior of Fast switching mode shows behavior of Fast switching mode after starting up

Figure 5.2 Startup behavior of Fast switching mode

[Prior to userApplication start up]



[After userApplication started]



5.1.1.1.2 NIC switching mode

NIC switching mode has the following address takeover functions. Select a function to be used depending on your operation.

- Logical address takeover

Using the logical address takeover function allows a LAN to have several virtual IP addresses. Ordinary communication will be done via a physical IP address, and a communication through GLS will be done via the virtual IP addresses.

For the remote system device to make a connection, a physical IP address should be specified as the connection address. Then, the remote system device can directly connect to the active or standby node and manage each of the nodes regardless of the status transition of the userApplication.

For this function, two IP addresses are assigned to one physical interface. To use a TCP/IP application that requires only one IP address to be specified, use the physical address takeover function I or II.

- Physical IP address takeover I

Use the Physical IP address takeover function I for a GLS network and an ordinary network to exist in a same LAN, sharing an IP address allocated to a physical interface.

This function allows a connection to be made for each of the active and standby nodes independently. However, IP address of the standby node changes according to the status transition of the userApplication. Thus, when clusters are switched, the TCP connection to the standby node is cleared. For the communication target device to make a connection again, the connection IP address must be changed.

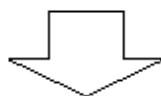
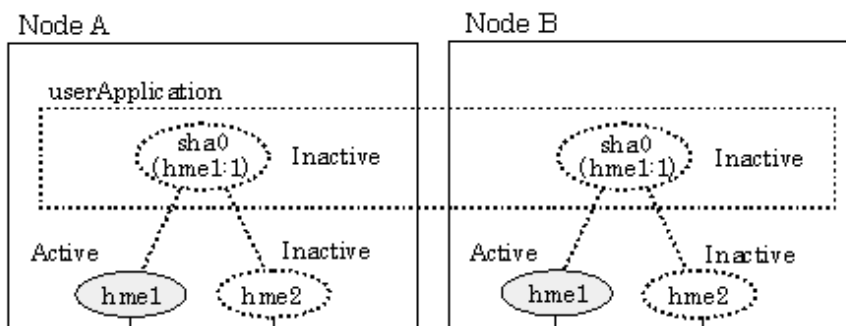
- Physical IP address takeover II

Use the Physical IP address takeover function II to use a LAN only for GLS networking. In this case, no connection can be made to the standby node because the LAN of the standby node is inactivated. Another LAN must be provided to make a connection.

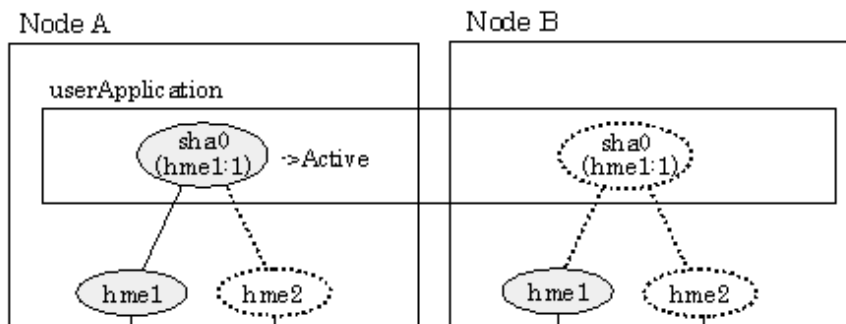
Figure 5.3 Startup behavior of NIC switching mode (take over logical IP) shows the active standby configuration diagram of duplicated operation in NIC switching mode (logical IP address takeover function). The operation in this figure is as follows: On active node A, the logical interface (hme1:1) of the secondary interface (hme1) is assigned the takeover virtual IP address (IP-A) and activated. If switching occurs due to a failure, the takeover virtual interface (hme1:1) that has been assigned the take over IP address (IP-A) is inactivated. Then, on standby node B, the logical interface (hme0:1) that has been assigned the take over IP address (IP-A) on the already activated primary interface (hme0) is activated.

Figure 5.3 Startup behavior of NIC switching mode (take over logical IP)

[Prior to userApplication startup]



[After userApplication startup]

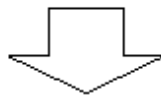
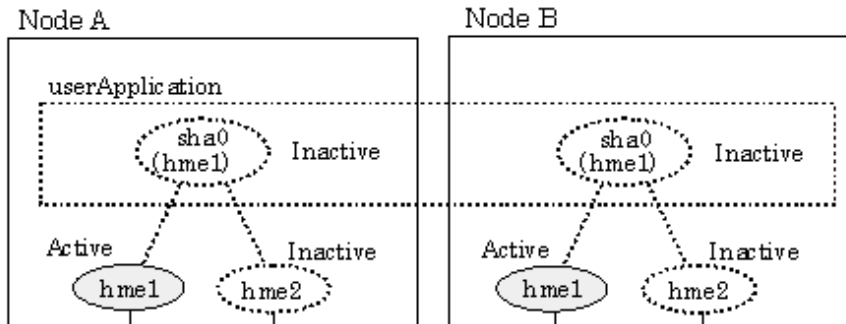


For taking over physical IP address I, activate the physical interface (hme1) for operating node and standby node when the Redundant Line Control function starts up. After the userApplication starts, it will activate the physical interface by allocating a take over IP address to the physical interface on the operating node. At this time, a physical interface (hme1) over the standby node remains to be inactive.

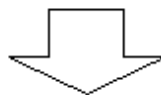
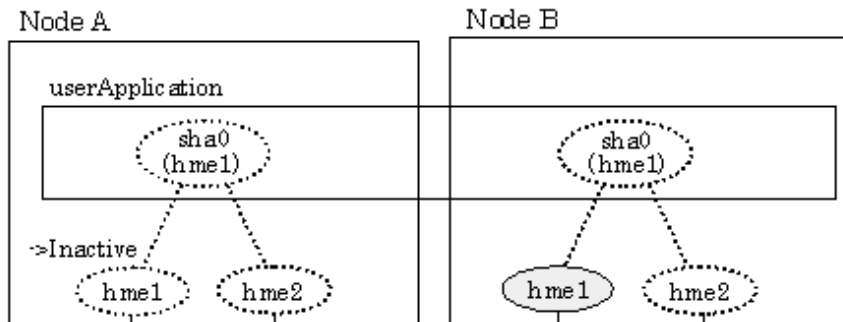
Figure 5.4 Startup behavior of NIC switching mode (takeover physical IP address I) shows a startup behavior of takeover physical IP address I

Figure 5.4 Startup behavior of NIC switching mode (takeover physical IP address I)

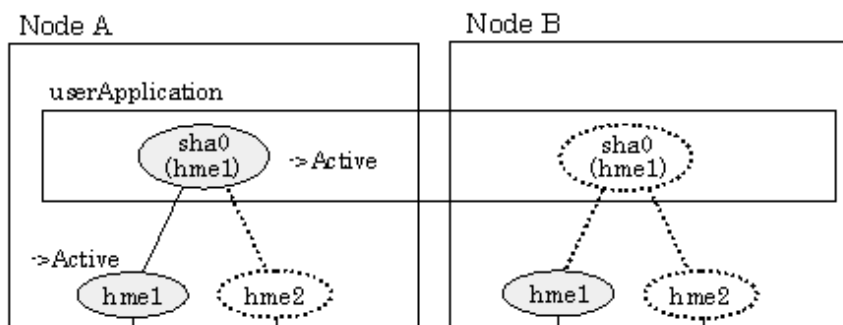
[Prior to userApplication startup]



[Running userApplication]



[After userApplication starts up]

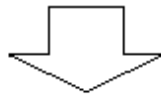
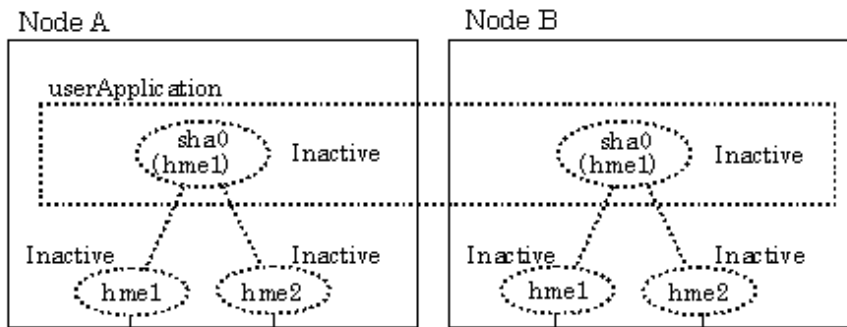


For taking over physical IP address II, it does not activate the physical interface (hme1) for both operating node and standby node when Redundant Line Control function starts up. Instead it allocates a take over IP address to the physical interface (hme1) on the operating node and then it activates the physical interface. In this case, the physical interface (hme1) for standby node remains inactive.

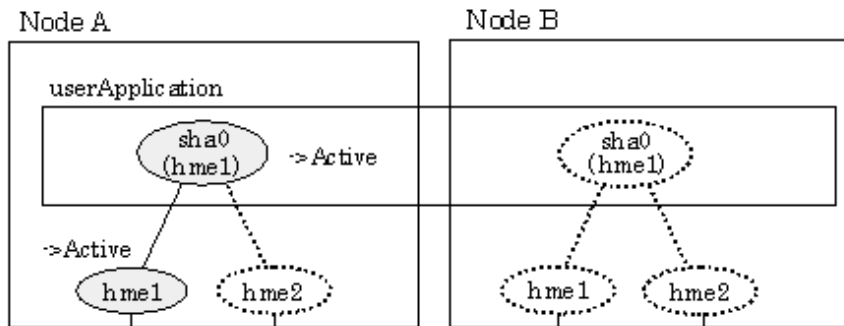
Figure 5.5 Startup behavior of NIC switching mode (takeover physical IP address II) shows a startup behavior of the takeover physical IP address II

Figure 5.5 Startup behavior of NIC switching mode (takeover physical IP address II)

[Prior to userApplication startup]



[After userApplication starts up]

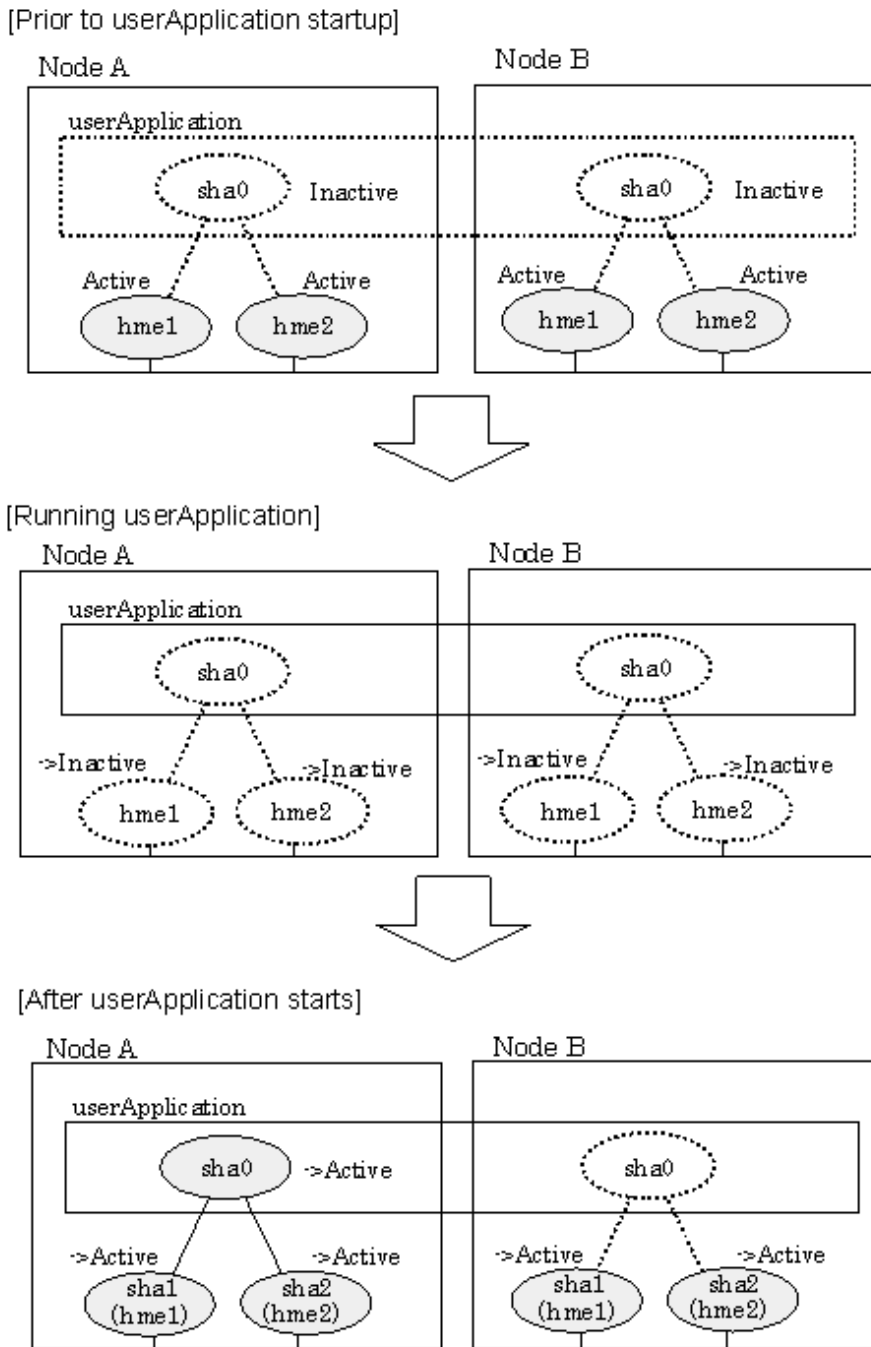


5.1.1.1.3 GS/SURE linkage mode

By starting userApplication, the take over virtual interface (sha0) over operating node becomes active allowing communication using the take over virtual IP address. When operating, GS/SURE linkage mode uses the Redundant Line Control function to communicate with the remote system.

Figure 5.6 Startup behavior of GS/SURE linkage mode shows startup behavior of GS/SURE linkage mode

Figure 5.6 Startup behavior of GS/SURE linkage mode



5.1.1.2 Switching

During normal operation, the system communicates with the remote system using Redundant Line Control function on the operating node.

If a failure (panic, hang-up, or line failure) occurs on the operating node, Redundant Line Control function switches the resources to the standby node. Then, applications make reconnection to take over the communication from the operating node.

5.1.1.2.1 Fast switching mode

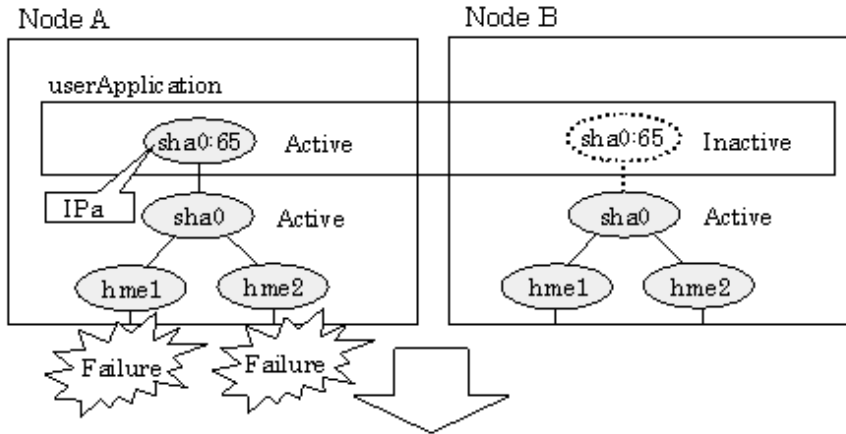
Figure 5.7 Switching behavior of Fast switching mode indicates switching behavior of Fast switching mode.

In the following figure, the take over IP address (IPa) is allocated to the takeover virtual interface (sha0:65) for operating node A. Then it activates the takeover virtual interface. When switching the interface due to failures in the transfer path, the takeover virtual interface

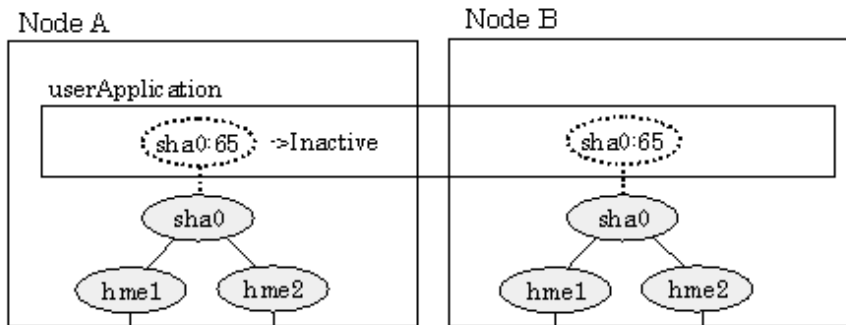
(sha0:65) for operating node A becomes inactive. Then in standby node B, the takeover virtual interface (sha0:65), which has allocated the take over IP address (IPa) becomes active. Note that the virtual interface (sha0) in node A remains unchanged.

Figure 5.7 Switching behavior of Fast switching mode

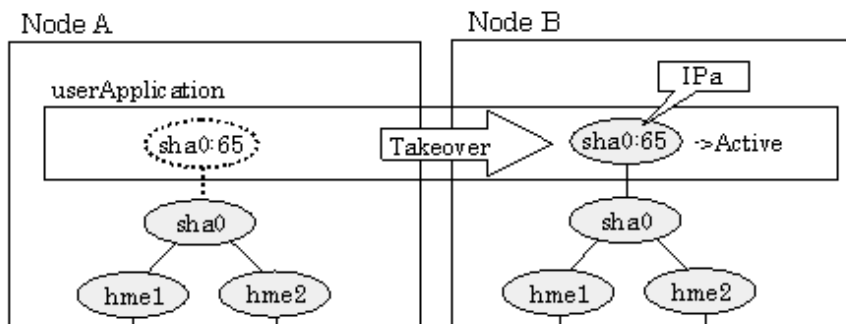
[Operation status (Failure occurred in node A)]



[Switching]



[Finished switching]



5.1.1.2.2 NIC switching mode

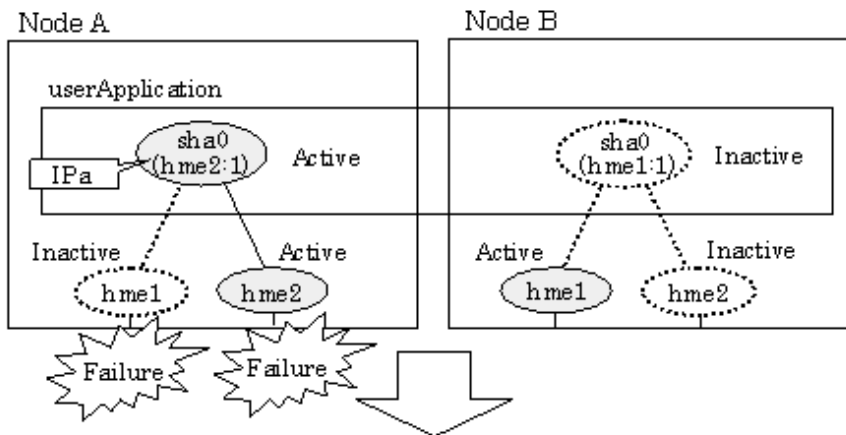
Figure 5.8 Switching behavior of NIC switching mode (takeover logical IP) illustrates switching behavior of NIC switching mode (logical IP address takeover function).

In the following figure, the take over virtual IP address (IPa) in the operating node A is allocated to the logical interface (hme2.1) for the secondary interface. Once IPa is allocated, the logical interface (hme2.1) for the secondary interface turns into activate state.

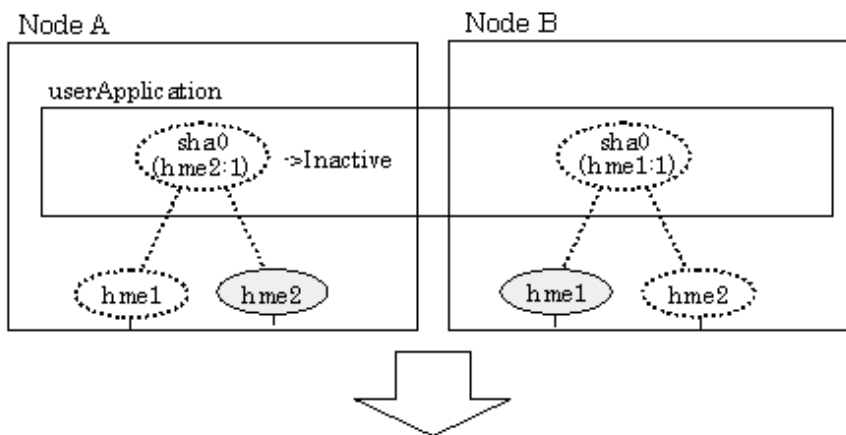
When switching the node due to failure in the transfer routes, NIC switching mode inactivates the logical virtual interface which has allocated the take over IP address (IPa) in the operating node A. Then it allocates the take over IP address to the primary interface (hme1) and finally activates the logical interface (hme1:1).

Figure 5.8 Switching behavior of NIC switching mode (takeover logical IP)

[Operation status (Failure occurred in node A)]



[Switching]



[Finished switching]

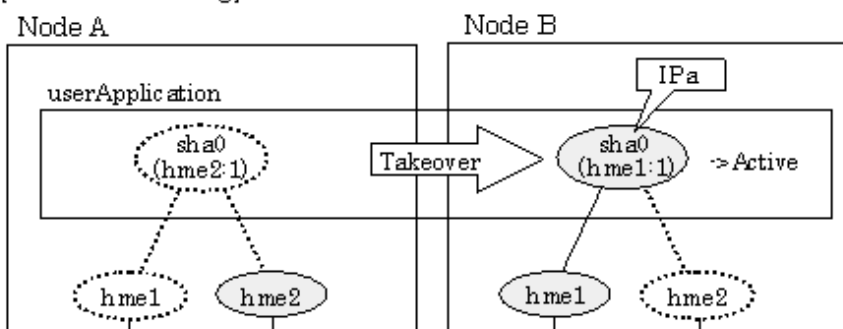


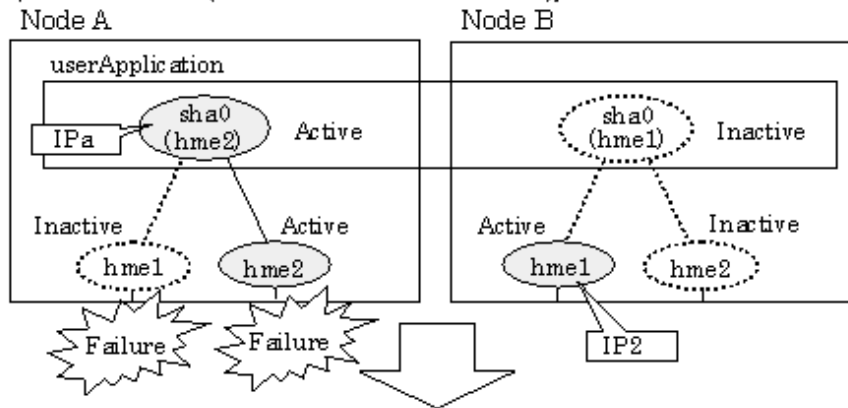
Figure 5.9 Switching behavior of NIC switching mode (takeover physical IP I) (continues) and Figure 5.10 Switching behavior of NIC switching mode (takeover physical IP I) illustrate switching behavior of NIC switching mode (take over physical IP address I).

In the following figure, the take over virtual IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

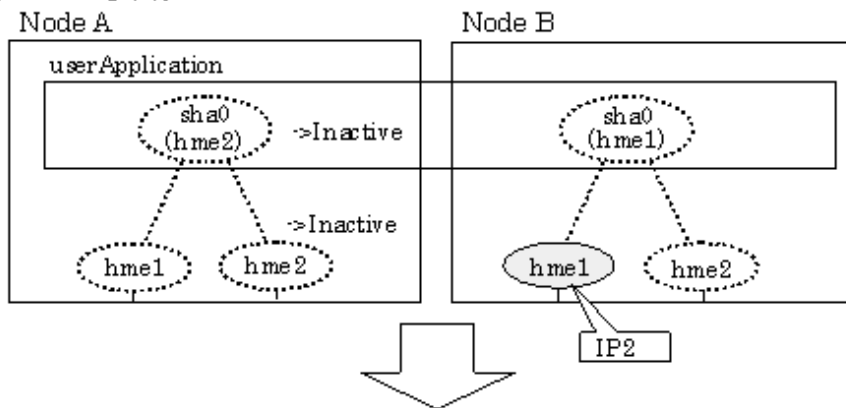
When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (hme1), which has been active in the standby node B. Then it allocates the take over IP address (IPa) to activate the primary interface (hme1). Once the primary interface activates, different IP address is allocated to the secondary interface (hme2) by means of inactivating hme2.

Figure 5.9 Switching behavior of NIC switching mode (takeover physical IP I) (continues)

[Operation status (Failure occurred in Node A)]



[Switching (1)]



[Switching (2)]

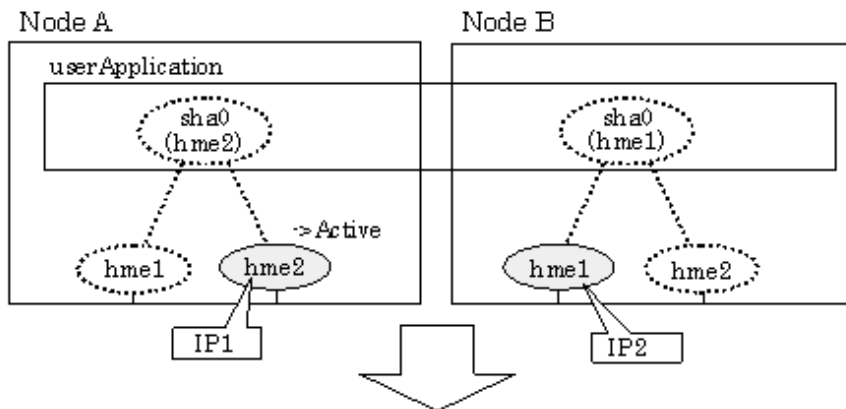


Figure 5.10 Switching behavior of NIC switching mode (takeover physical IP I)

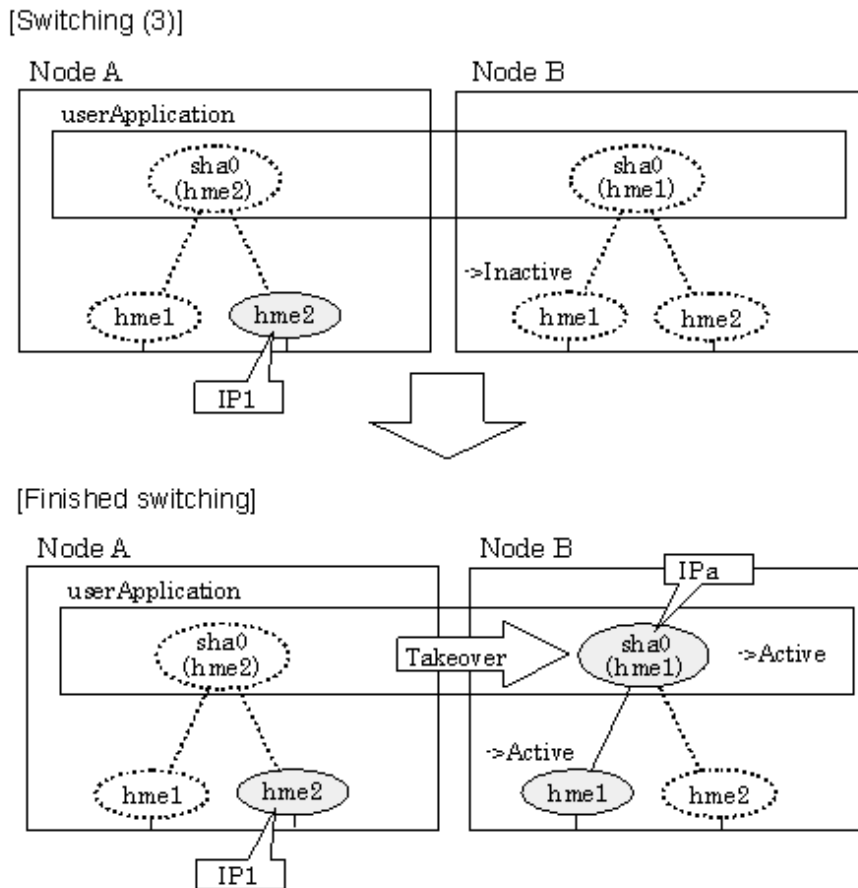
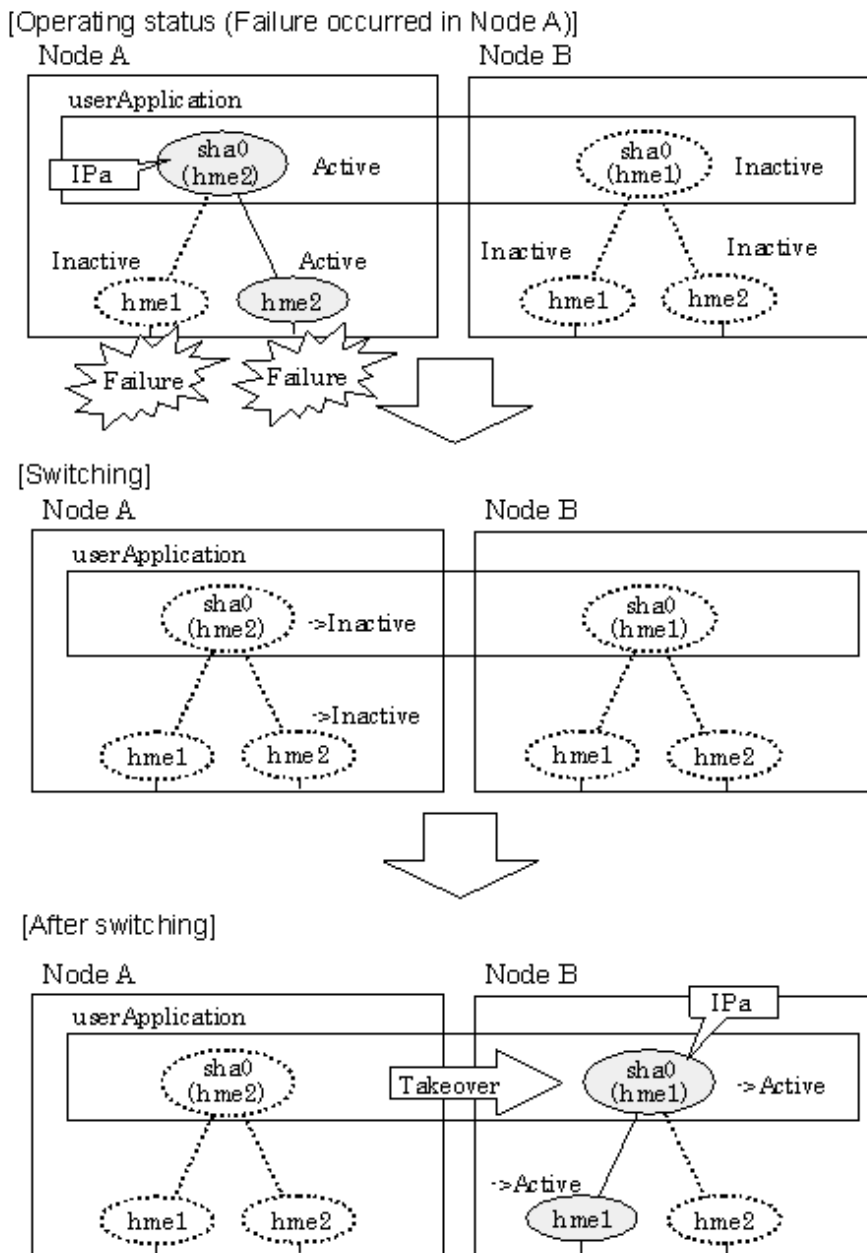


Figure 5.11 Switching behavior of NIC switching mode (takeover physical IP address II) illustrates switching behavior of NIC switching mode (takeover physical IP address II).

In the following figure, the take over IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

When switching the node because of a failure in the transfer path, the standby node B turns to be active by allocating the take over IP address (IPa) to the primary interface (hme1). After the IP address is successfully passed over to the standby node, the secondary interface (hme2), which previously owned the take over IP address (IPa) in node A becomes inactive.

Figure 5.11 Switching behavior of NIC switching mode (takeover physical IP address II)

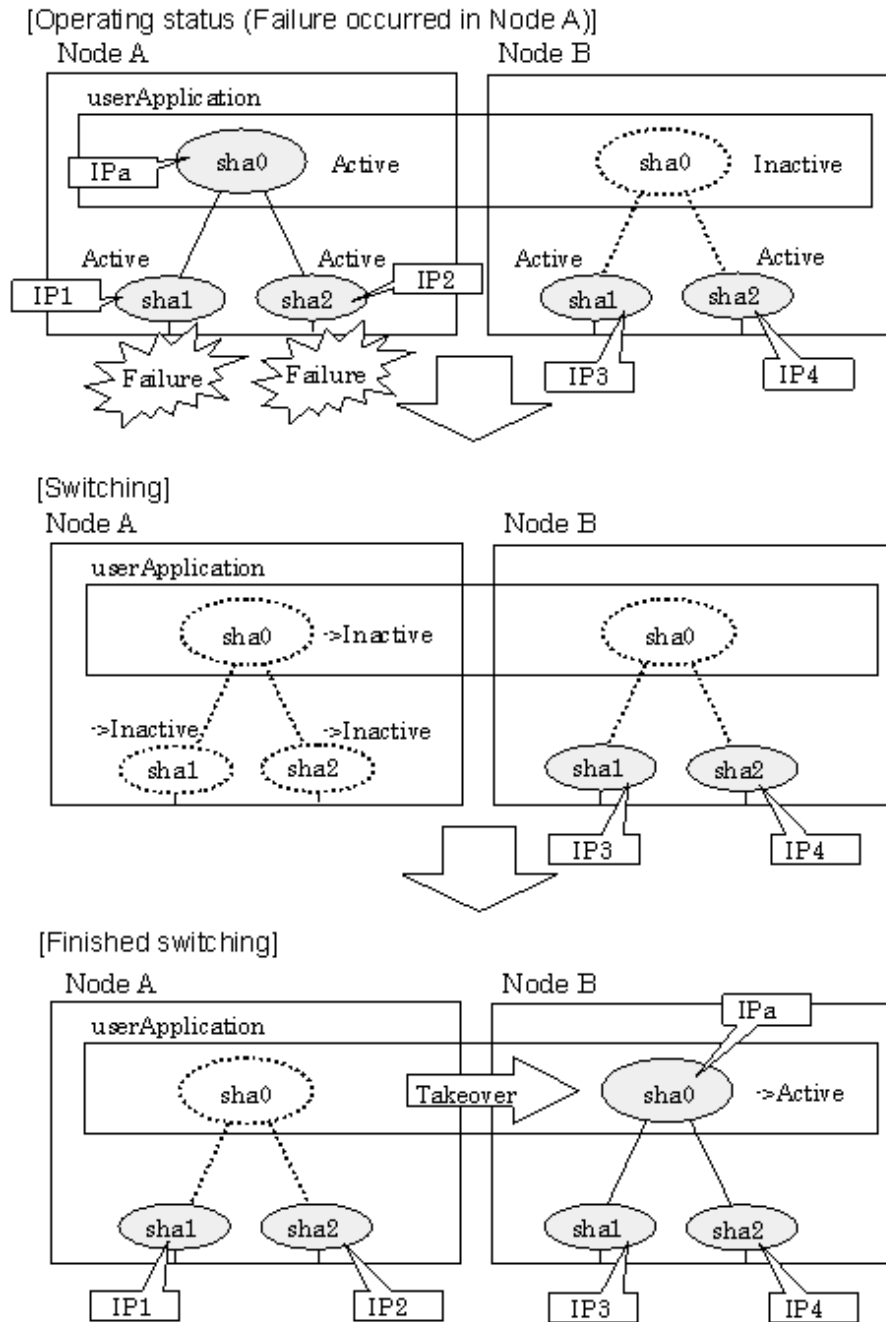


5.1.1.2.3 GS/SURE linkage mode

Figure 5.12 Switching behavior of GS/SURE linkage mode illustrates switching behavior of GS/SURE linkage mode.

In the figure below, a takeover virtual interface (sha0) is activated in the operating node. When switching occurs due to a failure, deactivate takeover virtual interface (sha0) and the virtual interfaces (sha1, sha2) in node A. Then, GS/SURE linkage mode activates the virtual interfaces (sha1, sha2). On standby node B, it activates the takeover virtual interface (sha0), which bundles the virtual interfaces (sha1, sha2).

Figure 5.12 Switching behavior of GS/SURE linkage mode



5.1.1.3 Fail-back

The following shows a procedure of performing fail-back after failure recovery if node switching occurs.

1) Make recovery for a node on which a failure has occurred.

If switching has occurred due to panic or hang-up, reboot the node that has panicked or hanged up.

If switching has occurred due to a line failure, restore the line to a normal status (perform necessary work such as reconnecting a cable, powering on a HUB again, and replacing a faulty HUB).

2) Restore the original operation status.

Restore the original operation status by performing fail-back operation for userApplication.

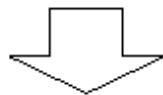
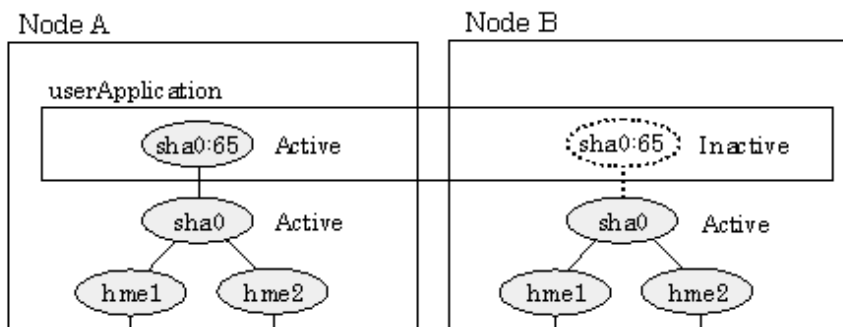
5.1.1.4 Stopping

5.1.1.4.1 Fast switching mode

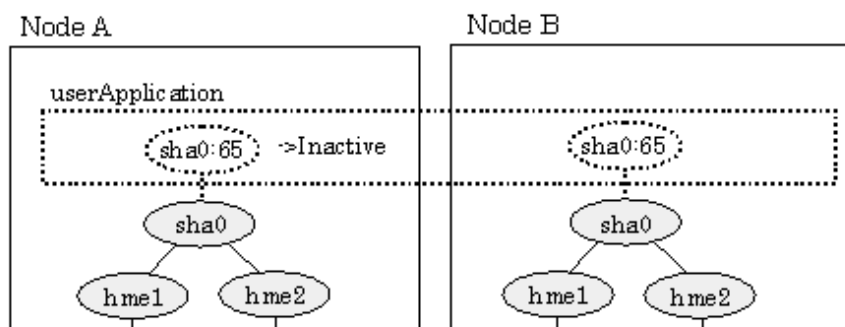
Figure 5.13 Stopping behavior of Fast switching mode illustrates stopping process of userApplication.

Figure 5.13 Stopping behavior of Fast switching mode

[Before an userApplication stop]



[After an userApplication stop]

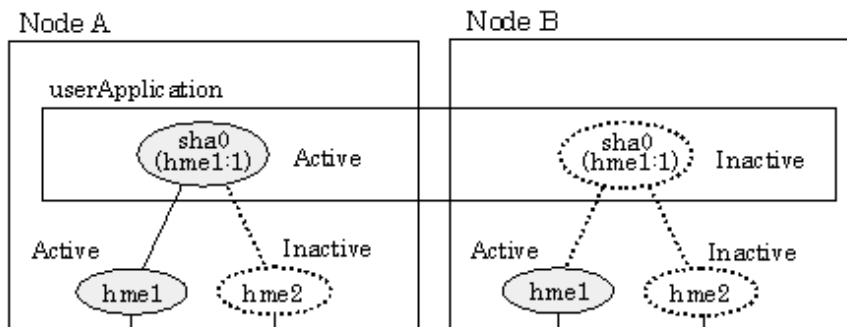


5.1.1.4.2 NIC switching mode

Figure 5.14 Stopping process of NIC switching mode (logical IP takeover) illustrates stopping process of userApplication for logical IP takeover.

Figure 5.14 Stopping process of NIC switching mode (logical IP takeover)

[Before an userApplication stop]



[After an userApplication stop]

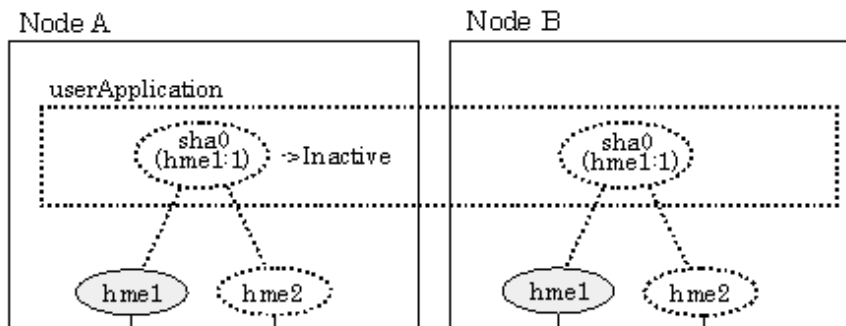
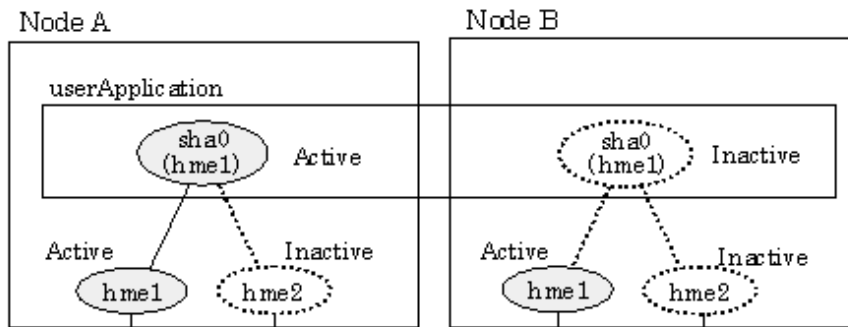


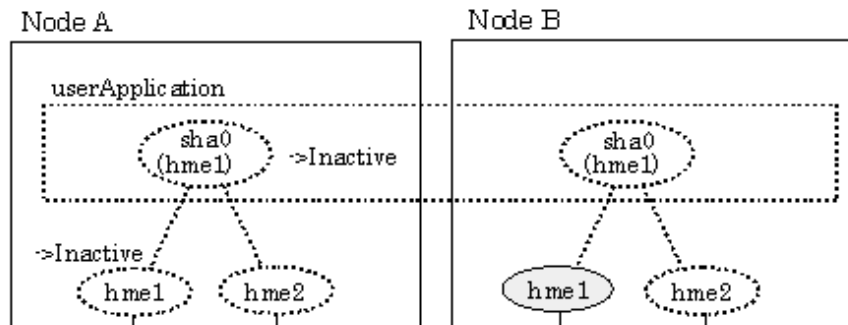
Figure 5.15 Stopping process of NIC switching mode (physical IP takeover) illustrates stopping behavior of userApplication for the physical IP takeover I.

Figure 5.15 Stopping process of NIC switching mode (physical IP takeover)

[Before an userApplication stop]



[Stopping]



[After an userApplication stop]

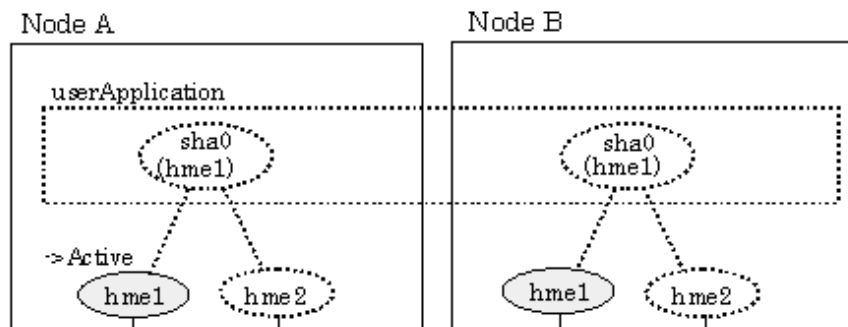
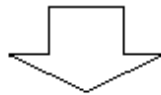
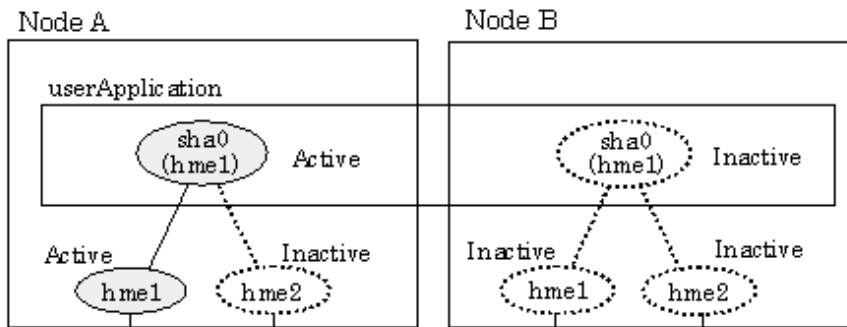


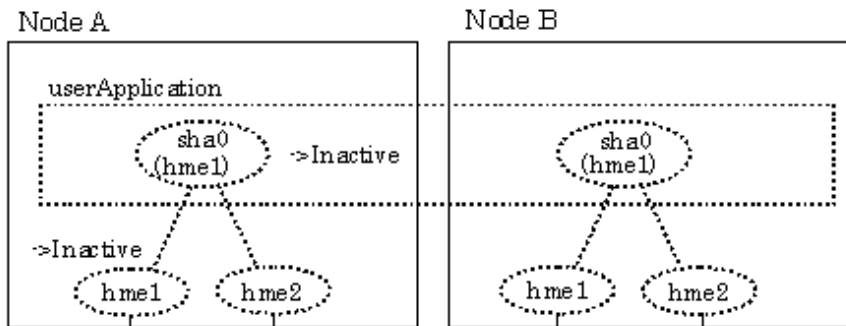
Figure 5.16 Stopping process of NIC switching mode (physical IP takeover II) illustrates stopping behavior of userApplication for the physical IP takeover II.

Figure 5.16 Stopping process of NIC switching mode (physical IP takeover II)

[Before an userApplication stop]



[After an userApplication stop]

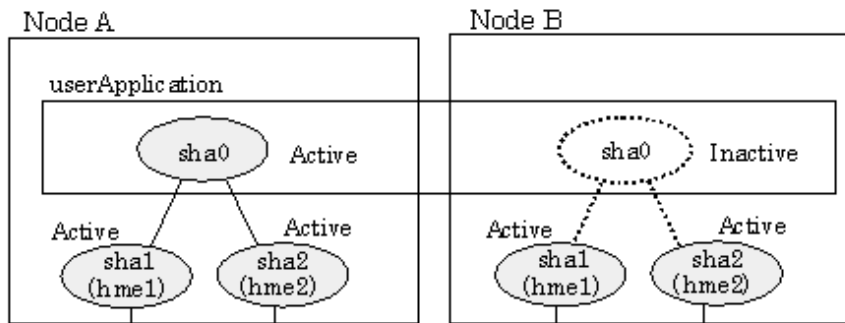


5.1.1.4.3 GS/SURE linkage mode

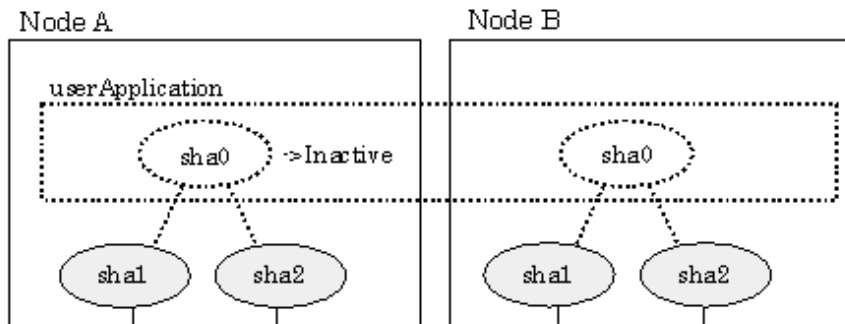
Figure 5.17 Stopping process of GS/SURE linkage mode illustrates stopping behavior of userApplication.

Figure 5.17 Stopping process of GS/SURE linkage mode

[Before an userApplication stop]



[After an userApplication stop]



5.1.2 Mutual standby

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

5.1.2.1 Starting

Starting process is equivalent to the standby operation, except that the mutual standby operation contains various userApplications. For details, please refer to "5.1.1.1 Starting".

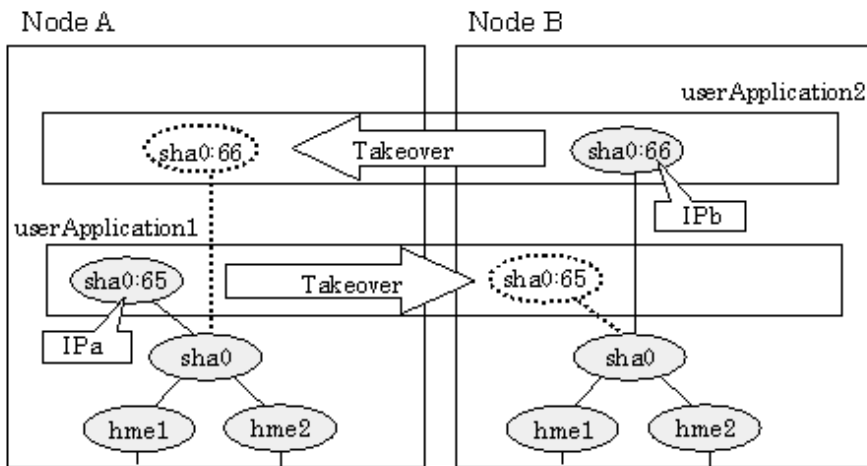
5.1.2.2 Switching

Usually, userApplication communicates with the remote system using the virtual interface on each node. If a failure (such as panic, hang-up, or transfer path failure) occurs on the operating node, the virtual interface comprised in that corresponding node is passed over to the standby node. With an application allowing reconnection, it takes over the connection of the operating node.

5.1.2.2.1 Fast switching mode

Figure 5.18 Mutual standby configuration diagram in Fast switching mode shows the mutual standby configuration diagram of duplicated operation in Fast switching mode. The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.1 Fast switching mode".

Figure 5.18 Mutual standby configuration diagram in Fast switching mode



5.1.2.2.2 NIC switching mode

Figure 5.19 Mutual standby configuration diagram in NIC switching mode (NIC non-sharing) shows the mutual standby configuration diagram in NIC switching mode (NIC non-sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.2 NIC switching mode".

Figure 5.19 Mutual standby configuration diagram in NIC switching mode (NIC non-sharing)

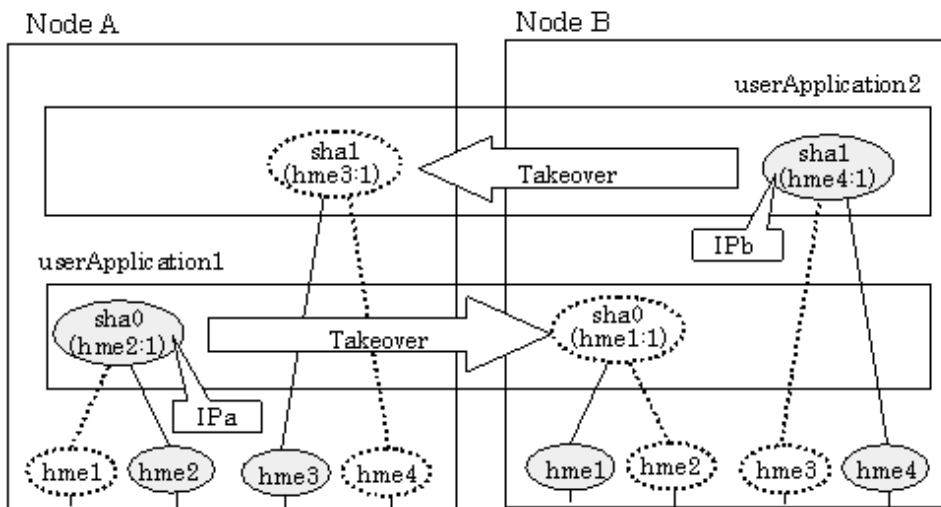
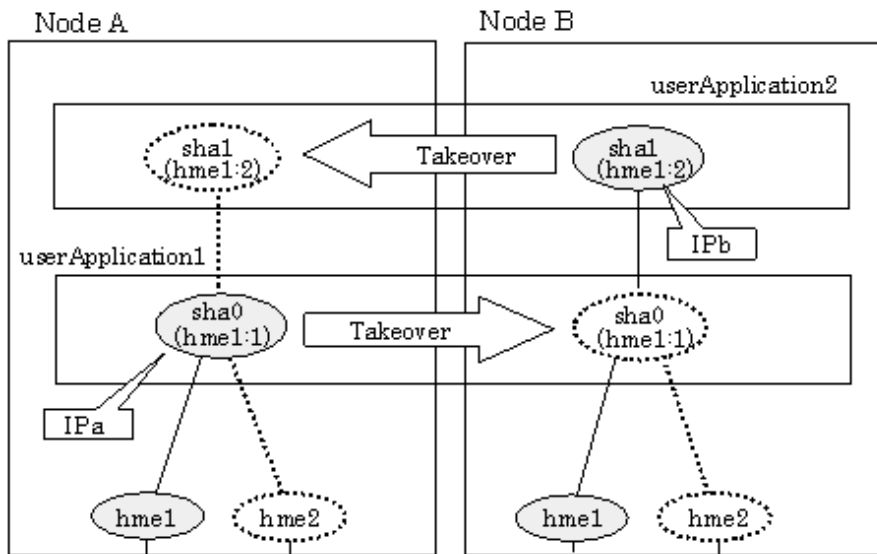


Figure 5.20 Mutual standby configuration diagram in NIC switching mode (NIC sharing) shows the mutual standby configuration diagram in NIC switching mode (NIC sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For information, see Section "5.1.1.1.2 NIC switching mode".

Figure 5.20 Mutual standby configuration diagram in NIC switching mode (NIC sharing)



5.1.2.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For more information, see "5.1.1.3 Fail-back".

5.1.2.4 Stopping

Stopping operation is equivalent to active standby connection. For detail, see "5.1.1.4 Stopping".

5.1.3 Cascade

5.1.3.1 Startup

5.1.3.1.1 Fast switching mode

When the userApplication starts up, the takeover virtual interface (sha0:65) becomes active on the operating node, allows to hold communication using the takeover virtual IP address.

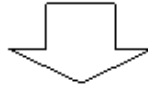
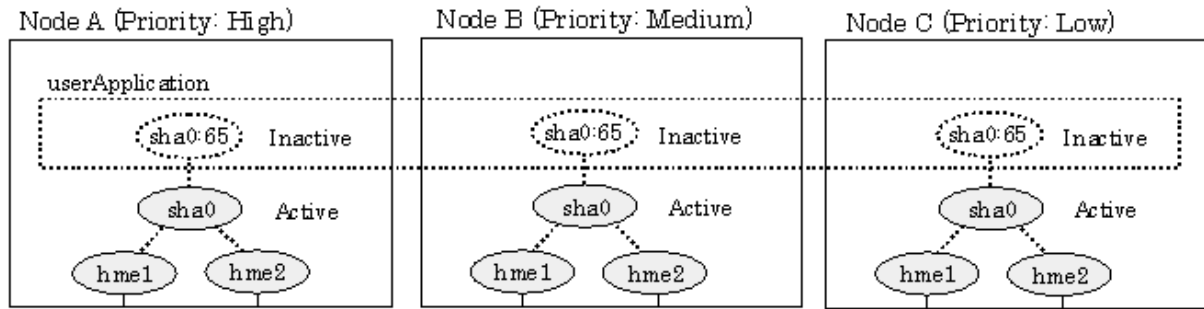
During normal operation, userApplication communicates with the remote system using the virtual interface on the operating node.

After the redundant control function start-up, the virtual interface is activated. Once it has been activated, regardless of the cluster system shutdown or restart, it stays to be active until the system shuts down.

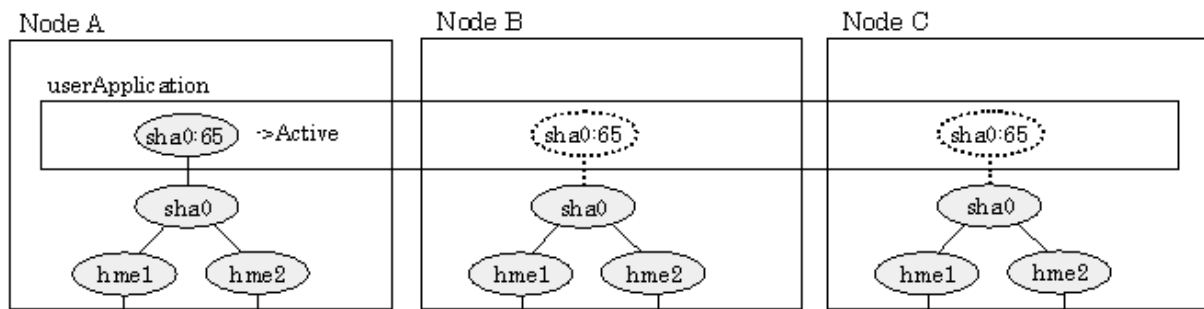
Figure 5.21 Start-up behavior of Fast switching mode illustrates start-up behavior of Fast switching mode.

Figure 5.21 Start-up behavior of Fast switching mode

[Prior to userApplication start up]



[After userApplication started]



5.1.3.1.2 NIC switching mode

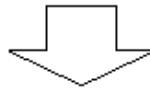
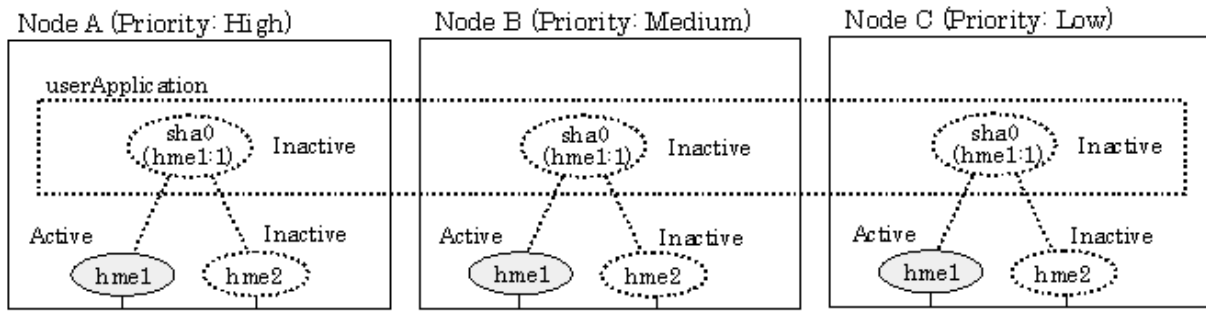
There are three types of IP takeover feature in NIC switching mode. For detail, refer to "5.1.1.1.2 NIC switching mode".

The physical interface (hme1) for each node becomes active when the redundant control function starts up for logical IP takeover. Once the userApplication starts up, takeover virtual interface (hme1:1) then becomes active on the operating node which has higher priority.

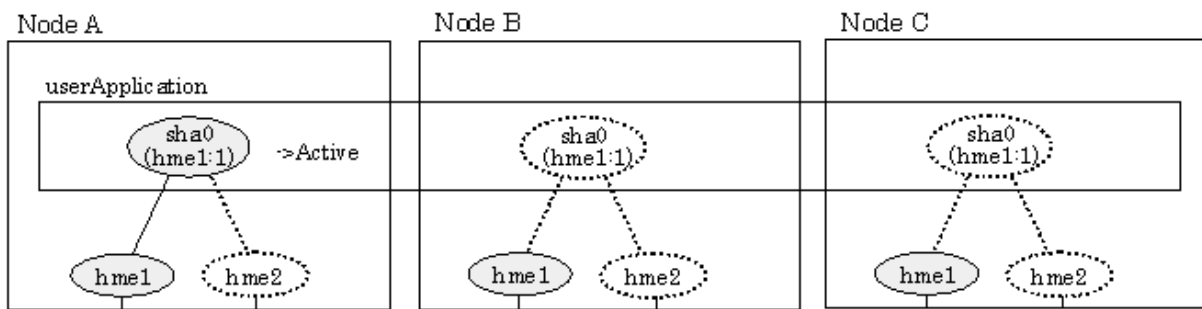
Figure 5.22 Start-up behavior of NIC switching mode (logical IP takeover) illustrates start-up behavior of logical IP takeover.

Figure 5.22 Start-up behavior of NIC switching mode (logical IP takeover)

[Prior to userApplication start up]



[After userApplication started]

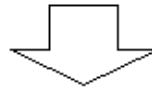
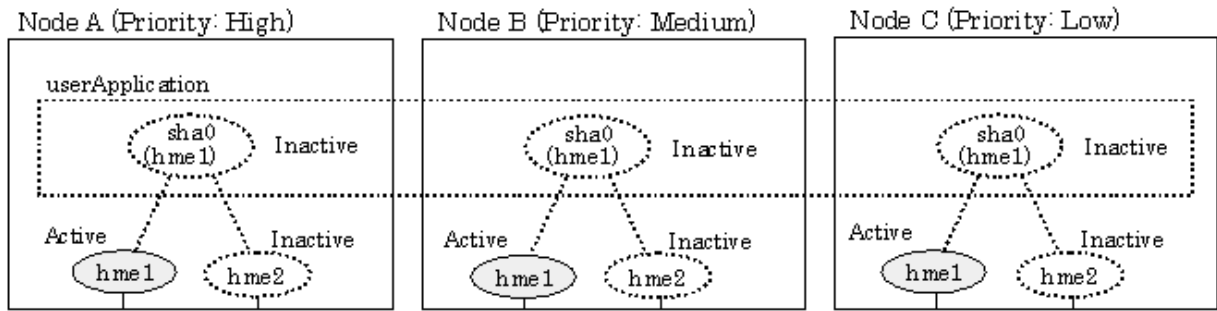


The physical interface (hme1) for each node becomes active when the redundant control function starts up for the physical IP takeover I. Once the userApplication starts up, it activates the physical interface (hme1) by allocating the take over IP address to the physical interface (hme1) on the operating node, which has a higher priority. During this process, the physical interface (hme1) on the standby node maintains its state.

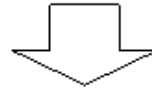
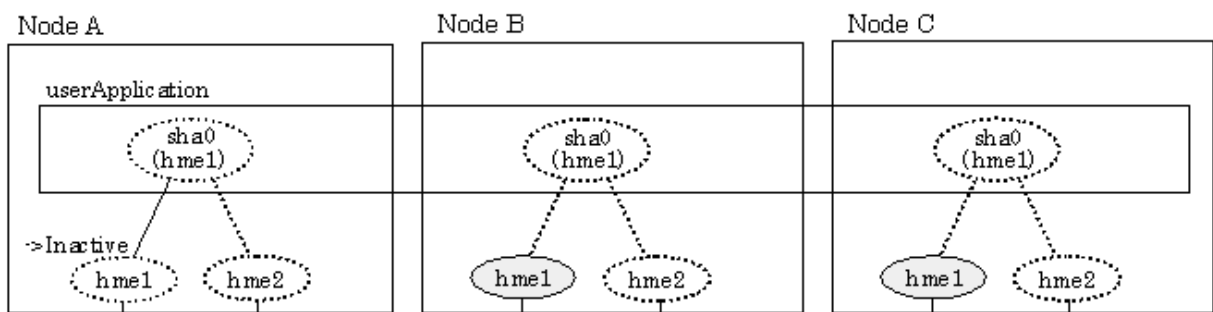
Figure 5.23 Start-up behavior of NIC switching mode (physical IP takeover) illustrates start-up behavior of the physical IP takeover I.

Figure 5.23 Start-up behavior of NIC switching mode (physical IP takeover)

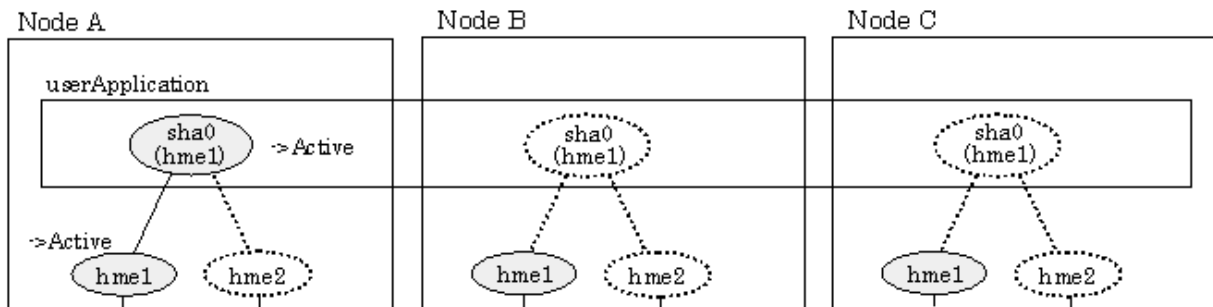
[Prior to userApplication start up]



[Starting]



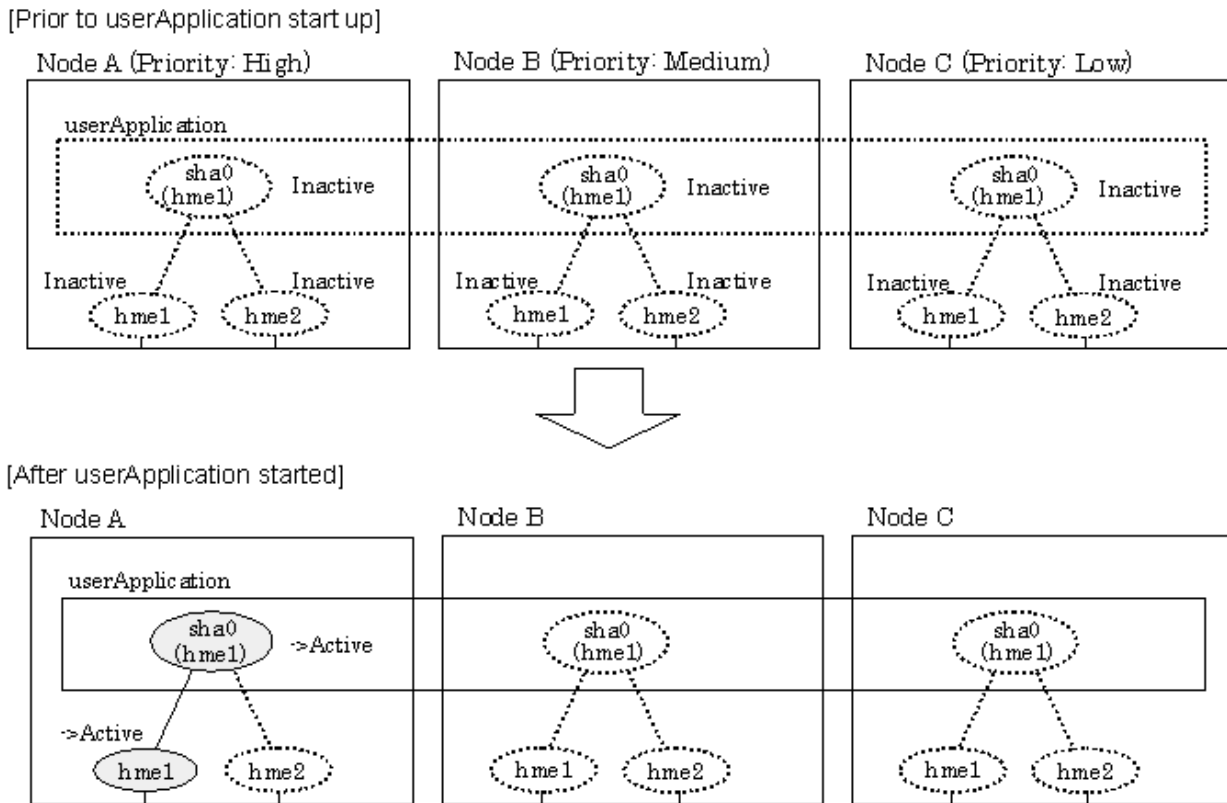
[After userApplication started]



The physical interface (hme1) for each node stays to be inactive when the redundant control function starts up for the physical IP takeover II. Once the userApplication starts up, it activates the physical interface (hme1) by allocating the take over IP address to the physical interface (hme1) on the operating node, which has a higher priority. While this process takes place, the physical interface on the standby node remains inactive.

Figure 5.24 Start-up behavior of NIC switching mode (physical IP takeover II) illustrates start-up behavior of physical IP takeover II

Figure 5.24 Start-up behavior of NIC switching mode (physical IP takeover II)



5.1.3.2 Switching

During normal operation, userApplication communicates with the remote system using the takeover virtual interface on the operating node.

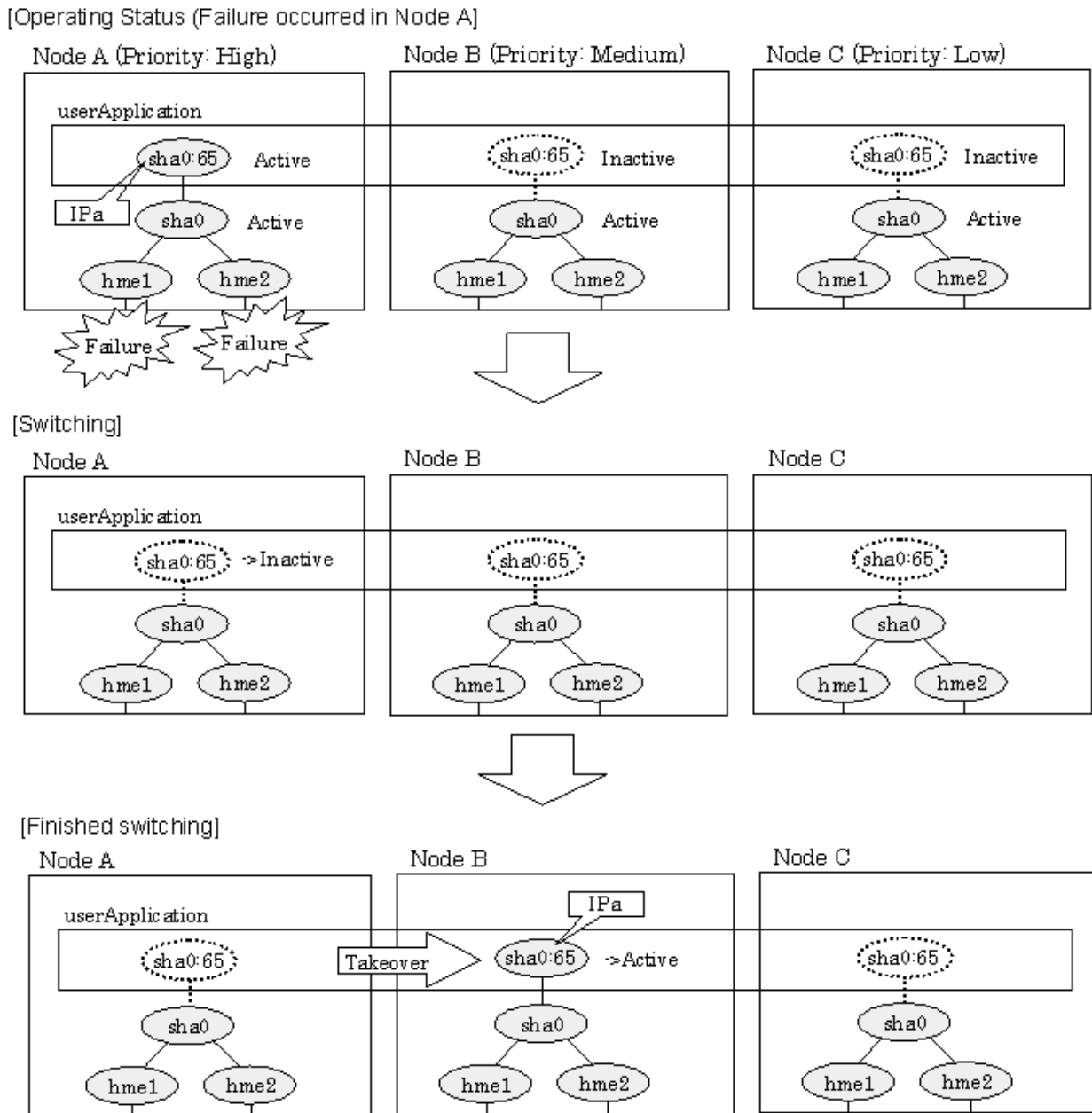
When a failure (panic, hang, detecting failure in transfer route) occurs in the operating node, redundant control function allows switching to the standby node, which has a higher priority within a several other standby nodes. It inherits the communication of operating node by reconnecting to the node using the application.

5.1.3.2.1 Fast switching mode

Figure 5.25 Switching operation of Fast switching mode illustrates switching behavior of Fast switching mode.

In the following figure, the take over IP address (IPa) is allocated to the takeover virtual interface (sha0:65) for operating node A. Then it activates the takeover virtual interface. When switching the interface due to failures in the transfer path, the takeover virtual interface (sha0:65) for operating node A becomes inactive. Then in standby node B, the takeover virtual interface (sha0:65), which has allocated the take over IP address (IPa) becomes active. Note that the virtual interface (sha0) in node A stays unchanged.

Figure 5.25 Switching operation of Fast switching mode



5.1.3.2.2 NIC switching mode

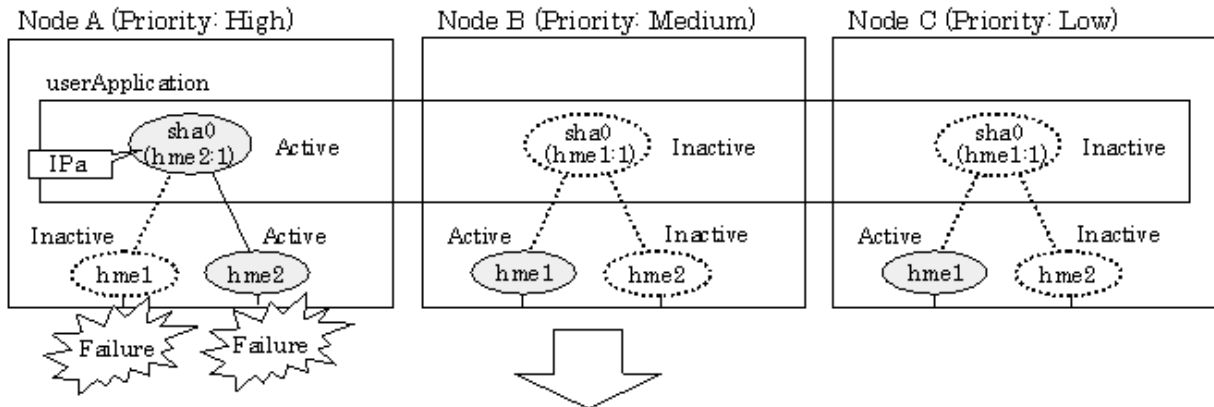
Figure 5.26 Switching operation of NIC switching mode (logical IP takeover) illustrates switching behavior of NIC switching mode (logical IP address takeover function).

In the following figure, the take over virtual IP address (IPa) in the operating node A is allocated to the logical interface (hme2.1) for the secondary interface. Once IPa is allocated, the logical interface (hme2.1) for the secondary interface turns into activate state.

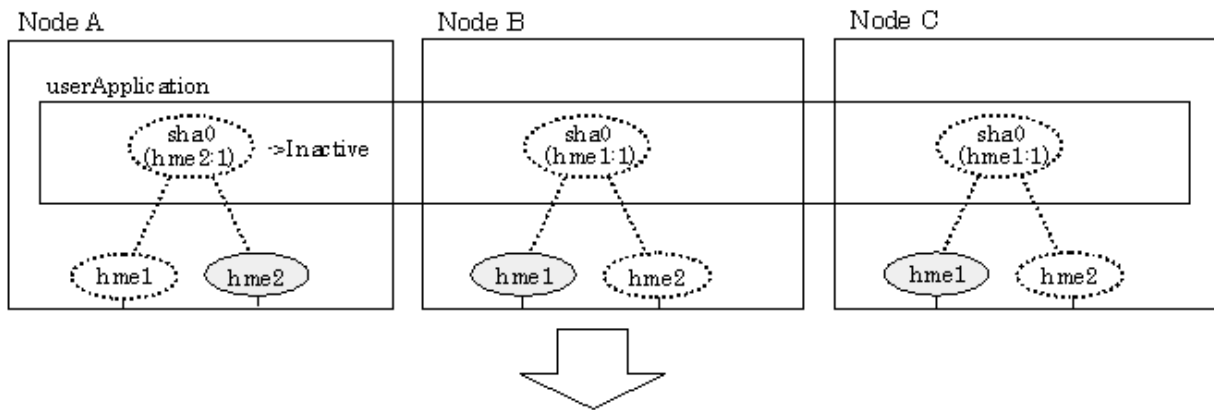
When switching the node due to failure in the transfer routes, NIC switching mode inactivates the logical virtual interface which has allocated the take over IP address (IPa) in the operating node A. Then it allocates the take over IP address to the primary interface (hme1) and finally activates the logical interface (hme1:1).

Figure 5.26 Switching operation of NIC switching mode (logical IP takeover)

[Operating Status (Failure occurred in Node A)]



[Switching]



[Finished switching]

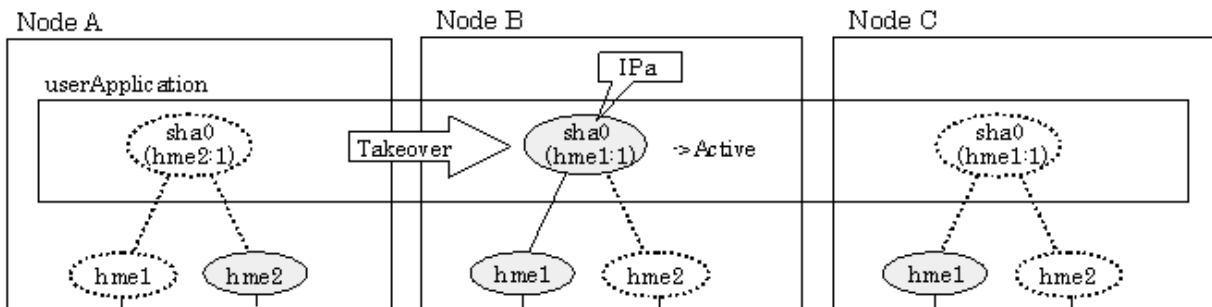


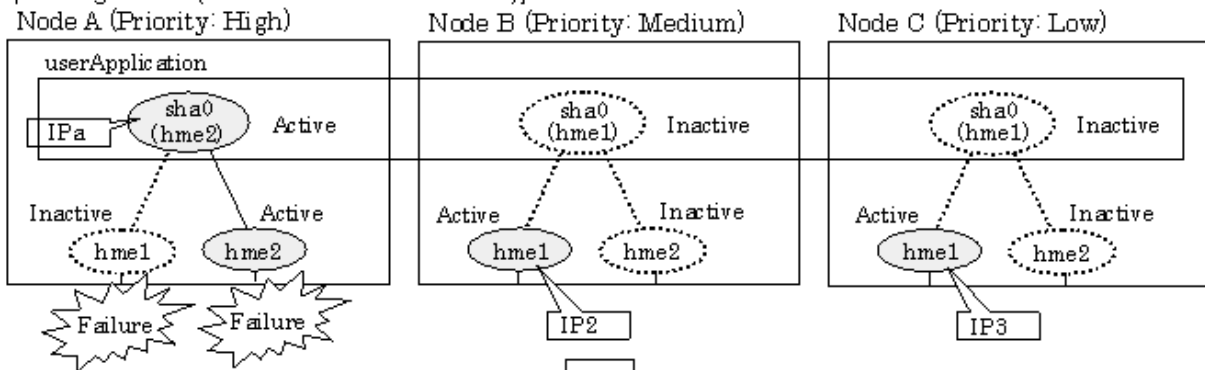
Figure 5.27 Switching operation of NIC switching mode (physical IP takeover I) (continues) and Figure 5.28 Switching operation of NIC switching mode (physical IP takeover I) illustrate switching behavior of NIC switching mode (takeover physical IP address I).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

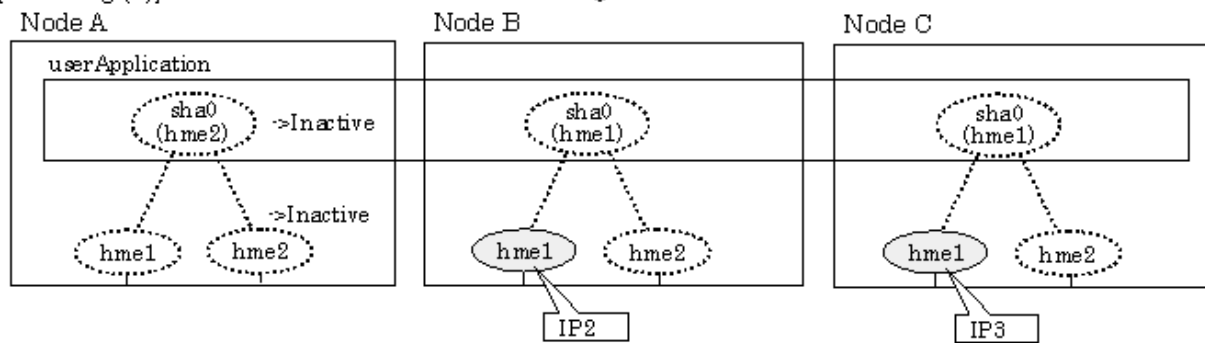
When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (hme1), which has been active in the standby node B. Then it allocates the take over IP address (IPa) to activate the primary interface (hme1). Once the primary interface activates, different IP address is allocated to the secondary interface (hme2) by means of inactivating hme2.

Figure 5.27 Switching operation of NIC switching mode (physical IP takeover I) (continues)

[Operating Status (Failure occurred in Node A)]



[Switching (1)]



[Switching (2)]

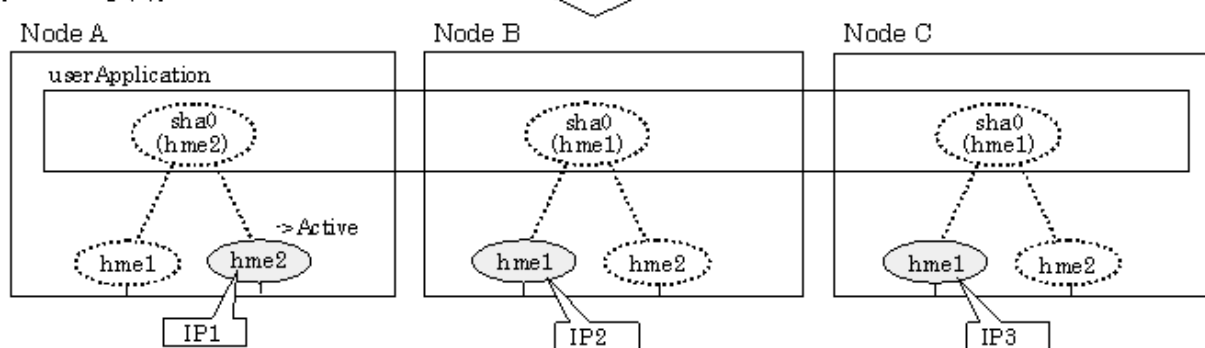


Figure 5.28 Switching operation of NIC switching mode (physical IP takeover I)

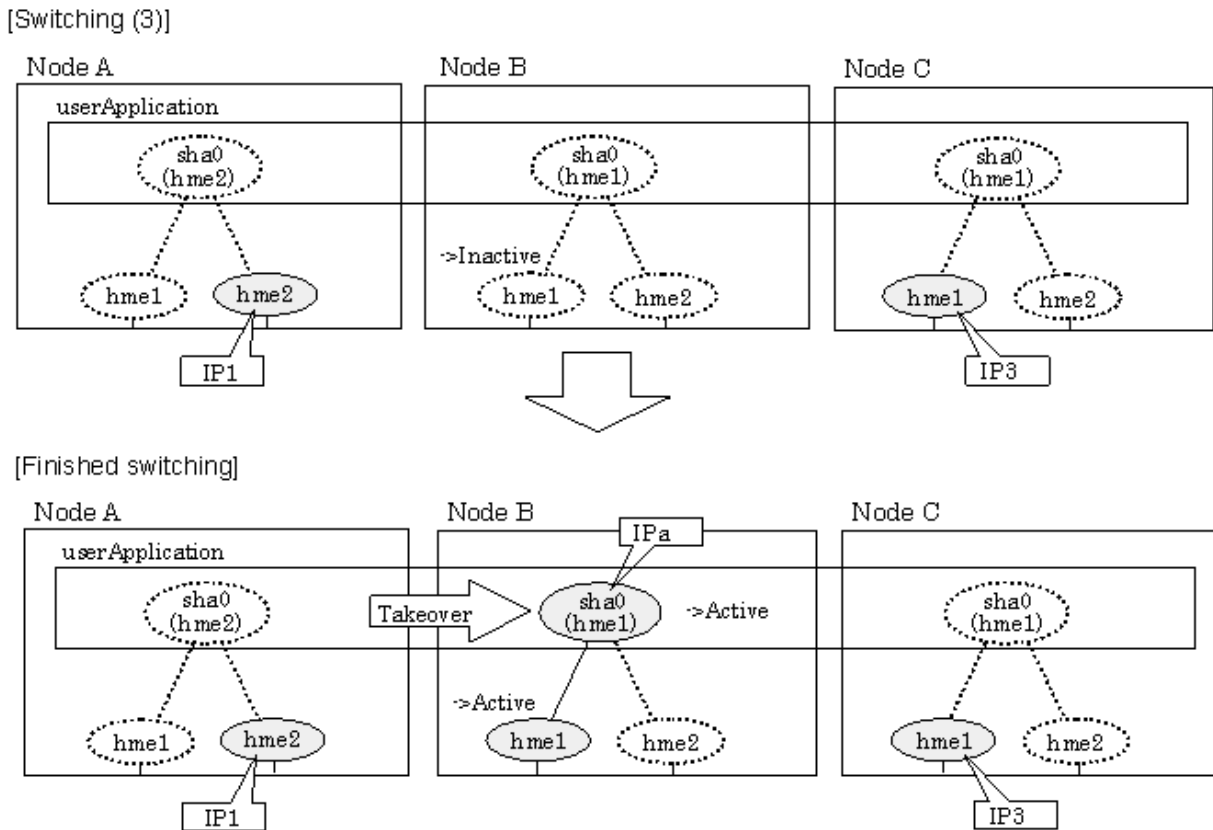
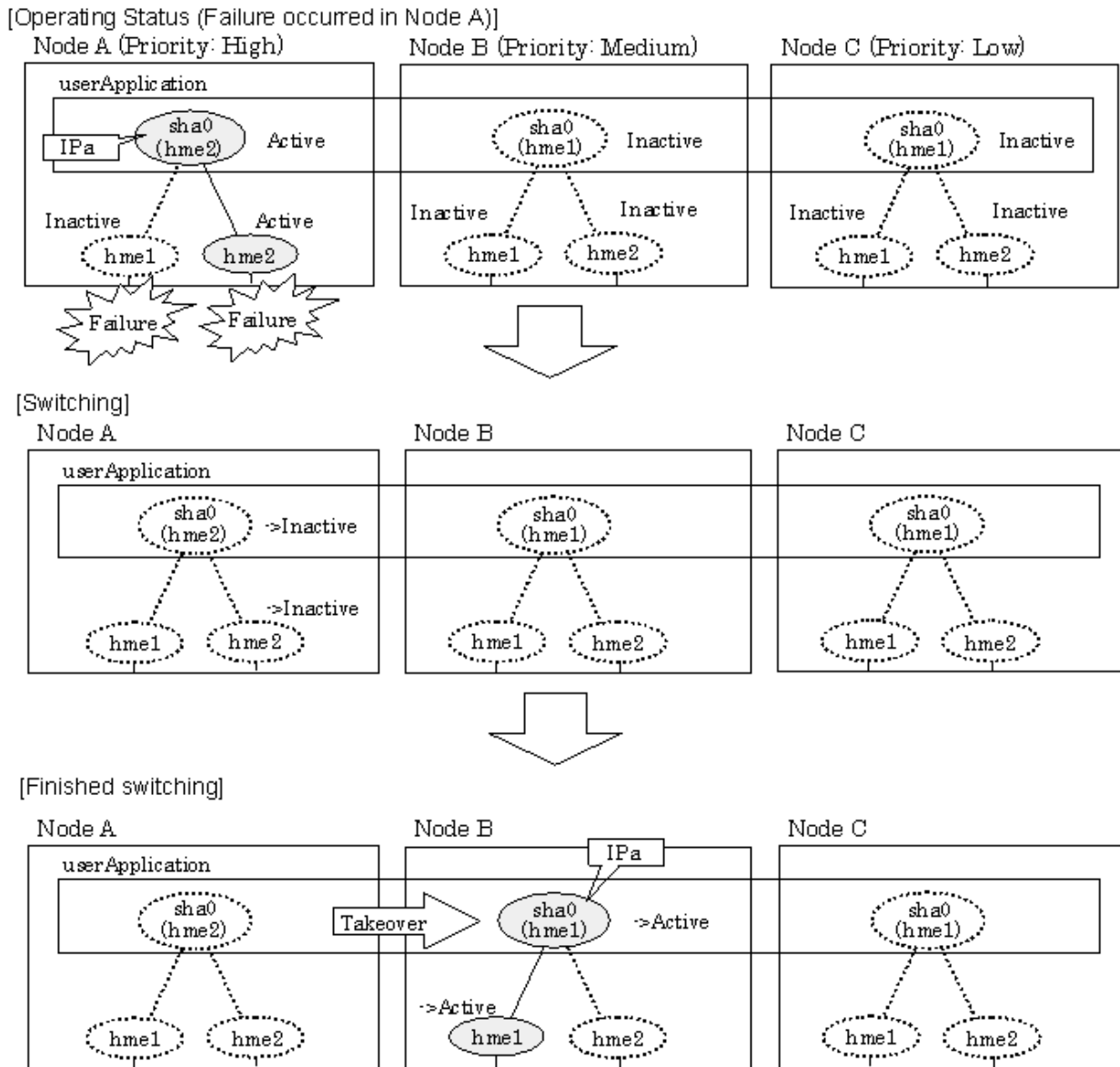


Figure 5.29 Switching operation of NIC switching mode (physical IP takeover II) illustrates switching behavior of NIC switching mode (takeover physical IP address I).

In the following figure, the take over IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

When switching the node because of a failure in the transfer path, activate the standby node B turns to be active by allocating the take over IP address (IPa) to the primary interface (hme1). After the IP address is successfully passed over to the standby node B, becomes inactive the secondary interface (hme2), which previously owned the take over IP address (IPa) in node A.

Figure 5.29 Switching operation of NIC switching mode (physical IP takeover II)



5.1.3.3 Fail-back

The following is a fail-back procedure, describing how to recover from the cluster switching.

1) Recovering the node, which encountered a failure

If switching was caused by panic or hang up, then reboot the node.

On the other hand, if switching was caused by a transfer path failure, then recover the transfer path encountered a failure. (Recovering options are reconnecting the cable, restore the power of HUB, and exchange the broken HUB.)

2) Fail-back to an arbitrary node on standby

Fails back a cluster application to an arbitrary node, which is on standby state.

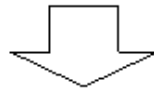
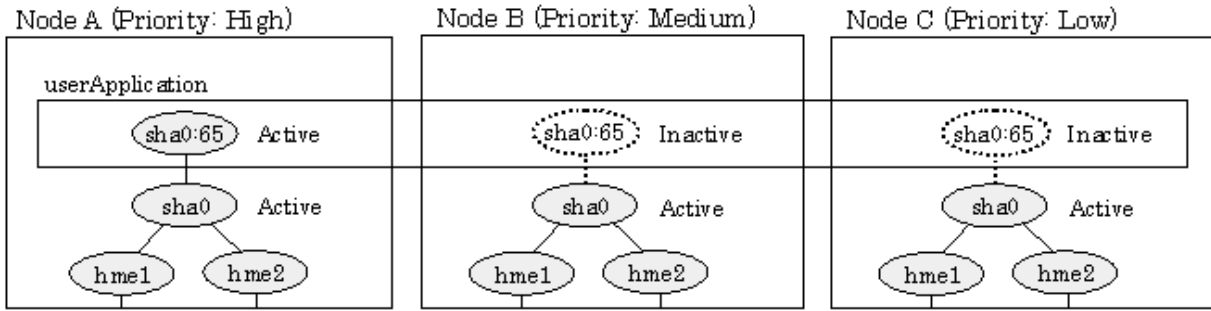
5.1.3.4 Stopping

5.1.3.4.1 Fast switching mode

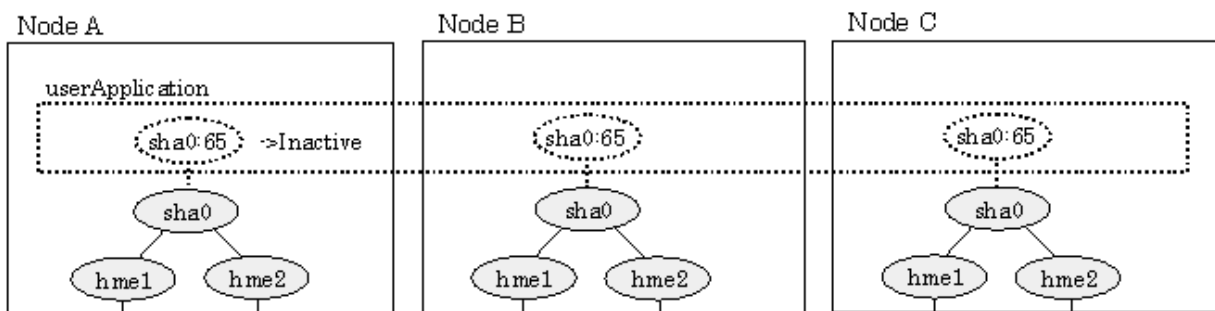
Figure 5.30 Stopping operation of Fast switching mode illustrates stopping operation of a userApplication

Figure 5.30 Stopping operation of Fast switching mode

[Before an userApplication stop]



[After an userApplication stop]

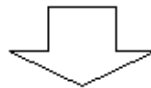
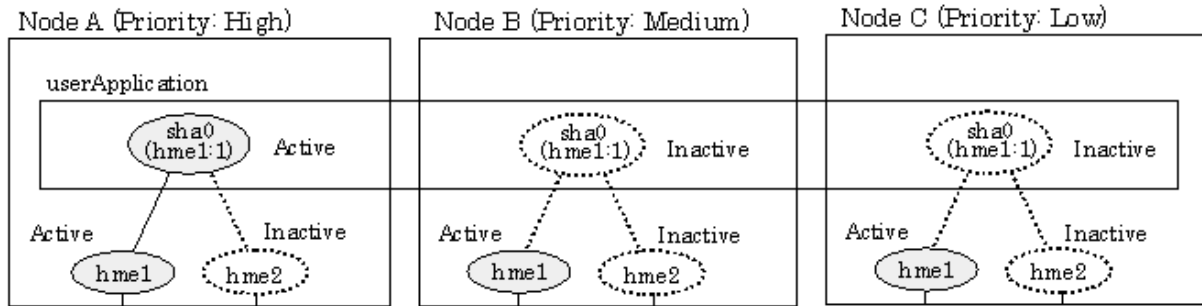


5.1.3.4.2 NIC switching mode

Figure 5.31 Stopping operation of NIC switching mode (logical IP takeover) illustrates stopping operation of a userApplication for logical IP takeover.

Figure 5.31 Stopping operation of NIC switching mode (logical IP takeover)

[Before an userApplication stop]



[After an userApplication stop]

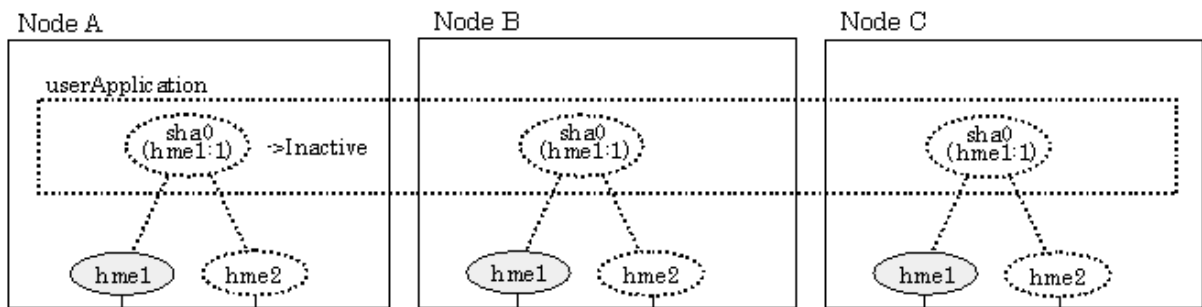
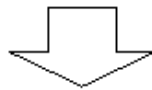
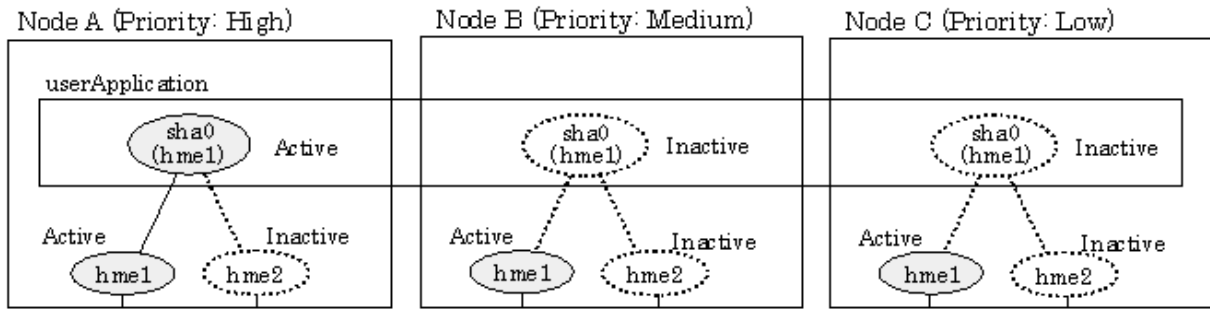


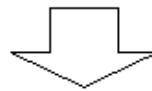
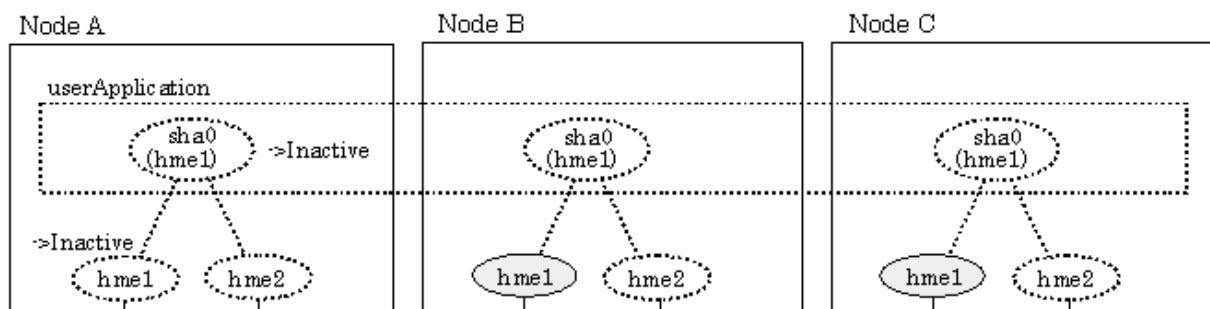
Figure 5.32 Stopping operation of NIC switching mode (physical IP takeover I) illustrates stopping operation of a userApplication for physical IP takeover I.

Figure 5.32 Stopping operation of NIC switching mode (physical IP takeover I)

[Before an userApplication stop]



[Stopping]



[After an userApplication stop]

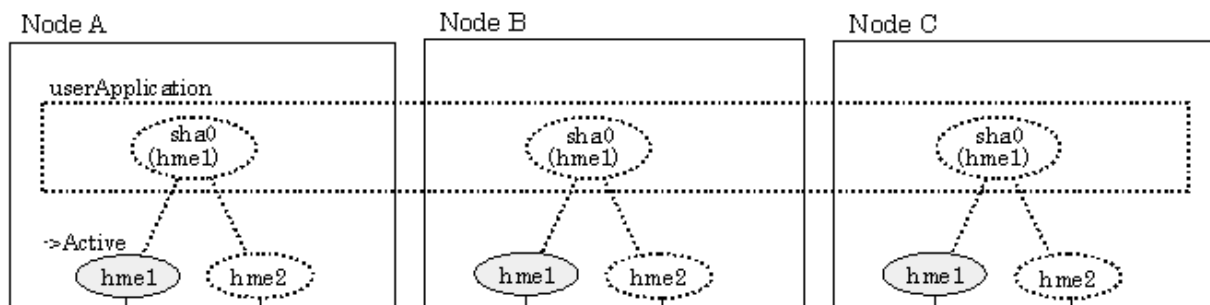
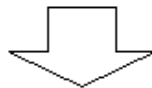
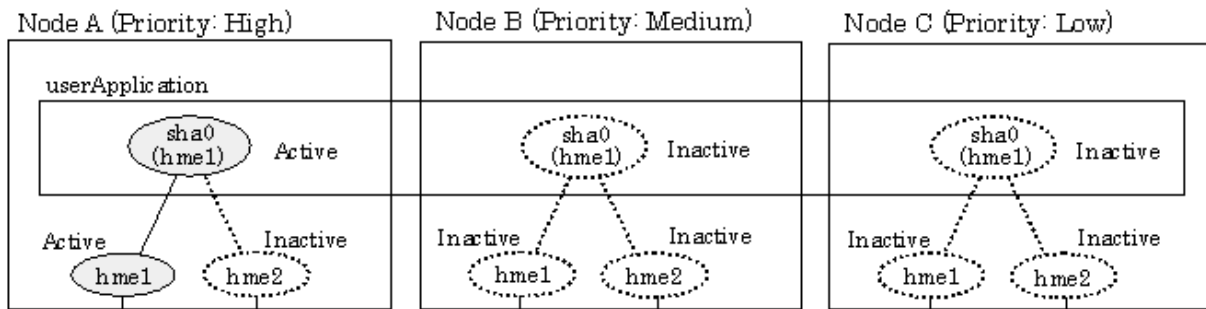


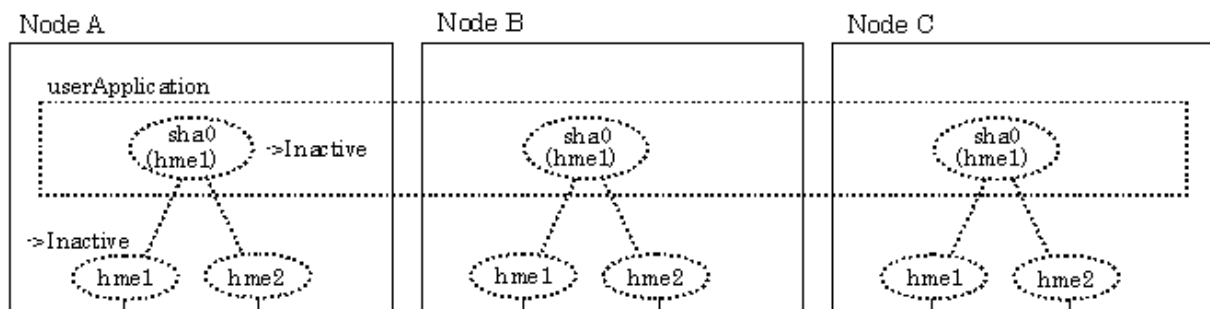
Figure 5.33 Stopping operation of NIC switching mode (physical IP takeover II) illustrates stopping operation of a userApplication for physical IP takeover II.

Figure 5.33 Stopping operation of NIC switching mode (physical IP takeover II)

[Before an userApplication stop]



[After an userApplication stop]



5.1.4 Monitoring resource status of standby node

In a userApplication for standby operation, it is possible to monitor an operating node as well as a status of resource used in standby node of GLS.

The following describes about monitoring GLS resource status of standby node.

5.1.4.1 Preface

Normally, a userApplication for standby operation does not monitor GLS resource status for standby node. In such case, even though a transfer path failure occurs in a standby node, the erroneous GLS resource remains to be unreleased and nothing is reported to the user. As a result, GLS resource error in standby node remains to be unsolved. To avoid this problem, GLS resource for standby node must be monitored with caution.

In order to monitor the GLS resource for a standby node, configure the "Standby Transition" when creating a userApplication.

Once the Standby Transition is successfully configured, it separates the erroneous GLS resource and reports the error to the user when a transfer failure occurs in a standby node. (This can be checked in "Cluster Admin" of Web-Based Admin View).



Note

When using GS/SURE linkage mode on a cluster system, the virtual interface for standby side is inactive so that the standby side stops monitoring the remote system. Due to this, it cannot monitor GLS resources on the standby node. Therefore, it is not necessary to configure "StandbyTransition" attribute while creating userApplication in GS/SURE linkage mode.

5.1.4.2 Configuration

Refer to "6.6.2 Creating UserApplications" in "PRIMECLUSTER Installation and Administration Guide" for configuration of monitoring GLS resource status for a standby node.

5.1.4.3 Recovering from a resource failure in Standby node

See the following procedure for recovering GLS resource.

1) Recovering the transfer path failure

Restore the erroneous transfer path (Reconnecting the cable, restore the power of Switch/HUB, and replace the erroneous Switch/HUB)

2) Initializing GLS resource error

Clear the erroneous GLS resource status. (Use hvutil -c)

From this operation, GLS resource for standby node is reconfigured in a userApplication as a standby status.

5.1.5 Tagged VLAN interface multiplexing on NIC switching mode (Standby)

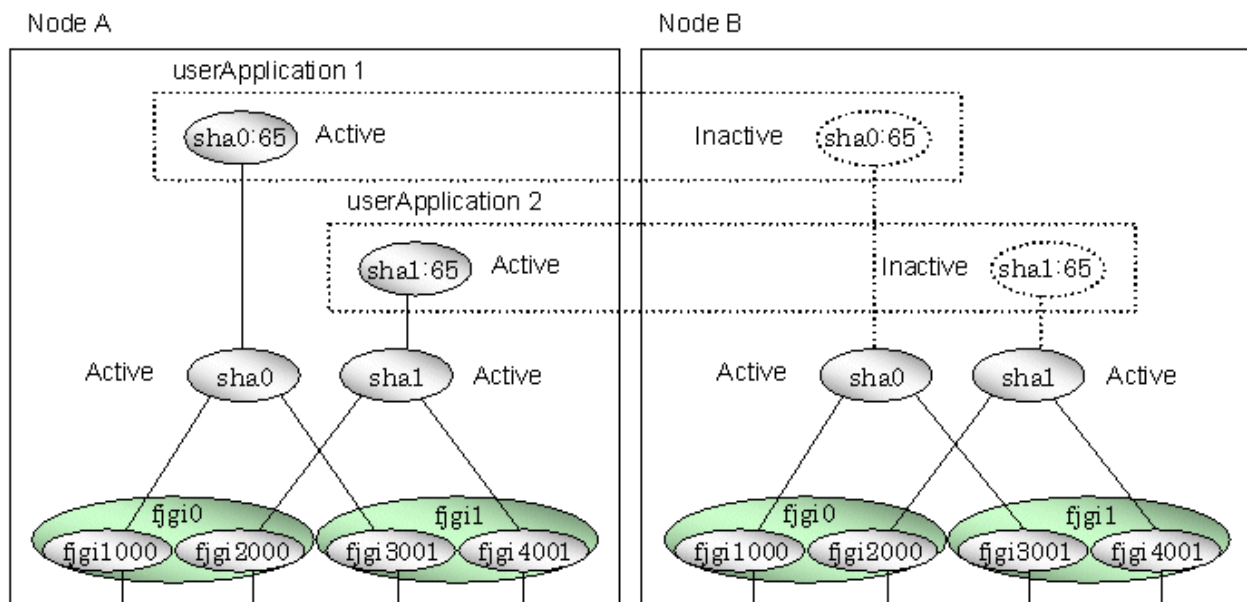
This section explains the transfer route multiplexing using tagged VLAN interface that operates on a cluster system.

5.1.5.1 Standby

5.1.5.1.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (standby).

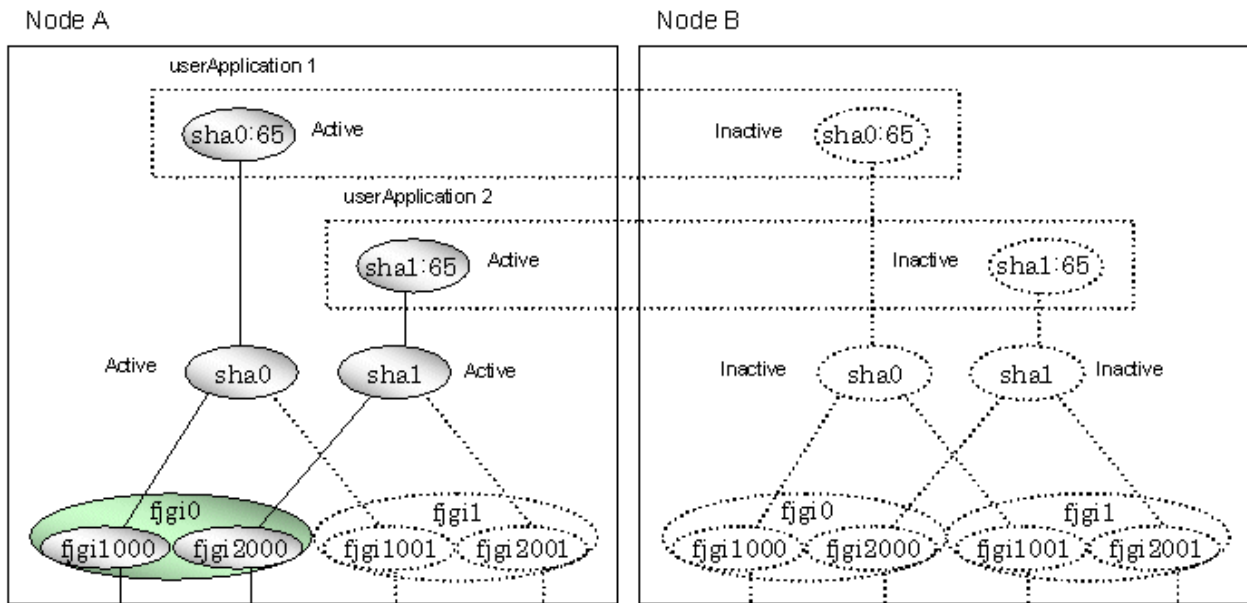
Figure 5.34 Tagged VLAN interface multiplexing on Fast switching mode (Standby)



5.1.5.1.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (standby).

Figure 5.35 Tagged VLAN interface multiplexing on NIC switching mode (Standby)

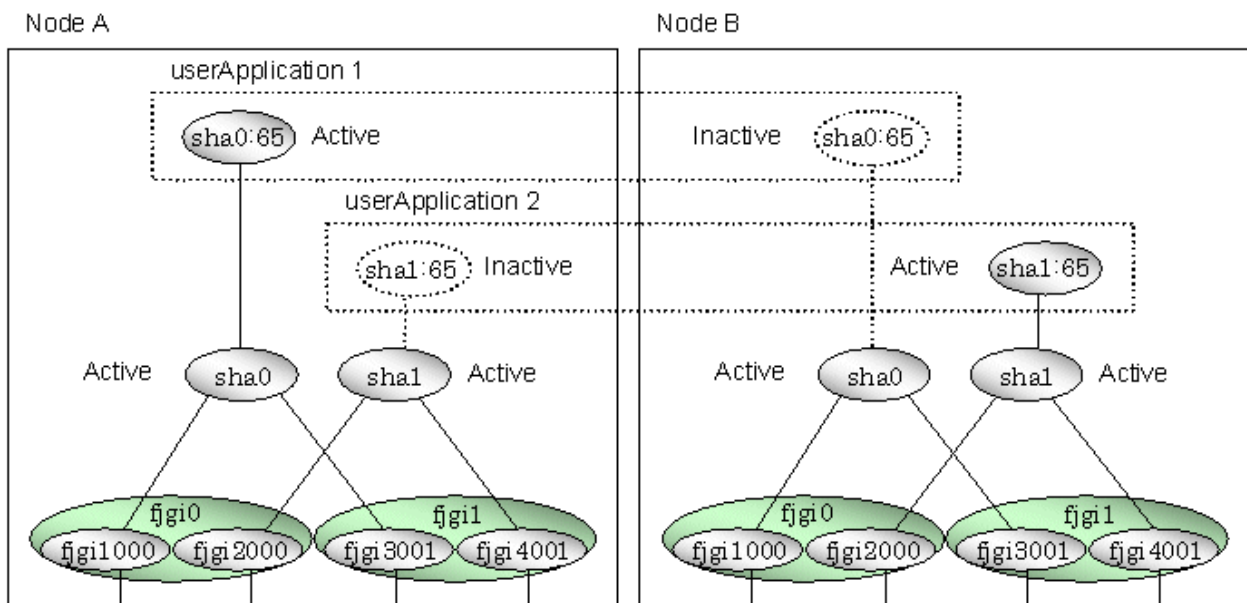


5.1.5.2 Mutual Standby

5.1.5.2.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

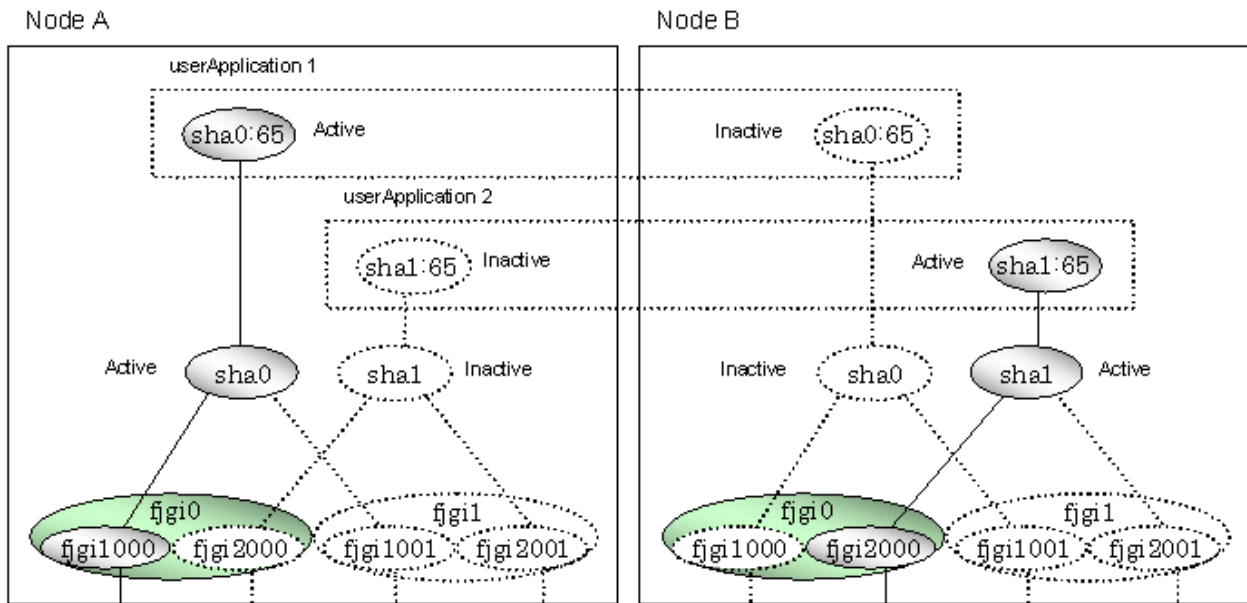
Figure 5.36 Tagged VLAN interface multiplexing on Fast switching mode (Mutual Standby)



5.1.5.2.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

Figure 5.37 Tagged VLAN interface multiplexing on NIC switching mode (Mutual Standby)

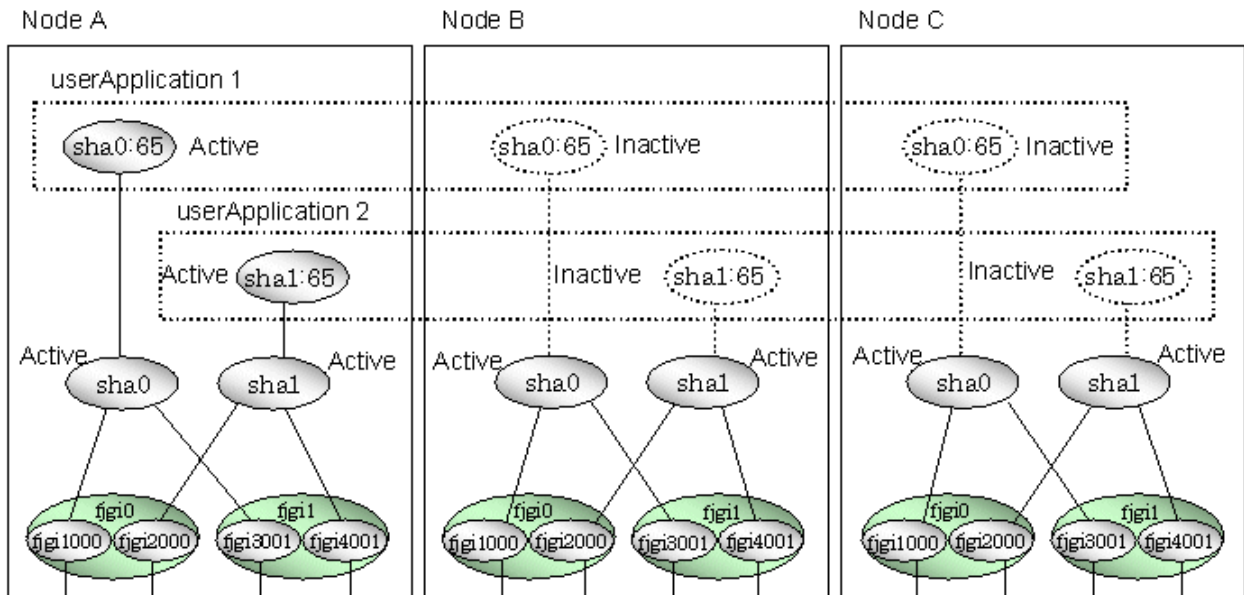


5.1.5.3 Cascade

5.1.5.3.1 Fast switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

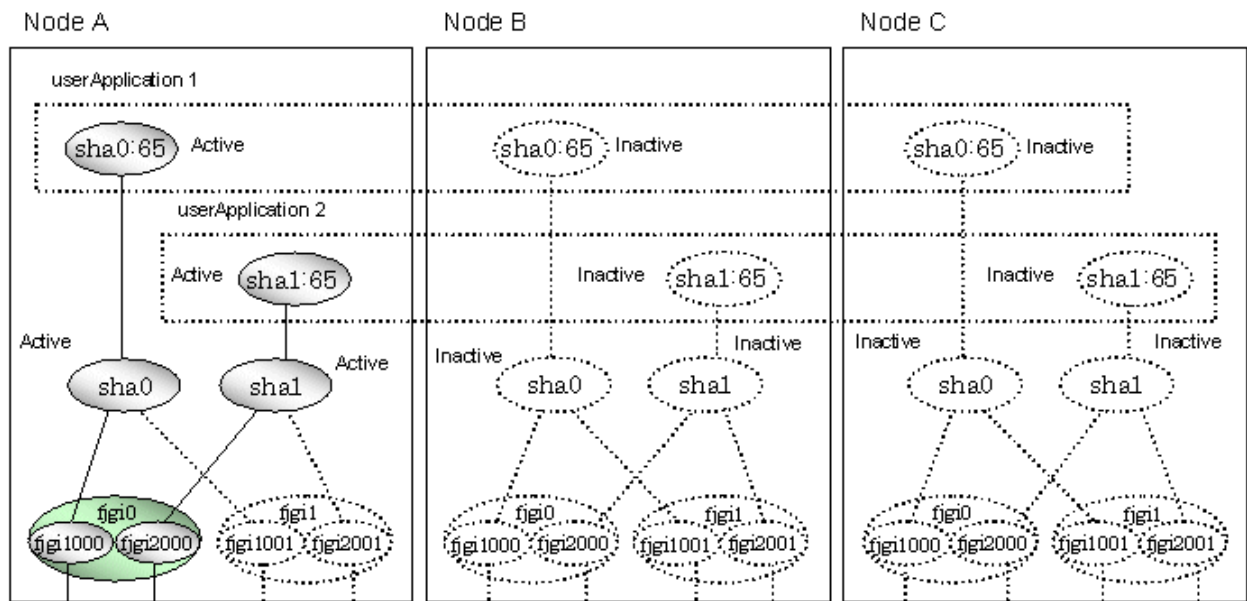
Figure 5.38 Tagged VLAN interface multiplexing on Fast switching mode (Cascade)



5.1.5.3.2 NIC switching mode

When specifying tagged VLAN interfaces for creating a virtual interface, the ones on disparate physical interfaces must be used. The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

Figure 5.39 Tagged VLAN interface multiplexing on NIC switching mode (Cascade)

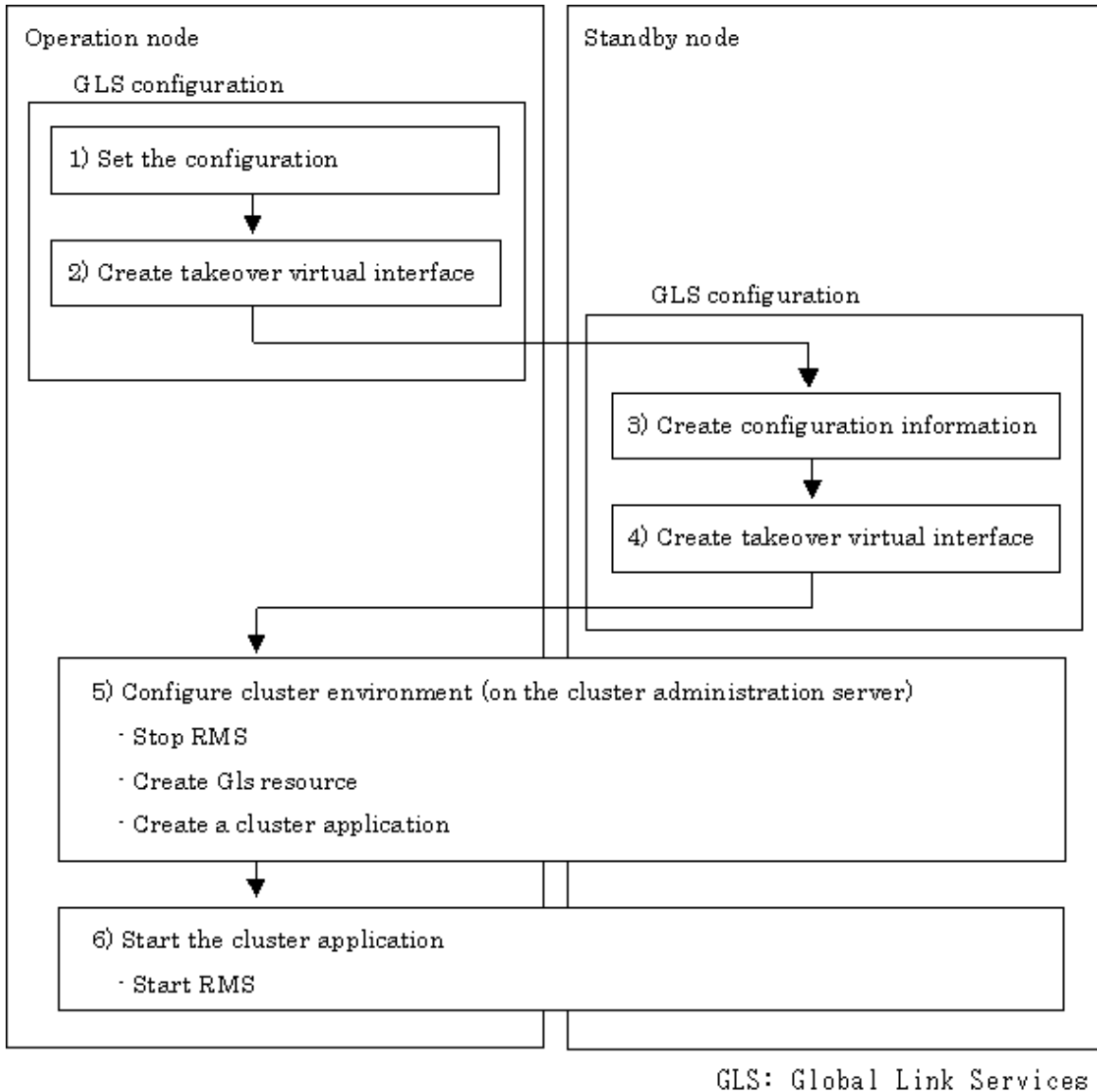


5.2 Adding configuration for Cluster System

In addition to configuring standard environment, configuration of takeover virtual interface and cluster environment is required for the cluster system.

Figure 5.40 Flowchart for adding configuration for cluster system shows a flow chart of configuring additional cluster environment for 1:1 Standby Operation. For mutual standby and N:1 operation standby, follow the steps from "1) Set the configuration information" to "5) Setup the cluster environment" for the number of necessary node. Refer to "Appendix B Examples of configuring system environments".

Figure 5.40 Flowchart for adding configuration for cluster system



Redundant Line Control function provides commands for defining cluster operations. To execute these commands, cluster system must be installed in the system.

Table 5.3 Cluster definition operation commands lists the cluster definition operation commands.

Table 5.3 Cluster definition operation commands

| Type | Command | Function | Authority |
|---|-----------------------------------|--|------------|
| Registration/ deletion/display of a virtual interface and the takeover resources. | /opt/FJShanet/usr/sbin/hanethvrsc | Registers/deletes/displays a virtual interface and the takeover resources. | Super user |

5.2.1 Creating configuration information

Create the necessary configuration information for constructing a virtual interface. The information must be created on both the active and standby nodes. For details about the creation procedure, see "Chapter 3 Environment configuration".

5.2.2 Creating Takeover virtual interface

Takeover virtual interface for registering with userApplication is set up. It is necessary to perform this setup on all nodes. When setting for Fast switching mode, it is necessary to set a "take over IP address". (Not necessary to set for NIC switching mode.) An example of the setting is as follows. See "[7.14 hanethvrsc Command](#)" for the detail of the command.



.....

If IPv6 address is used for the takeover virtual interface in Fast switching mode or NIC switching mode, it may take approximately 30 seconds to resume the connection after switching the node. However, by preliminary starting IPv6 routing daemon, the connection can be resumed immediately after switching the node. For details, refer to "[G.3 Troubleshooting](#)".

.....

[Configuring a takeover virtual interface]

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n "virtual-interface-name" [-i  
takeover-IP-address]
```

5.2.3 Configuring cluster system

Register the takeover virtual interface created in "[5.2.2 Creating Takeover virtual interface](#)" as GIs resource, and create a userApplication. Cluster system can be configured using RMS Wizard. Refer to "PRIMECLUSTER Installation and Administration Guide" for details.

5.2.4 Starting a userApplication

After completing the configuration for a cluster system, start the userApplication.
Refer to "PRIMECLUSTER Installation and Administration Guide" for details.

5.3 Modifying configuration for Cluster System

Configuration information and takeover resource information operated by the cluster system cannot be changed directly. Delete the takeover resource information first, and after changing corresponding configuration information, register the takeover resources information again.

5.4 Deleting configuration for Cluster System

For deleting the configuration of a cluster system, follow the figure below. For mutual standby operation, follow the steps from "2) Delete takeover virtual interface" up to "5) Delete configuration information" for the number of necessary nodes.

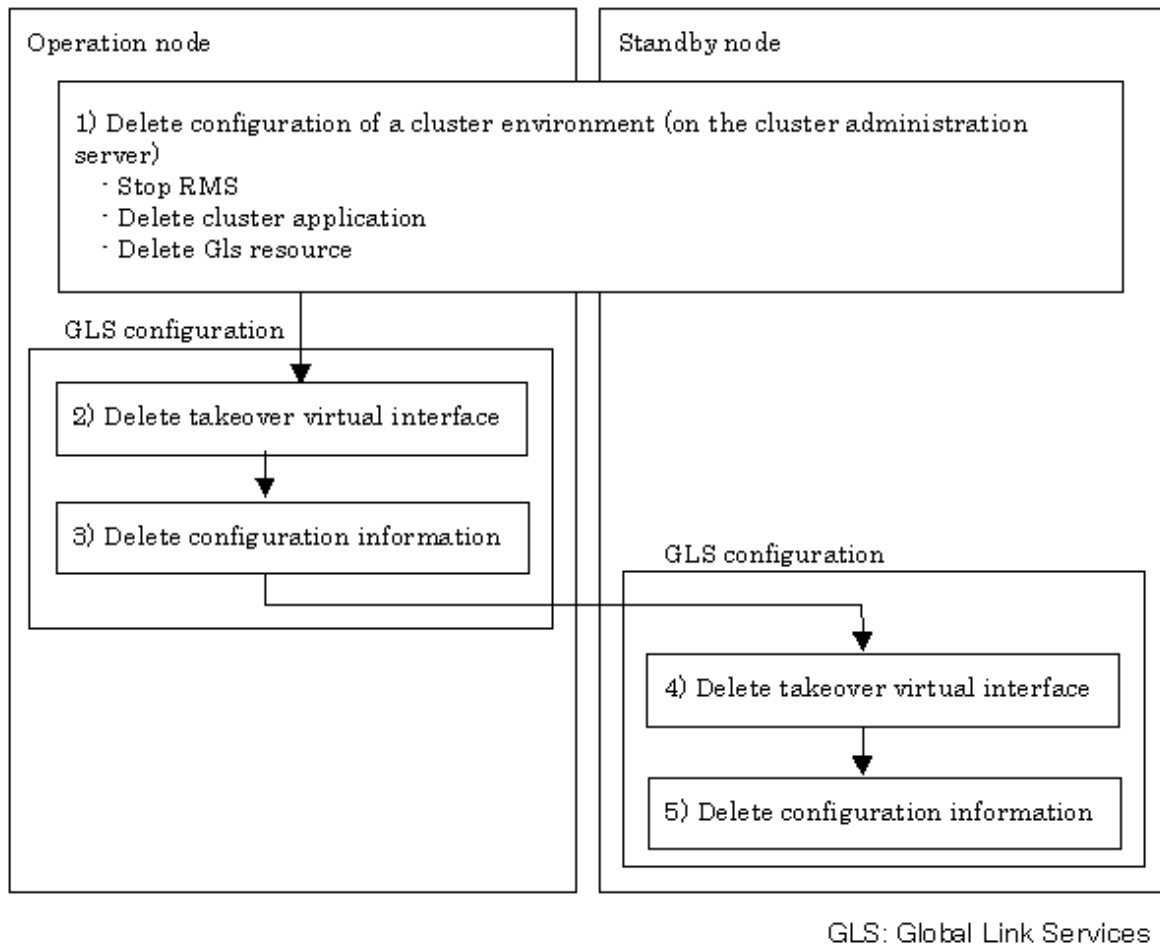


.....

Before deleting cluster configuration settings, it is recommended to backup the configuration settings of the cluster system. By preliminary backing up the configuration settings, it is possible to restore the system in case system trouble occurs and unable to recover from it. Refer to "[5.5 Backup/Restore Cluster configuration settings](#)" for details.

.....

Figure 5.41 Flowchart for deleting configuration for cluster system



5.4.1 Deleting configuration for a cluster environment

Stop the RMS and delete the userApplication and Gls resource. Use RMS Wizard for this operation. Refer to "PRIMECLUSTER Installation and Administration Guide" for detail.

5.4.2 Deleting Takeover virtual interface

Delete a virtual interface to control a cluster from the resources database. It is necessary to perform this operation on all nodes.

An example of deletion is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n "logical-virtual-interface-name"
```

For detail, refer to "7.14 hanethvrsc Command".

5.4.3 Deletion of a Configuration information

Delete configuration information. Perform deletion process on the operating node and standby node. For deletion procedure, refer to "3.5 Deleting configuration information".

5.5 Backup/Restore Cluster configuration settings

When operating Redundant Line Control function on a cluster system, it is possible to backup/restore the GLS configuration together with the cluster system configuration.

Refer to "Backing Up and Restoring a PRIMECLUSTER System" in "PRIMECLUSTER Installation and Administration Guide" and backup/restore configuration settings of both cluster system and Redundant Line Control function.

Chapter 6 Maintenance

This chapter focuses on a general approach to troubleshooting. It presents a troubleshooting strategy and identifies commands that are available in Resource Coordinator for finding and correcting problems. Further, it discusses how to collect troubleshooting information.

6.1 Redundant Line Control function Troubleshooting Data to be Collected

In the event of a problem in Redundant Line Control function operation, see "[6.1.1 Command to collect materials](#)" or "[6.1.2 Collecting Information by FJQSS \(Information Collection Tool\)](#)," and collect information. When collecting only information for investigation of Redundant Line Control Function, use `hanet_snap` command. Use FJQSS if you want to collect examination materials for other FJQSS compatible middleware products.

1) Collecting materials common to each mode

Collect the following materials for examination when an error occurred in the workings of a Redundant Line Control function:

- The content of the detailed operation and error messages when a phenomenon occurred.
- A console log (`/var/adm/messages`) file
- A log file (`/var/opt/FJSVhanet/log/*`) of a Redundant Line Control function
- An environment setting file (`/etc/opt/FJSVhanet/config/*`) of a Redundant Line Control function
- The result of executing `/opt/FJSVnet/usr/sbin/dsphanet`
- The result of executing `ifconfig -a`
- The result of executing `netstat -ni`
- The result of executing `netstat -nr`
- The result of executing `netstat -np`
- Packet trace (For details on collecting packet traces, see "[6.2 Packet Trace](#)".)

2) When an error occurred in Fast switching mode

When an error occurred in Fast switching mode, perform "1)Collecting materials common to each mode" and collect the following materials:

- The result of executing `/opt/FJSVhanet/usr/sbin/dsphanet -o`

3) When an error occurred in NIC switching mode

When an error occurred in NIC switching mode, perform "1) Collecting materials common to each mode" and collect the following materials:

- The result of executing `ps -ef`
- Debug information of the HUB monitoring function (See "[6.1.3 Collecting debug information/Output command](#)" as to how to set, etc.)

4) When an error occurred in GS/SURE linkage mode

When an error occurred in GS/SURE linkage mode, perform "1) Collecting materials common to each mode" and collect the following materials:

- The result of executing `/opt/FJSVhanet/usr/sbin/dsphanet -c`
- The result of executing `/opt/FJSVhanet/usr/sbin/dsppoll -c`
- Debug information of the communication target monitoring function (See "[6.1.3 Collecting debug information/Output command](#)" as to how to set, etc.)

6.1.1 Command to collect materials

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanet_snap [-s] [save-directory]
```

[Feature description]

This command collects examination materials necessary for maintaining a Redundant Line Control function. In addition, only in the case of super-user authority, this command can be executed.

[Option]

It is possible to specify following options and parameters.

-s:

Specify **-s** to collect the minimum examination materials.
When omitted this option, all examination materials are collected.

save-directory:

Specify **save-directory** to store collected materials.
When omitted this parameter, materials are stored in **"/tmp"**.

A list of the collected information is as follows:

[Meaning of the symbols] Y: It extracts. N: It does not extract.

| Type | File name when collected | Collected information | Minimum examination materials |
|--------------------------------|---|---|-------------------------------|
| System information: OSInfo/ | etc/ | /etc/hosts | Y |
| | | /etc/netmasks | Y |
| | | /etc/nsswitch.conf | Y |
| | | /etc/gateways | Y |
| | | /etc/hostname* | Y |
| | | /etc/defaultrouter | Y |
| | | /etc/notrouter | Y |
| | | /etc/mnttab | Y |
| | | /etc/vfstab | Y |
| | | etc/inet/ | /etc/inet/* |
| | etc/svc/volatile/ Note: This information is collected only on Solaris 10. | /etc/svc/volatile/* | N |
| | etc/ipf/ | /etc/ipf/* | Y |
| | adm/ | /var/adm/messages* | N |
| | var/svc/log/ | /var/svc/log/network-loopback:default.log | N |

| Type | File name when collected | Collected information | Minimum examination materials |
|------|---|---|-------------------------------|
| | | /var/svc/log/network-physical:default.log | N |
| | | /var/svc/log/network-initial:default.log | N |
| | | /var/svc/log/network-service:default.log | N |
| | | /var/svc/log/system-zones:default.log | N |
| | | /var/svc/log/network-inetd:default.log | N |
| | | /var/svc/log/network-fjshvhanet:default.log | N |
| | | /var/svc/log/network-fjshvhanet-poll:default.log | N |
| | | /var/svc/log/network-fjssrvnet:default.log | N |
| | | /var/svc/log/system-filesystem-minimal:default.log | N |
| | uname_a | uname -a | Y |
| | ifconfig_a | ifconfig -a | Y |
| | dladm_info [Note 1] The following are collected only on Solaris 10: - show-link - show-aggr - show-linkprop - show-dev [Note 2] show-dev is not collected on Solaris 11 or later. | dladm show-link dladm show-aggr dladm show-linkprop dladm show-phys dladm show-bridge dladm show-vlan dladm show-wifi dladm show-ether dladm show-secobj dladm show-vnic dladm show-etherstub dladm show-iptun dladm show-part dladm show-ib dladm show-dev dladm show-link -P dladm show-phys -P | Y |
| | ipadm_info Note: This information is collected only on Solaris 11 or later. | ipadm show-if ipadm show-ifprop ipadm show-addr ipadm show-addrprop ipadm show-prop | Y |
| | netstat | netstat -na netstat -ni netstat -np netstat -nr netstat -ng | Y |
| | filelist_etc | ls -l /etc/hostname* | Y |
| | ip_forward | /usr/sbin/ndd -get /dev/ip ip_forwarding | Y |
| | ipcs_a | ipcs -a | Y |
| | ipadrssel | ipadrssel | Y |
| | ipfstat | ipfstat -io | Y |
| | ps_ef | ps -ef | N |

| Type | File name when collected | Collected information | Minimum examination materials |
|--|--------------------------|--|-------------------------------|
| | pstack | pstack pid | N |
| | svcs | /bin/svcs -apv | Y |
| | uam/ | /var/opt/FJSVfupde/log/* | Y |
| | timezone | date +%Z | Y |
| | virtinfo_info | virtinfo virtinfo -a | Y |
| | ldm_list-domain_e | ldm list-domain -e | Y |
| | prtconf_vb | prtconf -vb | Y |
| | pfctl_sa | pfctl -sa | Y |
| GLS information: hanetInfo/ | config/ | /etc/opt/FJSVhanet/config/* | Y |
| | log/ | /var/opt/FJSVhanet/log/* | Y |
| | version | hanetconfig version | Y |
| | filelist_tmp | ls -la /var/opt/FJSVhanet/tmp/ | Y |
| | dsphanet | dsphanet dsphanet -o dsphanet -c | Y |
| | dsppoll | dsppoll dsppoll -c | Y |
| | script/ | /etc/opt/FJSVhanet/script/* | Y |
| | print_conf | hanetconfig print hanetpoll print hanetparam print hanetgw print hanetobserv print hanethvrsc print | Y |
| Virtual NIC mode information: rvnetinfo/ | config/ | /etc/opt/FJSVrvnet/config/* | Y |
| | log/ | /var/opt/FJSVrvnet/log/* | Y |
| | version | rvnetadm version | Y |
| | filelist_tmp | ls -la /var/opt/FJSVrvnet/tmp/* | Y |
| | rvnetadm_print | rvnetadm print | Y |
| | rvnetadm_show-prop | rvnetadm show-prop | Y |
| | rvnetadm_show-param | rvnetadm show-param | Y |
| | rvnetstat_v | rvnetstat -v | Y |
| | rvnetstat_s_v | rvnetstat -s -v | Y |
| | rvnetstat_f | rvnetstat -f | Y |
| Cluster information (CRM): SCInfo/ | version_clapi | pkgparam FJSVclapi VERSION | N |
| | clgettree | clgettree | N |
| | clgettree_s | clgettree -s | N |
| Cluster information (RMS): RCInfo/ | log/ | /var/opt/reliant/log/* | N |

| Type | File name when collected | Collected information | Minimum examination materials |
|------|--------------------------|-----------------------|-------------------------------|
| | hvdisp_a | hvdisp -a | N |

[Output form]

The collected materials are compressed and stored by tar and compress commands. A stored file name is "machine name" + "Date collected (YYMMDDhhmmss)".tar.Z.

Ex.) hostname031030084916.tar.Z

[Examples]

- When collecting all examination materials under /tmp.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap
```

- When collecting the minimum examination materials under /tmp.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap -s
```

- When collecting the minimum examination materials under /export/home/user1.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap -s /export/home/user1
```

6.1.2 Collecting Information by FJQSS (Information Collection Tool)

[Detail of the function]

By using FJQSS (Information Collection Tool), collect the investigation material required to maintain the Redundant Line Control Function.

The collected material includes all the investigation materials in the list of the collected information in ["6.1.1 Command to collect materials."](#)

[Using example]

1. Execute the following command.

```
# /opt/FJSVqst1/fjqss_collect
```

2. The product selection menu appears. Input the number of the product of which you want to collect the investigation material ("PRIMECLUSTER GL"), then input "[Enter]".
For the cluster system, if the number of the cluster product (PRIMECLUSTER HA Server, for example) is specified, the investigation material of PRIMECLUSTER including GLS can be collected at once.
3. Press the [Y] key according to the instruction in the prompt.
4. After the FJQSS has completed the collection, the name of the output directory of the collected investigation material appears. Verify that the investigation material has been collected in the directory.
5. Send the created file to field engineers.

[Output form]

The following file is created in the output directory of the collected material.

resultYYYYMMDDHHMMSS.tar.gz

(YYYYMMDDHHMMSS: time (year, month, day, hour, minute, and second) that the collection started)

Information

About FJQSS (Information Collection Tool) and its usage

You can collect the information necessary for the trouble investigation with FJQSS (Information Collection Tool). See the FJQSS (Information Collection Tool) User's Guide bundled to the installation medium of the product.

When you see the FJQSS (Information Collection Tool) User's Guide, open the following file in the installation medium of the product by the browser.

documents/fjqss-manual_sollnx/index_en.html

6.1.3 Collecting debug information/Output command

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/dbghanet enable|disable|trace|stat
```

[Feature description]

Specifies whether the debug information for the HUB monitoring function is collected and outputs the log information. The following are the debug information to be collected:

- Execution log of the ping command

If a line failure is detected due to no response from the ping monitoring, execute the ping command to collect the result and packets sent and received. These logs are useful for determining the point where an error occurred or identifying the cause of the failure when a network failure occurs. The execution logs of the ping command are collected only when collecting the debug information is enabled.

- Statistical information of the ping command

Statistical information of the execution time of the ping command for the monitoring target is logged periodically. The maximum value, the minimum value, the average value, and the distribution of the execution time of the ping command are logged in the statistical information. These logs are useful for determining the load condition of the system. Statistical information is collected regardless of whether collecting the debug information is enabled or not.

This information is output to the log information of the Redundant Line Control function, and also included in the information collected by the "hanet_snap" command.

[Options]

It is possible to specify following options and parameters.

enable

Enables collecting the debug information. When enabled collecting the debug information, the execution logs of the ping command are collected.

disable

Disables collecting the debug information of the HUB monitoring function.

trace

Outputs the log information of the Redundant Line Control function where the execution logs of the ping command are recorded.

stat

Outputs the log information of the Redundant Line Control function where the statistical information of the ping command is recorded.

[Notes]

When collecting the debug information is enabled, it takes about three to five seconds longer to switch NICs or clusters for collecting logs, comparing to the case when collecting the debug information is not enabled. Switching will be continued regardless of whether the ping command, which is executed to collect logs, fails or not.

[Examples]

- To enable collecting the execution logs of the ping command

```
# /opt/FJSVhanet/usr/sbin/dbghanet enable
```

- To disable collecting the execution logs of the ping command

```
# /opt/FJSVhanet/usr/sbin/dbghanet disable
```

- To output the execution logs of the ping command

```
# /opt/FJSVhanet/usr/sbin/dbghanet trace
```

- To output the statistical information of the ping command

```
# /opt/FJSVhanet/usr/sbin/dbghanet stat
```

6.2 Packet Trace

This section describes how to collect packet traces of Redundant Line Control function.

6.2.1 Collecting packet traces

If you want to collect packet traces of virtual interfaces, follow the example below.

1. Execute hanetconfig print to check the physical interfaces bundled with the virtual interface which you want to obtain.

```
[IPv4,Patrol]

Name          Hostname          Mode MAC Adder/Phys ip Interface List
+-----+-----+-----+-----+-----+
sha0          hostA             t           hme0,hme1
sha12         -                 p           02:00:00:00:00:01 sha11
sha2          hostC             d           fjgi1000,fjgi1001
sha3          -                 p           02:00:00:00:00:10 sha2
sha4          192.168.10.50    n           fjgi4
sha5          192.168.20.50    n           fjgi5
sha6          192.168.100.50   c           sha4,sha5

[IPv6]

Name          Hostname/prefix   Mode Interface List
+-----+-----+-----+-----+
sha10         -                 t           qfe0,qfe1
sha10:2       hostB/64          d           qfe2,qfe3
sha11         fec0:1::123/64    d           qfe2,qfe3
```

2. Execute the snoop command or the tshark command to collect packet traces.

If a virtual interface bundles several physical interfaces, execute the snoop(1M) command or the tshark(1) command for all physical interfaces in the bundle.

Execution examples for the snoop command are shown below:

- sha0

```
# snoop -d hme0 -o /tmp/packet_trace.hme0
# snoop -d hme1 -o /tmp/packet_trace.hme1
```

- sha2 and sha3

```
# snoop -d fjgi1000 -o /tmp/packet_trace.fjgi1000
# snoop -d fjgi1001 -o /tmp/packet_trace.fjgi1001
```

- sha10 and sha10:2

```
# snoop -d qfe0 -o /tmp/packet_trace.qfe0
# snoop -d qfe1 -o /tmp/packet_trace.qfe1
```

- sha11 and sha12

```
# snoop -d qfe2 -o /tmp/packet_trace.qfe2
# snoop -d qfe3 -o /tmp/packet_trace.qfe3
```

- sha4, sha5, and sha6

```
# snoop -d fjgi4 -o /tmp/packet_trace.fjgi4
# snoop -d fjgi5 -o /tmp/packet_trace.fjgi5
```

Information

For the snoop(1M) command or the tshark(1) command, refer to the Solaris manual.

Note

Even if you execute the snoop(1M) command or the tshark(1) command for a virtual interface, you cannot collect any packets. Do not specify a virtual interface as the target for collecting packets by using the snoop(1M) command or the tshark(1) command.

Chapter 7 Command reference

This chapter outlines GLS commands.

7.1 hanetconfig Command

[Name]

hanetconfig - Setting, modifying, deleting, and displaying a configuration definition of Redundant Line Control function

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetconfig command [args]
```

[Feature description]

The hanetconfig command defines configuration information required for the operation of Redundant Line Control function. This command also modifies, deletes, and displays a setting.

| Command | Process outline | Authority |
|---------|------------------------------------|--------------|
| create | Creates configuration information | Super user |
| copy | Copies configuration information | Super user |
| print | Displays configuration information | General user |
| modify | Modifies configuration information | Super user |
| delete | Deletes configuration information | Super user |
| version | Displays the version | General user |

(1) create command

Configuration information must be defined for a virtual interface before Redundant Line Control function can be operated. Use the create command to create a definition of configuration information. The create command can also create definitions of more than one logical virtual interface on the virtual interface. The following is the command format for building a virtual interface:

- When creating a virtual interface

```
Fast switching mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet] -n devicename -m t -i
ipaddress -t interfacel[,interface2,...]
Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n devicename -m t -t
interfacel[,interface2,...]
GS/SURE linkage mode (physical interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m n -i ipaddress
-t interface
GS/SURE linkage mode (virtual interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m c -i ipaddress
-t interfacel[,interface2,...]
NIC switching mode (IPv4: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet] -n devicename -m d -i
ipaddress1 -e ipaddress2 -t interfacel[,interface2]
NIC switching mode (IPv6: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n devicename -m d -i
ipaddress/prefix -t interfacel[,interface2]
NIC switching mode (physical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m e -i
ipaddress1 [-e ipaddress2] -t interfacel[,interface2]
Standby patrol function (automatic failback if a failure occurs /
```



```
immediate automatic failback):  
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m {p | q} [-a  
MAC_address] -t interface
```

- When creating a logical virtual interface

```
Fast switching mode (IPv4):  
/opt/FJSVhanet/usr/sbin/hanetconfig create [inet] -n devicename -i  
ipaddress  
Fast switching mode (IPv6):  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n devicename -i  
ipaddress/prefix
```

[inet | inet6]

Specify an IP address form to set to a virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of "create") before other options.

This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename:

Specify the name of a virtual interface or logical virtual interface for which the configuration information should be set. Specify the virtual interface name with a string "sha" and is followed by a value (0 to 255) (such as sha0 and sha10). Specify the logical virtual interface name as "virtual-interface-name: value (2 to 64)" (such as sha0:2 and sha10:5). If you specify a virtual interface or logical virtual interface in any other format, an error message is output and this command terminates abnormally. In addition, Logical virtual interface can only be configured on operation mode "t".

-m t|n|c|d|e|p|q:

Specify an operation mode. If devicename is a logical virtual interface, specify the operation mode of a corresponding virtual interface.

t: Fast switching mode

Specify this parameter to use the Redundant Line Control function in Fast switching mode.

n: GS/SURE linkage mode (physical interface definition)

Specify this parameter to use the Redundant Line Control function in GS/SURE linkage mode. A physical interface used to actually perform communication is created.

c: GS/SURE linkage mode (virtual interface definition)

Specify this parameter to use the Redundant Line Control function in GS/SURE linkage mode. A virtual interface that bundles physical interfaces defined in operation mode n to perform communication is created.

d: NIC switching mode (logical IP address takeover function)

Specify this parameter to use the Redundant Line Control function in NIC switching mode. This mode activates logical interface and physical interface.

e: NIC switching mode (physical IP address takeover function)

Specify this parameter to use the Redundant Line Control function in NIC switching mode. This mode activates only physical interface.

p: Standby patrol function (automatic failback if a failure occurs)

Specify this parameter to use the Redundant Line Control function in NIC switching mode and monitor the status of the standby NIC. If the standby NIC is communicating due to a failure and the active NIC recovers, no failback occurs until the currently used NIC encounters a failure.

q: Standby patrol function (immediate automatic failback)

Specify this parameter to use the Redundant Line Control function in NIC switching mode and monitor the status of the standby NIC. If the standby NIC is communicating due to a failure and the active NIC recovers, a failback immediately occurs.

The following table lists options that can be specified in each operation mode.

| Operation mode | Specifiable parameter | | | | | |
|--|-----------------------|----|--------|--------|--------|--------|
| | inet inet6 | -n | -i | -e | -a | -t |
| 't' (Fast switching mode) | Support | A | A (*8) | N | N | A (*1) |
| 'n' (GS/SURE linkage mode (physical interface definition)) | Not support | A | A | N | N | A (*2) |
| 'c' (GS/SURE linkage mode (virtual interface definition)) | Not support | A | A | N | N | A (*3) |
| 'd' (NIC switching mode (logical IP address takeover function)) | Support | A | A | A (*6) | N | A (*4) |
| 'e' (NIC switching mode (physical IP address takeover function)) | Not support | A | A | A (*7) | N | A (*4) |
| 'p' (Standby patrol function (automatic failback if a failure occurs)) | Not support | A | N | N | A (*9) | A (*5) |
| 'q' (Standby patrol function (immediate automatic failback)) | Not support | A | N | N | A (*9) | A (*5) |

[Meaning of the symbols] A: Required, N: Not required

*1 Specify a physical interface (The same physical interface can be specified if the operation mode is "t"). 1 to 8 physical interfaces can be assigned.

*2 Specify one physical interface that is not specified in any other operation mode. Only one physical interface can be assigned.

*3 Specify a virtual interface created in operation mode "n". 2 to 8 interfaces can be assigned.

*4 Specify a physical interface that is not specified in any other operation mode. One or two physical interface can be assigned.

*5 Specify a virtual interface specified in the operation mode "d" or "e". Only one interface can be assigned.

*6 It is not possible to specify this parameter when set inet6 to an address form.

*7 This parameter may be omitted if the physical IP address takeover function II is used (not activating an interface on the standby node in the cluster system).

*8 It can specify, only when creating logical virtual interface.

*9 The MAC address is automatically set even when the option is omitted.

-i ipaddress1[/prefix]:

ipaddress1

Specify a host name or an IP address to assign to a virtual interface or a logical virtual interface (devicename specified by -n option). The host name that can be specified is within 16 characters. The specified IP address or host must be defined in an /etc/inet/hosts file (IPv4) or an /etc/inet/ipnodes file (IPv4,IPv6). When assigning an IP address to a logical virtual interface, it is necessary to specify the same subnet as that of a virtual interface. If specified a different subnet, occasionally it is not possible to communicate.

[/prefix]

Specify the length of a prefix of `ipaddress1` following "/" (slash). The range possible to specify is between zero to 128. This parameter is required only when specifying an IPv6 address to `ipaddress1` or a host name defined in an `/etc/inet/ipnodes` file. It is not possible to specify for an IPv4 address.

-e ipaddress2:

Specify an IP address or a host name to assign to a physical interface. It is possible to set an IP address or a host name in an IPv4 form only and must be defined in an `/etc/inet/hosts` and `/etc/inet/ipnodes` files. It is possible to specify this option only when specified `inet` for an address form. (When specified `inet6`, a link local address is automatically assigned.) It is necessary to set this option in NIC switching mode (operation mode is "d" or "e").

This parameter can be omitted in the following cases:

- When using physical IP address takeover function with a single system.
- When using physical IP address takeover function II (inactivating a virtual interface in a standby node) with a cluster system.

-t interface1[,interface2,...]:

Specify interface names to be bundled by a virtual interface, by listing them delimited with a comma (,).

For NIC switching mode, "interface1" is specified as the primary interface, while "interface2" is specified as the secondary interface. Specify virtual interface names (such as `sha1` and `sha2`) for GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

To configure other than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"), specify the name of physical interface (such as `eri0` or `hme0`) or the name of tagged VLAN interface (such as `ce1000` or `fjgi1000`).

-a MAC_address:

Specify a MAC address to be allocated to the standby NIC as `XX:XX:XX:XX:XX:XX` (X represents a hexadecimal from 0 to F).

In the environment where the MAC addresses of the active NIC and the standby NIC are the same, specify the local MAC address (`02:XX:XX:XX:XX:XX : "02"` in the beginning indicates that this is a local MAC address). In the environment where the MAC addresses of the active NIC and the standby NIC are not the same, specify `0:0:0:0:0:0` so that the global address set to the NIC is to be used as it is.

If this option is not specified, the local MAC address based on the global address is automatically set in the environment where the MAC addresses of the active NIC and the standby NIC are the same, and `0:0:0:0:0:0` is automatically set in the environment where the MAC addresses of the active NIC and the standby NIC are not the same.



Note

- Do not use the MAC address of a node connected on the same LAN. No normal operation is guaranteed if duplicate addresses are used.
- When multiplexing the virtual networks (`vsw` and `vnet`) in Oracle VM environments, specify `0:0:0:0:0:0` to the MAC address because the virtual MAC address generated by the operating system must be used as it is.
- You cannot use the `-a` option in the following cases:
 - When setting the standby patrol for a virtual interface bundling tagged VLAN interfaces with Solaris 11 or later
 - When setting the standby patrol for a virtual interface in the exclusive-IP zone or Kernel Zones

(2) copy command

Use the `copy` command to create different configuration information while sharing an NIC used in other configuration information (virtual interface in NIC switching mode (operation mode "d")). This command thus allows configuration information to be automatically created by using the copy source information and without requiring you to specify an IP address to be attached to a physical interface, interface names to be bundled by a virtual interface, and an operation mode. This command realizes simpler operation than directly executing the `hanetconfig create` command.

In addition, this command can copy only virtual interface of NIC switching mode (operation mode "d").

The following is the command format for copying a virtual interface:

- When duplicating a virtual interface of IPv4 from a virtual interface of IPv4

```
/opt/FJSSVhanet/usr/sbin/hanetconfig copy [inet] -n  
devicename1,devicename2 -i ipaddress
```

- When duplicating a virtual interface of IPv4 from a virtual interface of IPv6 (dual stack configuration)

```
/opt/FJSSVhanet/usr/sbin/hanetconfig copy [inet] -n  
devicename1,devicename1 -i ipaddress1 -e ipaddress2
```

- When duplicating a virtual interface of IPv6 from a virtual interface of IPv6

```
/opt/FJSSVhanet/usr/sbin/hanetconfig copy inet6 -n  
devicename1,devicename2 -i ipaddress/prefix
```

- When duplicating a virtual interface of IPv6 from a virtual interface of IPv4 (dual stack configuration)

```
/opt/FJSSVhanet/usr/sbin/hanetconfig copy inet6 -n  
devicename1,devicename1 -i ipaddress/prefix
```

[inet | inet6]

Specify an IP address form to set to a copy-to virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a strings of copy) before other options.

-n devicename1,devicename2:

devicename1:

Specify a copy-from virtual interface name. It is possible to specify only a virtual interface name of NIC switching mode (operation mode is "d").

devicename2:

Specify a copy-to virtual interface name. When configuring IPv4/IPv6 dual stack, specify the same virtual interface name (devicename1) as that of copy-from.

-i ipaddress1[/prefix]:

Specify a host name or an IP address to assign to a copy-to virtual interface specified by devicename2. See -i option of a create command for the detail of how to set.

-e ipaddress2:

Specify an IP address or a host name to assign to a physical interface. This option is required to duplicate a virtual interface of IPv4 from that of IPv6 (dual stack configuration). See -e option of a create command for the detail of how to set.

(3) print command

Use the print command to display the current configuration information. The following is the format of the print command.

```
/opt/FJShanet/usr/sbin/hanetconfig print [-n
devicename1[,devicename2,...]]
```

-n devicename1[,devicename2,...]:

Specify the name of a virtual interface or logical virtual interface whose configuration information should be displayed. If this option is not specified, the print command displays all the configuration information for the currently set virtual interfaces and logical virtual interfaces.

The following shows an example of displaying configuration information.

```
[IPv4,Patrol]

Name      Hostname      Mode MAC Adder/Phys ip Interface List
-----+-----+-----+-----+-----+
sha0      hostA         t                hme0,hme1
sha12     -             p 02:00:00:00:00:01 sha11
sha2      hostC         d                fjgi1000,fjgi1001
sha3      -             p 02:00:00:00:00:10 sha2

[IPv6]

Name      Hostname/prefix      Mode Interface List
-----+-----+-----+-----+
sha10     -                    t   qfe0,qfe1
sha10:2   hostB/64              d   qfe2,qfe3
sha11     fec0:1::123/64       d   qfe2,qfe3
```

| Item | | Explanation |
|---------------|-------------------|---|
| [IPv4,Patrol] | | The information of an IPv4 virtual interface and standby patrol |
| [IPv4,Patrol] | Name | Outputs a virtual interface name. |
| | Hostname | Outputs the host name or virtual IP address of a virtual interface. |
| | Mode | Outputs the operation mode of a virtual interface. (For details, please refer to "-m" option of the create command.) |
| | MAC Adder/Phys ip | Outputs a MAC local address used by standby patrol mode, or physical IP address defined as the virtual interface. |
| | Interface List | Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). Outputs a physical interface name (such as le0 and hme0) in any other mode than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). |
| [IPv6] | | The information of an IPv6 virtual interface |
| [IPv6] | Name | Outputs a virtual interface name. |
| | Hostname/prefix | A host name or an IP address and a prefix value of a virtual interface |
| | Mode | Outputs the operation mode of a virtual interface. |

| Item | | Explanation |
|------|----------------|---|
| | Interface List | Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). Outputs a physical interface name (such as le0 and hme0) in any other mode than GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q"). |

(4) modify command

Use the modify command to modify the configuration of Redundant Line Control function.

The following is the format of the modify command that modifies configuration information for a virtual interface:

- When changing configuration information of a virtual interface

```
Fast switching mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename {[ -m {r |
b}] [-i ipaddress1] [-t interface1[,interface2,...]]}
Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename -t
interface1[,interface2,...]
GS/SURE linkage mode (physical interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[ -i ipaddress]
[-t interface]}
GS/SURE linkage mode (virtual interface definition):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[ -i ipaddress]
[-t interface1[,interface2,...]]}
NIC switching mode (IPv4: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename {[ -i
ipaddress1] [-e ipaddress2] [-t interface1[,interface2]]}
NIC switching mode (IPv6: logical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename {[ -i
ipaddress1/prefix] [-t interface1[,interface2]]}
NIC switching mode (physical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[ -i ipaddress1]
[-e ipaddress2] [-t interface1[,interface2]]}
Standby patrol function:
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[ -a
MAC_Address] [-t interface1]}
```

- When changing configuration information of a virtual interface

```
Fast switching mode (IPv4):
/opt/FJSVhanet/usr/sbin/hanetconfig modify [inet] -n devicename -i
ipaddress
Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename -i
ipaddress/prefix
```

[inet | inet6]

Specify an IP address form to set to a changing virtual interface.

```
inet          : IPv4 address
inet6         : IPv6 address
```

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of modify) before other options.

This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename:

Specify the name of a virtual interface or logical virtual interface whose configuration information should be modified. This parameter is required.

-m t:

Specify this parameter to change the operation mode (Fast switching mode) of a virtual interface to be modified. One of Fast switching mode can be selected ("t" indicates Fast switching mode).

-i ipaddress1[/prefix]:

Specify a host name or IP address to be attached to a virtual or logical virtual interface (devicename specified by -n option) to be used for Redundant Line Control function. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. When you specify address information for a logical virtual interface, be sure to specify an address in the same subnet as the address of a corresponding virtual interface. Communication may be disabled if any other subnet is specified.

-e ipaddress2:

Specify an IP address to be attached to a physical interface. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

This parameter can be modified only if the operation mode of a virtual interface to be modified is NIC switching mode (operation mode "d" or "e").

-t interface1[,interface2,...]:

Specify interface names to be bundled by a virtual interface, by listing them delimited with a comma (,).

Specify virtual interface names (such as sha1 and sha2) if the operation mode of a virtual interface to be modified is GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

Specify physical interface names (such as le0 and hme0) if the operation mode of a virtual interface to be modified is not GS/SURE linkage mode (operation mode "c") or standby patrol function (operation mode "p" or "q").

-a MAC_address:

This parameter can be changed only if the operation mode of a virtual interface to be modified is standby patrol function (operation mode "p" or "q").

(5) delete command

Use the delete command to delete the configuration of Redundant Line Control function. The following is the format of the delete command:

```
/opt/FJSVhanet/usr/sbin/hanetconfig delete [inet | inet6] -n  
{devicename1[,devicename2,...] | all}
```

[inet | inet6]

Specify an IP address form of a deleting virtual interface.

inet : IPv4 address
inet6 : IPv6 address

When omitted, it is dealt with as specified inet. It is necessary to specify this option first (immediately after a string of delete) before other options.

This option can be specified only when using Fast switching mode or NIC switching mode (a logical IP address takeover function).

-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces (such as sha0 and sha1) or logical virtual interfaces (such as sha0:2 and sha1:10) whose configuration information should be deleted.

all:

Specify this parameter to delete all the defined virtual and logical interfaces. In addition, the definition of IPv4 interface and IPv6 interface cannot be deleted simultaneously. Please specify IPv4 interface and IPv6 interface individually, respectively and delete them.

(6) version command

The version of this product is displayed. The following is the format of the version command.

```
/opt/FJSVhanet/usr/sbin/hanetconfig version
```

The following shows an example of displaying version information.

```
HA-Net version 2.10
```

[Notes]

- When you define a logical virtual interface, be sure to define also a virtual interface to which the logical virtual interface belongs. (For example, when you define a logical virtual interface of sha2:2, sha2 must also be defined.)
- When you define a logical virtual interface, no input item except required items (the physical interface name and operation mode used in the logical virtual interface) can be set in the logical virtual interface definition. This is because the values specified for the virtual interface are set for them.
- Only a value from 2 to 64 can be specified as the logical number of the logical virtual interface.
- A new virtual interface can be added while other virtual interfaces are active. No new logical virtual interface can be attached to an active virtual interface. Add a logical virtual interface after deactivating the relevant virtual interface.
- If the HUB monitoring is set, no relevant configuration information can be deleted. Delete configuration information after deleting the relevant information of the HUB monitoring function.
- A physical interface to be specified for GS/SURE linkage mode (operation mode "n") must not be defined for the use in conventional TCP/IP. (Check if or not there is /etc/hostname.interface file. If exists, change a name or delete it, then execute "/usr/sbin/ifconfig interface unplumb" command.)
- An IP address or host name to be specified to create, copy, or modify configuration information must be defined in /etc/inet/hosts and /etc/inet/ipnodes.
- If more than one virtual interface is created while sharing a NIC bundled in NIC switching mode, the standby patrol need not be set for each of the virtual interfaces.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- As for an actual interface to configure Fast switching mode, (the operation mode is "t"), be sure to define to use in TCP/IP before defining a virtual interface. (Check if or not there is /etc/hostname.interface file. If not, create it and reboot a system.)
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.

- When using an IPv6 address, an IP address that is set by -i option of a create command is not a target of address automatic configuration by an IPv6 protocol. Therefore, specify the same to a prefix and the length of a prefix as those set in an IPv6 router on the connected network. Set a value different from that of the other system for an "interface IP" inside an IP address field.
- When configuring a virtual interface for Fast switching mode as Dual Stack, the bundled physical interfaces cannot be modified with "modify --t" command. To apply changes, delete the configuration information of the virtual interface and then reconfigure.
- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in /etc/inet/hosts and /etc/inet/ipnodes so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.
- When configuring a standby patrol function for a virtual interface which is using the tagged VLAN interfaces, it is required to reboot the OS in order to enable the standby patrol function. GLS withholds a modification of MAC address of the secondary interface, so that it prevents communication errors on other tagged VLAN interfaces which are sharing a physical communication line.

[Examples]

(1) create command

The following shows an example of the setting command used in Fast switching mode to bundle two physical interfaces (hme0 and hme1) as the virtual interface host "hahost" to duplicate the virtual interface sha0.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hahost -
t hme0,hme1
```

The following shows an example of the setting command used to define two logical virtual interfaces (sha0:2 and sha0:3) on the virtual interface (sha0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hostf -
t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i hostg
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:3 -i hosth
```

The following shows an example of the setting command used to have the virtual interface (sha0) bundle only one physical interface (hme0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hosti -
t hme0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (hme0 and hme1) and use the logical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i hostg -
e hosth -t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a
02:00:00:00:00:01 -t sha0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (hme0 and hme1) and use the physical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i hosti -
t hme0,hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a
02:00:00:00:00:01 -t sha0
```

The following shows an example of the setting command used in GS/SURE linkage mode to have two physical interfaces (hme0 and hme1) bundled. For this purpose, first set the physical interfaces in GS/SURE linkage mode (operation mode "n"), then create virtual

interfaces in GS/SURE linkage mode (operation mode "n"), and have the virtual interfaces bundled to set GS/SURE linkage mode (operation mode "c").

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i hostd -
t hme0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i hoste -
t hme1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i hostf -
t sha1,sha2
```

The following is an example that set two physical interfaces (hme0 and hme1) to use a logical IP address takeover function by an IPv6 address in NIC switching mode. It is necessary to set a HUB monitoring function other than this setting.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig inet6 create -n sha0 -m d -i
fec0:1::1/64 -t hme0,hme1
or
# /opt/FJSVhanet/usr/sbin/hanetconfig inet6 create -n sha0 -m d -i
hostg/64 -t hme0,hme1
```

The following is an example of configuring two physical interfaces (hme0 and hme1) and creating a virtual interface (sha0) using IPv6 address.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t
hme0,hme1
```

The following shows an example of the setting command used in NIC switching mode to set two VLAN interfaces (fjgi1000 and fjgi1001) and use the logical IP address takeover function and the standby patrol function (operation mode "p"). Before NIC switching mode can be used, the HUB monitoring function must be set.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i hostg -
e hosth -t fjgi1000,fjgi1001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a
02:00:00:00:00:01 -t sha0
```

(2) modify command

The following is an example of modifying bundled physical interfaces (hme0 and hme1) in the virtual interface (sha0) to different physical interfaces (hme2 and hme3).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -t hme2,hme3
```

The following is an example of modifying the virtual IP address defined in the virtual interface (sha0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i hostc
```

The following is an example of modifying the value of the local MAC address to be allocated in the standby NIC used in NIC switching mode.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha1 -a
02:00:00:00:00:01
```

(3) copy command

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv4) for NIC switching mode (operation mode "d"), with another virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha2 -i host4
```

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv6) for NIC switching mode (operation mode "d"), with another virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha0 -i host4 --e  
hostp
```

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv6) for NIC switching mode (operation mode "d"), with another virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha2 -i  
host6/64
```

The following is an example of sharing the NIC, used in the virtual interface (sha0 for IPv4) for NIC switching mode (operation mode "d"), with another virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i  
host6/64
```

(4) delete command

The following is an example of deleting the virtual interface (sha2 for IPv4).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n sha2
```

The following is an example of deleting the virtual interface (sha2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete inet6 -n sha2
```

The following is an example of deleting the logical virtual interface (sha0:2).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n sha0:2
```

The following is an example of deleting the logical virtual interface (sha0:2 for IPv6).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete inet6 -n sha0:2
```

7.2 strhanet Command

[Name]

strhanet - Activation of virtual interfaces

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/strhanet [inet | inet6 | dual] [-n devicename1[,devicename2,...]]
```

[Feature description]

The strhanet command activates virtual interfaces in accordance with the generated configuration information.

[Option]

It is possible to specify the following options:

[inet | inet6 | dual]

Specify an IP address form assigned to a virtual interface to be activated.

| | |
|-------|--------------------------------------|
| inet | : IPv4 address |
| inet6 | : IPv6 address |
| dual | : IPv4/IPv6 dual stack configuration |

When omitted, virtual interfaces of all forms are to be dealt with. IPv4 and IPv6 addresses are activated at the same time in a virtual interface of dual stack configuration. It is not possible to activate only an IPv4 address or only an IPv6 address respectively. Dual stack configuration in this case does not mean IPv4 and IPv6 addresses are set on each of the stacked physical interfaces, but they are set to one virtual interface defined in a Redundant Line Control function. This option is valid only in Fast switching mode (operation mode is "t") or NIC switching mode (operation mode is "d").

-n devicename1[,devicename2,...]

Specify a virtual interface name to be activated. Multiple virtual interfaces can be specified by delimiting them with a comma (.). Configuration information for virtual interface names specified here must have been generated with the hanetconfig create command. If this option is not specified, all created virtual interfaces are activated.

[Related commands]

```
hanetconfig
stphanet
dsphanet
```

[Notes]

- If an additional virtual interface is activated in Fast switching mode, nodes that have been activated in Fast switching mode may be temporarily overloaded.
- This command can activate a virtual interface only if configuration information has already been set by using the hanetconfig command before executing this command. For details, see "[Chapter 3 Environment configuration](#)".
- Virtual interfaces used in a cluster system cannot be activated with this command.
- No logical virtual interface can be specified for the -n option. Logical virtual interfaces are automatically activated when corresponding virtual interfaces are activated.
- This command can be specified for virtual interfaces in Fast switching mode (operation mode "t"), NIC switching mode (operation mode "d" or "e"), and GS/SURE linkage mode (operation mode "c"). This command cannot be specified for virtual interfaces in Standby patrol function (operation mode "p" or "q"), and GS/SURE linkage mode (operation mode "n").
- A standby patrol function ("p" or "q") is automatically activated when activated a virtual interface of the corresponding NIC switching mode ("d" or "e").
- A virtual interface of GS/URE linkage mode ("n") is automatically activated when activated a virtual interface of GS/SURE linkage mode ("c") that bundles this interface.
- Be sure to use a strhanet command to activate a virtual interface. Do not use an ifconfig command to do the operation. Do not operate physical interfaces that a virtual interface bundles with an ifconfig command while activating a virtual interface.
- A virtual interface for the shared-IP zone must be activated prior to zone startup. Normally, the virtual interface is activated during system startup. When the virtual interface is added after system startup, however, it is necessary to activate the virtual interface using the strhanet command before starting the zone.

[Examples]

The following is an example in which all virtual interfaces defined in the configuration information for Redundant Line Control function are activated.

```
# /opt/FJSSVhanet/usr/sbin/strhanet
```

The following is an example in which only the virtual interface sha2 defined in the configuration information for Redundant Line Control function is activated.

```
# /opt/FJSSVhanet/usr/sbin/strhanet -n sha2
```

The following shows an example to activate all virtual interfaces of Fast switching mode or NIC switching mode and also in an IPv6 address form from virtual interfaces defined in the configuration information.

```
# /opt/FJSSVhanet/usr/sbin/strhanet inet6
```

7.3 stphanet Command

[Name]

stphanet - Inactivation of virtual interfaces

[Synopsis]

```
/opt/FJSSVhanet/usr/sbin/stphanet [inet | inet6 | dual] [-n devicename1[,devicename2,...]]
```

[Feature description]

The stphanet command makes it possible to deactivate a virtual interface.

[Option]

It is possible to specify the following options:

[inet | inet6 | dual]

Specify an IP address form assigned to a virtual interface to be deactivated.

| | |
|-------|--------------------------------------|
| Inet | : IPv4 address |
| inet6 | : IPv6 address |
| dual | : IPv4/IPv6 dual stack configuration |

When omitted, virtual interfaces of all forms are to be dealt with. IPv4 and IPv6 addresses are deactivated at the same time in a virtual interface of dual stack configuration. It is not possible to deactivate only an IPv4 address or only an IPv6 address respectively. Dual stack configuration in this case does not mean IPv4 and IPv6 addresses are set on each of the stacked physical interfaces, but they are set to one virtual interface defined in a Redundant Line Control function. This option is valid only in Fast switching mode (operation mode is "t") or NIC switching mode (operation mode is "d").

-n devicename1[,devicename2,...]

Specify a virtual interface name to be inactivated. Multiple virtual interfaces can be specified by delimiting them with a comma (.). Virtual interface names specified here must have been activated by using the strhanet command. If this option is not specified, all active virtual interfaces are inactivated.

[Related commands]

strhanet
dsphanet

[Notes]

- Virtual interfaces used in a cluster system cannot be inactivated with this command.
- Only logical virtual interfaces cannot be inactivated. By terminating virtual interfaces, related logical virtual interfaces are automatically terminated.
- When inactivating virtual interfaces and logical virtual interfaces, a high-level application must be terminated first.
- It is possible to specify this command to a virtual interface of Fast switching mode (operation mode is "t"), NIC switching mode ("d" or "e"), and GS/SURE linkage mode ("c"). It is not possible to specify to a virtual interface of a standby patrol function ("p" or "q") and GS/SURE linkage mode ("n"). A Standby patrol function ("p" or "q") is automatically deactivated when deactivated a virtual interface of the corresponding NIC switching mode ("d" or "e"). A virtual interface of GS/SURE linkage mode ("n") is automatically deactivated when deactivated a virtual interface of GS/SURE linkage mode ("c") that bundles this virtual interface.
- Be sure to use a sphanet command to deactivate a virtual interface. Do not use an ifconfig command to do the operation.
- A virtual interface of standby patrol set after activated NIC switching mode and activated by strptl command is not deactivated. Use stppl command to deactivate.
- When a virtual interface of NIC switching mode is deactivated and only a virtual interface of standby patrol is activated, use stppl command to deactivate the virtual interface of standby patrol.
- If the shared-IP zone is using the virtual interface, you cannot deactivate it. First, stop the zone then deactivate the virtual interface by executing the sphanet command.
- For execution of this command for a virtual interface of NIC switching mode, if physical interfaces bundled by a virtual interface are not used in any other virtual interfaces, physical IP is also deactivated in addition to virtual IP.

[Examples]

The following is an example in which all virtual interfaces (excluding virtual interfaces in cluster operation) defined in the configuration information for Redundant Line Control function are inactivated.

```
# /opt/FJSVhanet/usr/sbin/stphanet
```

The following is an example in which only the virtual interface sha2 defined in the configuration information for Redundant Line Control function is inactivated.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha2
```

The following shows an example to inactivate all virtual interfaces of Fast switching mode or NIC switching mode and also in dual stack configuration.

```
# /opt/FJSVhanet/usr/sbin/stphanet dual
```

7.4 dsphanet Command

[Name]

dsphanet - Displaying the operation status of virtual interfaces

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/dsphanet [-n devicename1[,devicename2,...] | -o | -c]
```

[Feature description]

The dsphanet command displays the current operation status of virtual interfaces and logical virtual interfaces.

[Option]

You can specify the following options:

-n devicename1[,devicename2,...]

Specify the name of a virtual interface whose status should be displayed. You can specify more than one virtual interface by listing them delimited with a comma (.). If this option is not specified, this command displays all the virtual interfaces that are properly defined.

-o

Displays all communication parties of virtual interfaces defined in Fast switching mode (operation mode "t"). This option does not display communication parties of virtual interfaces not yet activated using the strhanet command.

-c

Displays the number of assigned connections defined in GS/SURE linkage mode (operation mode "c"). The number of connections is displayed as "-" if the concerned virtual interface is not activated. The number of connections is displayed as "-" also if the communication target monitoring function is not set or no connection is yet established.

[Display format]

The following shows the display formats used when no option is specified and when the -n option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL   Device
+-----+-----+-----+-----+-----+
sha0      Active   d    OFF  qfe0(ON),qfe1(OFF)
sha1      Active   d    OFF  qfe2(OFF),qfe3(ON)
sha2      Active   t    OFF  hme0(ON),hme1(ON)
sha3      Active   p    OFF  sha0(ON)
sha4      Active   q    OFF  sha1(ON)
[IPv6]
Name      Status   Mode CL   Device
+-----+-----+-----+-----+-----+
sha0      Active   d    OFF  qfe0(ON),qfe1(OFF)
sha1      Active   d    OFF  qfe2(OFF),qfe3(ON)
sha5      Active   t    OFF  hme2(ON),hme3(ON)
```

| Item | Explanation |
|---------------|--|
| [IPv4,Patrol] | Displays virtual interface information of an IPv4 address and standby patrol form. |
| [IPv6] | Displays virtual interface information of an IPv6 address form. |
| Name | Outputs a virtual interface name. |
| Status | Outputs the status of a virtual interface. |
| Status | Active Inactive |
| Mode | Outputs the operation mode of a virtual interface. |
| Mode | t Fast switching mode |

| Item | | Explanation |
|--------|------|---|
| | n | GS/SURE linkage mode (physical interface definition) |
| | c | GS/SURE linkage mode (virtual interface definition) |
| | d | NIC switching mode (logical IP address takeover function) |
| | e | NIC switching mode (physical IP address takeover function) |
| | p | Standby patrol function (automatic failback if a failure occurs) |
| | q | Standby patrol function (immediate automatic failback) |
| CL | | Cluster definition status |
| CL | ON | Cluster resource |
| | OFF | None cluster resource |
| Device | | Outputs the physical interface names bundled by a virtual interface and, enclosed in parentheses, the statuses of the physical interfaces. |
| Device | ON | Enabled Displays the status if the interface is enabled and also available. For the standby patrol interface, the status is displayed if the transfer path is valid. |
| | OFF | Disabled Displays the status if the virtual interface in disabled. For Fast switching and GS/SURE modes, it also displays the status when the failure is detected in the remote systems. In NIC switching mode, it displays the status when the standby patrol function is disabled. |
| | STOP | Ready for use Displays the status immediately after configuring the environment for NIC switching mode. |
| | FAIL | Error in one system Displays the status if the failure is detected on standby patrol function. |
| | CUT | Unused Displays the status if temporally dispatched by hanetnic delete command. |
| | LOST | System unstable Displays the status when the physical interface is disabled by a third person. NIC switching mode automatically recovers this symptom. However, the other redundant modes require manual recovery. |

The following shows the display format used when the -o option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -o
NIC      Destination Host Status
+-----+-----+-----+
hme0     hahostA      Active
          hahostB      Active
          hahostC      Inactive
hme1     hahostA      Active
```


| | |
|---------|----------|
| hahostB | Active |
| hahostC | Inactive |

| Item | | Explanation |
|------------------|----------|---|
| NIC | | Outputs a physical interface name. |
| Destination Host | | Outputs the host name of the communication target. (If the target host does not exist, it will display "none".) |
| Status | | Outputs the status of the communication target. |
| Status | Active | Active status |
| | Inactive | Inactive status |

The following shows the display format used when the -c option is specified.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
  Name  IFname  Connection
+-----+-----+-----+
sha0   sha2     -
      sha1     -
sha10  sha12    5
      sha11    7
```

| Item | | Explanation |
|------------|--|--|
| Name | | Outputs a virtual interface name in GS/SURE linkage mode (operation mode "c"). |
| IFName | | Outputs a virtual interface name in GS/SURE linkage mode (operation mode "n"). |
| Connection | | Outputs the number of connections. When a virtual interface is not activated, "-" is displayed. When a function to monitor the other end of communication is not set, or when a connection is not established, "-" is displayed as well. |

[Related commands]

```
strhanet
stphanet
```

[Notes]

- This command can be specified for any virtual interfaces.
- Only one option can be specified at one time.

[Examples]

The following shows an example of displaying the active or inactive status of all virtual interfaces that are properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
```

The following shows an example of displaying all the communication parties of virtual interfaces in Fast switching mode (operation mode "t") properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -o
```

The following shows an example of displaying the number of assigned connections of virtual interfaces in GS/SURE linkage mode (operation mode "c") properly defined in the configuration information for Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
```

7.5 hanetobserv Command

[Name]

hanetobserv - Setting, modifying, deleting, and displaying the information for the communication target monitoring function

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetobserv command [args]
```

[Feature description]

The hanetobserv command sets, modifies, deletes, and displays the monitoring destination information required for the operation in GS/SURE linkage mode.

| Command | Process outline | Authority |
|---------|---|--------------|
| create | Sets a monitoring destination | Super user |
| print | Displays monitoring destination information | General user |
| modify | Modifies monitoring destination information | Super user |
| delete | Deletes monitoring destination information | Super user |

(1) create command

The operation in GS/SURE linkage mode requires the monitoring of the communication target. This enables the system to continue communication using other communication paths when a failure occurs. Use the create command to generate a communication target. The following is the command format for generating a monitoring destination:

```
GS communication (If adding ipaddress):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t
nicaddress1[,nicaddress2,...] -m {on | off} [-r {on | off}]
GS communication (If adding more nicaddress to an already defined
ipaddress):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t
nicaddress3[,nicaddress4,...]
SURE communication (using SURE communication function):
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t
nicaddress1:pm-id[,nicaddress2:pm-id,...] -m {on | off} [-r {on | off}]
SURE communication (using TCP relay function):
/opt/FJSVhanet/usr/sbin/hanetobserv create -i ipaddress -c
clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]
```

-n node:

Specify a name by which to identify the node of a communication target, using up to 16 one-byte characters.

-i ipaddress:

Specify a host name or IP address of a virtual interface held by the communication target. This host name must correspond to an IP address in a network database such as the `/etc/inet/hosts` and `/etc/inet/ipnodes` files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation.

-t nicaddress1[:pm-id][,nicaddress2[:pm-id],...]:

Specify the host names or IP addresses of physical interfaces bundled by a virtual interface, by listing them delimited with a comma (,).

nicaddressX:

Specify the host name or IP address of a physical interface bundled by a virtual interface.

pm-id:

Specify the identifier of the PM (processor module) group to which the physical interface of the communication target belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication target is GS.

-m on | off:

Set whether or not to monitor the virtual interface of the monitoring destination that has been set.

Since the local host need not monitor the communication target if the remote host monitors it, specify a mode depending on the setting of the remote host.

In hot standby configuration (GS), specify this parameter only on one of the active and standby nodes when their monitoring destination information is defined.

on:

The local host monitors the communication target.

off:

The local host does not monitor the communication target.

-r on | off:

Sets if or not a RIP packet is sent from the other device. It is possible to omit this option. When omitted, RIP sending on (ON) is set. When GS has a hot standby configuration, define this parameter only in one node at setting the monitor-to information of an operation node or a standby node.

Notes)

Be sure to set RIP to "on" in order to decide which of an operation node or a standby node is working by RIP when the other system has a hot standby configuration.

on:

When sending a notification of node switching to the other system, it sends a notification of node switching waiting for receiving RIP from the other system.

off:

When sending a notification of node switching to the other system, it sends a notification of node switching to all routes without waiting for receiving RIP from the other system.

-c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]:

Specify the communication parties and destination networks with which communication should be performed using the virtual interface of the relay destination, by listing them delimited with a comma (,).

clientaddressX:

Specify the host name or IP address of a remote host or network with which communication should be actually performed. This host name must correspond to an IP address in a network database such as the /etc/inet/hosts and /etc/inet/ipnodes files. You can directly specify an IP address instead of a host name. In this case, you must specify the IP address in dotted decimal notation. If a remote network is specified, a "subnetmask" must be specified.

subnetmask:

This option must be specified when a remote network is specified in "clientaddressX". Specify the subnet mask value of the network in dotted decimal notation.

(2) print command

Use the print command to display the current monitoring destination information. The following is the format of the print command. If no option is specified, information on both the monitoring destination and the relay destination is output.

```
/opt/FJSVhanet/usr/sbin/hanetobserv print [-o] [-c]
```

-o:

Specify this option to output information on only the monitoring destination.

-c:

Specify this option to output information on only the relay destination.

The following shows an example of displaying monitoring destination information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
Destination Host Virtual Address POLL RIP NIC Address(:PMgroupID)
+-----+-----+-----+-----+-----+
hahostA          ipaddressB      ON   OFF  ipaddressC,ipaddressD
                ipaddressE,ipaddressF
hostB            ipaddressG      ON   ON   ipaddressH:1,ipaddressJ:1

Virtual Address Client Address
+-----+-----+-----+-----+
ipaddressG      host   ipaddressK
                net    10.0.0.0:255.0.0.0
```

| Item | Explanation |
|------------------|---|
| Destination Host | Outputs the host name of the communication target. |
| Virtual Address | Outputs the virtual interface name. |
| POLL | Outputs the monitoring mode. |
| RIP | With or without an RIP packet sent from the other end device. |
| POLL | ON The local host monitors the communication target. |

| Item | | Explanation |
|-------------------------|-----|--|
| | OFF | The local host does not monitor the communication target. |
| RIP | ON | With an RIP packet sent from the other host. |
| | OFF | Without an RIP packet sent from the other host. |
| NIC Address(:PMgroupID) | | Outputs the IP address or host name of a physical interface bundled by a virtual interface. An ID value is shown in parentheses. |

| Item | | Explanation |
|-----------------|------|---|
| Virtual Address | | Outputs the virtual interface name. |
| Client | | Outputs the network type of the communication destination. |
| Client | host | Indicates that the host address of the communication destination is output in "Address". |
| | net | Indicates that the network address of the communication destination is output in "Address". |
| Address | | Outputs address information of the communication destination. |

(3) modify command

Use the modify command to modify the monitoring destination information generated using the create command. The following is the format of the modify command:

```
/opt/FJSVhanet/usr/sbin/hanetobserv modify -n node,new-node |
-n node -i ipaddress,new-ipaddress |
-n node -i ipaddress -t nicaddress,new-nicaddress1[:pm-id][,new-
nicaddress2[:pm-id],...] |
-n node -i ipaddress {-m {on | off} | -r {on | off}} |
-i ipaddress -c clientaddress[:subnetmask],new-clientaddress[:subnetmask]
```

-n node,new-node:

Specify the node name of the monitoring destination information to be modified.

node:

Specify a node name that is set in the monitoring destination information (to be modified).

new-node:

Specify a node name to be used after modification.

If this parameter is specified, none of parameters "-i", "-t", and "-m" needs to be specified.

-i ipaddress,new-ipaddress:

Specify a host name or IP address of a virtual interface of the monitoring destination information to be modified. This parameter cannot be specified at the same time as when the node name or operation mode is modified.

ipaddress:

Specify a host name or IP address that is set in the monitoring destination information (to be modified).

new-ipaddress:

Specify a host name or IP address to be used after modification.

If this parameter is specified, none of new-node in parameter "-n" and parameters "-t" and "-m" needs to be specified.

-t nicaddress,new-nicaddress1[:pm-id][,new-nicaddress2[:pm-id],...]:

Specify the IP address or host name of physical interfaces bundled by a virtual interface of the monitoring information to be modified. This parameter cannot be specified at the same time as when the node name, host name or IP address of the virtual interface, or operation mode is modified.

nicaddress:

Specify the first IP addresses or host names in the IP address or host name list that bundles physical interface that are set in the monitoring destination information (to be modified). Check the first real interface names using the print command of hanetobserv.



.....
If the monitoring target data displayed from executing "hanetobserv print" command contains "ipaddressC,ipaddressD" under "NIC Address(:PMgroupID)" section, in such a case, use the headmost entry or "ipaddressC".
.....

new-nicaddress1[:pm-id][,new-nicaddress2[:pm-id],...]:

Specify all the IP address or host name of a physical interface to be bundled after modification, by listing them delimited with a comma (,).

If this parameter is specified, none of new-node in parameter "-n", new-ipaddress in parameter "-i", and parameter "-m" needs to be specified.

new-nicaddressX:

Specify the host name or IP address of interfaces to be bundled by a virtual interface.

pm-id:

Specify the identifier of the PM (processor module) group to which the physical interface of the communication target belongs when it is the SURE system. Specify a number from 1 to 8. This option is not required if the communication target is GS.

-m on | off:

Specify the operation mode of the monitoring destination information to be modified. This parameter cannot be simultaneously specified, when changing other parameters.

-r on | off:

Specify the existence of the RIP transmission from a remote system. This parameter cannot be simultaneously specified, when changing other parameters.

-c clientaddress[:subnetmask],new-clientaddress[:subnetmask]:

Modify the host name or IP address of the party with which communication should be actually performed. If a subnet mask value is specified in the information to be modified, the subnet mask value must be specified for modification.

clientaddress[:subnetmask]:

Specify the client information to be modified. If a subnet mask value is specified in the information that has been defined, the subnet mask value must be specified.

new-clientaddress[:subnetmask]:

Specify the client information to be used after modification. To specify a network, the subnet mask value must be specified.

(4) delete command

The following is the format of the delete command used to delete the monitoring destination information created using the create command:

```
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n all |
-n node1[,node2,...] |
-n node -i ipaddress1[,ipaddress2,...] |
-n node -i ipaddress -t nicaddress1[:pm-id][,nicaddress2[:pm-
id],...] |
-c all |
-i ipaddress -c all |
[-i ipaddress] -c clientaddress1[:subnetmask]
[,clientaddress2[:subnetmask],...]
```

-n all:

If all is specified, all monitoring destination information is deleted.

-n node1[, node2, ...]:

Specify a remote node name or IP address that is set in the monitoring destination information and should be deleted. You can specify more than one remote node name or IP address by listing them delimited with a comma.

-n node -i ipaddress1[,ipaddress2,...]:

Delete the virtual interface information under the node information that is set in the monitoring destination information. Specify a node name or virtual IP address attached to the virtual interface under the remote node name to be deleted. You can specify more than one node name or IP address by listing them delimited with a comma. If only one virtual interface is defined under node, the node definition information is also deleted.

-n node -i ipaddress -t nicaddress1[:pm-id][,nicaddress2[:pm-id],...]:

This command deletes the list of IP addresses or host names of physical interface assigned under virtual interface. Specify the host name or IP address of the physical interface you wish to delete. It is possible to specify more than one name or IP addresses by separating them with comma.

In the case where a single list of hostname or IP address of the physical interface is defined, the virtual interface will be deleted as well. Furthermore, if only one virtual interface is defined under the node, the configuration data including the mutual interface will be deleted as well. The host name or IP address or the physical interface can be verified using hanetobserv print command.

-c all

Delete the definition that is set to use the TCP relay function.

`-i ipaddress -c all`

Delete all the information under the virtual interface information specified in the "-i" option.

`[-i ipaddress] -c clientaddress1[:subnetmask][,clientaddress2[:subnetmask],...]`

Delete all the real NIC information to be relayed. Specify the "-i" option to delete only the real NIC information under a specific virtual interface. You can specify more than one NIC by listing them delimited with a comma.

[Notes]

- Configuration information must be defined before a monitoring destination is created.
- This command can be set if a virtual interface in GS/SURE linkage mode (operation mode "c") is defined.
- To add, delete, or change a monitoring destination, the virtual interface in GS/SURE linkage mode (operation mode "c") must be inactivated.
- No monitoring destination registered in a cluster can be deleted or changed. First release the cluster definition and then delete or change the monitoring destination.
- An IP address or host name to be specified when the communication target monitoring function is set or changed must be defined in `/etc/inet/hosts` and `/etc/inet/ipnodes`.
- The node name information must not be specified as "all".
- Up to 32 physical interfaces can be specified to be bundled by the virtual interface of the communication target to be specified in the monitoring destination information.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change the corresponding host name on the host database of such as `/etc/inet/hosts` and `/etc/inet/ipnodes` files. To change the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.
- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in `/etc/inet/hosts` and `/etc/inet/ipnodes` so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.

[Examples]

(1) create command

The following shows a setting example in which monitoring is performed while the communication target's node hahostA has virtual IP address "vip1", which bundles two physical IP address ipaddressC and ipaddressD. The host name is assumed to be associated with the IP address in the `/etc/inet/hosts` file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip1 -t  
ipaddressC,ipaddressD -m on
```

The following shows a setting example in which monitoring is not required because the already defined communication target hahostA has virtual IP address "vip2", which bundles physical IP address ipaddressF and ipaddressG. The host name is assumed to be associated with the IP address in the `/etc/inet/hosts` file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip2 -t  
ipaddressF,ipaddressG -m off
```

The already defined communication target hahostA has virtual IP address "vip2", which bundles two physical IP addresses ipaddressF and ipaddressG. The following shows a setting example in which new physical IP addresses ipaddressH and ipaddressJ are bundled and

added to virtual IP address "vip2". The system takes over the monitoring mode used when physical IP addresses ipaddressF and ipaddressG are set. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip2 -t
ipaddressH,ipaddressJ
```

Define the SURE interface to be used to communicate with the node of the communication target when the TCP relay function in GS/SURE linkage mode is used. The SURE virtual IP address "vip2" to be used is assumed to be already defined. The following shows a setting example in which a network (10.0.0.0) is added to the communication target. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -i vip2 -c
10.0.0.0:255.0.0.0
```

(2) print command

The following shows an example of displaying the configuration information list of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
```

(3) modify command

The following shows an example of changing the node name (hahostB) in the communication target monitoring destination information to hahostH.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB,hahostH
```

The following shows an example of changing the virtual IP address "vip1" of the node (hahostB) in the communication target monitoring destination information to "vip2".

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1,vip2
```

The following shows an example of changing the physical IP addresses (ipaddress1 and ipaddress2) bundled by virtual IP address "vip1" of the node (hahostB) in the communication target monitoring destination information to ipaddress3, ipaddress4, and ipaddress5.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip1 -t
ipaddress1,ipaddress3,ipaddress4,ipaddress5
```

The following shows an example of changing the physical IP addresses (ipaddress6 and ipaddress7) bundled by virtual IP address "vip2" of the node (hahostB) in the communication target monitoring destination information to ipaddress7 and ipaddress8.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -i vip2 -t
ipaddress6,ipaddress7,ipaddress8
```

The following shows an example of changing the "on" setting of the monitoring mode of the node (hahostB) in the communication target monitoring destination information to "off".

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -n hahostB -m off
```

The following shows an example of changing the communication target (ipaddress6) in the relay destination information (ipaddress6 and ipaddress7) of the virtual IP address "vip2" in the communication target monitoring destination information to a network specification (10.0.0.0, 255.0.0.0).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv modify -i vip2 -c
10.0.0.0:255.0.0.0,ipaddress7
```

(4) delete command

The following shows an example of deleting all the monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n all
```

The following shows an example of deleting all the information held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA
```

The following shows an example of deleting the information under the virtual IP address "vip1" held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA -i vip1
```

The following shows an example of deleting the information under the virtual IP address "vip1" held by the monitored host (hahostA).

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA -i vip1
```

The following shows an example of deleting the physical IP addresses (ipaddressC, ipaddressD) under the virtual IP address "vip1" in the TCP relay information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -i vip1 -c
ipaddressC,ipaddressD
```

7.6 hanetparam Command

[Name]

hanetparam - The setting value of various functions is changed or displayed

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetparam {-w sec | -m times | -l times | -p sec | -o times | -d {plumb |
unplumb} | -c {on | off} | -s {on | off}}
/opt/FJSVhanet/usr/sbin/hanetparam print
```

[Feature description]

The hanetparam command sets up the monitoring function when the Fast switching operation or the standby patrol function is used. This command also changes the method of activating and inactivating Fast switching mode and NIC switching mode.

[Option]

You can specify the following options:

< Valid options in fast switching mode >

-w value

Specify the interval (value) for monitoring the communication target in Fast switching mode. A value from 0 to 300 can be specified. No monitoring is performed if 0 is specified in value. By default, 5 is specified. This parameter is enabled only for Fast switching mode.

-m value

Specify the monitoring retry count (value) before message output when the message output function for a line failure is enabled.

Specify the monitoring retry count (value) before message output. A value from 0 to 100 can be specified. No message is output if 0 is specified in value. By default, no message is output. This parameter is enabled only for Fast switching mode.

-l value

Specify the cluster failover function.

Specify how many times (count) communication with the communication target can fail consecutively before cluster failover is performed. A value from 0 to 100 can be specified. No cluster failover is performed if 0 is specified in value. When performing cluster failover, the number of times for repeating surveillance is specified in the range from 1 time to 100 times until it cluster failover. By default, cluster failover is specified to be performed if communication fails five consecutive times. This parameter is enabled only for Fast switching mode on a cluster system.

-c value

When operating Fast switching mode on a cluster system and when an error occurred in all transfer routes at the activation of a userApplication, sets if or not to execute failover between clusters (job switching between nodes).

Specify "on" to value for executing failover between clusters (job switching between nodes) when an error occurred in all transfer routes at activation of a userApplication.

Specify "off" to value for not executing failover between clusters when an error occurred in all transfer routes at activation of a userApplication.

"off" is set to value as an initial setting value.

-s value

Specify if or not to output a message when a physical interface, which a virtual interface uses, changed the status (detected an error in a transfer route or recovery). A value possible to specify is "on" or "off". When specified "on", a message is output (message number: 990, 991, and 992). When specified "off", a message is not output. The initial value is "off". This parameter is valid only in fast switching mode.

< Valid options in NIC switching mode >

-p value

Specify the interval (value) in seconds for monitoring paths between operation NIC and standby NIC when the standby patrol function is enabled. A value from 0 to 100 can be specified. No monitoring is performed if 0 is specified in value.

Do not specify 0 to this parameter when set a user command execution function (executing a user command when standby patrol detected an error or recovery). User command execution does not function if specified 0.

By default, 15 is specified. This parameter is enabled only for NIC switching mode.

-o value

Specify the monitoring retry count (value) before message output when the message output function for a standby patrol failure is enabled.

Specify the monitoring retry count (value) before message output. A value from 0 to 100 can be specified.

When specified 0, stop outputting messages and make monitoring by a standby patrol function invalid. Do not specify 0 to this parameter when set a user command execution function (executing a user command when standby patrol detected an error or recovery). User command execution does not function, if specified 0.

By default, 3 is specified. This parameter is enabled only for NIC switching mode. The number of the times of continuous monitoring is "a set value of this option x 2" immediately after started standby patrol.

-d value

Use this parameter to change the method of inactivating the standby interface in NIC switching mode. Specify "plumb" in value to inactivate the standby interface and set "0.0.0.0" as the IP address. Specify "unplumb" in value to inactivate and delete the standby interface. Initially, "plumb" is specified in value.

Do not specify "unplumb" for the following situations:

- When configuring high-reliable networks of the shared-IP zone with the NIC switching mode
- When configuring high-reliable LinkAggregation which the LACP mode is active with the NIC switching mode

If other than "plumb" is specified, the communication will be down after NIC switching.

| Setting | Interface | | | | | |
|---------|-----------|------------|---------------------------|----------|------------|---------------------------|
| | Operating | | | Standby | | |
| | Status | IP address | Allocation of logical I/F | Status | IP address | Allocation of logical I/F |
| plumb | Active | Yes | Possible | Inactive | 0.0.0.0 | Possible |
| unplumb | Active | Yes | Possible | Unused | - | Impossible |

< Valid options in all modes >

print:

Outputs a list of settings.

The following shows the output format:

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
Line monitor interval(w)      :5
Line monitor message output (m) :0
Cluster failover (l)         :5
Standby patrol interval(p)    :15
Standby patrol message output(o) :3
NIC switching mode(d)        :Plumb
Cluster failover in unnormality (c):OFF
Line status message output (s) :OFF
```

| Item | Explanation | |
|-----------------------------------|---|---|
| Line monitor interval (w) | Outputs the setting for the transfer path monitoring interval. | |
| Line monitor message output (m) | Outputs the monitoring retry count before message output when a line failure occurs. | |
| Cluster failover (l) | Outputs the consecutive monitoring failure count before execution of cluster failover. | |
| Standby patrol interval (p) | Outputs the monitoring interval of the standby patrol. | |
| Standby patrol message output (o) | Outputs the consecutive monitoring failure count before output of a message when a standby patrol failure occurs. | |
| NIC switching mode (d) | Outputs the method of inactivating the standby interface in NIC switching mode. | |
| NIC switching mode (d) | Unplumb | Inactivates the standby interface and deletes. |
| | Plumb | Inactivates the standby interface and sets the IP address as "0.0.0.0". |

| Item | | Explanation |
|------------------------------------|-----|---|
| Cluster failover in unnormality(c) | | Workings when an error occurred in all transfer routes at activating a userApplication. |
| Cluster failover in unnormality(c) | ON | Cluster switching immediately occurs. |
| | OFF | Cluster switching does not occur at activating a userApplication. |
| Line status message output (s) | | With or without a message output when a physical interface changed the status. |
| Line status message output (s) | ON | A message is output. |
| | OFF | A message is not output. |

[Related command]

hanetpoll

[Notes]

- This command can be specified for a virtual interface in Fast switching mode (operation mode "t"), NIC switching mode (operation mode "d" or "e"), and standby patrol function (operation mode "p" or "q").
- The setting by this command is valid in the whole system. It is not possible to change in a unit of virtual interface.
- After executing this command, reboot the system immediately. The applied value will not be effective until the system restarts.

[Examples]

< Example of Fast switching mode >

(1) Example of setting monitoring the communication target interval

The following shows an example of using this command to perform monitoring at intervals of 5 seconds.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -w 5
```

(2) Example of enabling or disabling the message output function used when a line failure occurs

The following shows an example of using this command to output a message if communication with the communication target fails five consecutive times.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -m 5
```

(3) Example of setting the cluster failover function

The following shows an example of using this command to perform cluster failover if communication with the communication target fails five consecutive times.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -l 5
```

(4) A setting example of the workings when an error occurred in every transfer route at the activation of a userApplication

An example of a command to execute failover between clusters when an error occurred in every transfer route immediately after activated a userApplication is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -c on
```

(5) An example of setting with/without outputting a message when a physical interface, which a virtual interfaces uses, changed the status

An example of a command to output a message when a physical interface, which a virtual interface uses, changed the status is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanetparam -s on
```

< Example of NIC switching mode >

(1) Example of setting the standby patrol monitoring interval

The following shows an example of using this command to perform monitoring at intervals of five seconds.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -p 5
```

(2) Example of setting the message output function used when a standby patrol failure occurs

The following shows an example of using this command to output a message when communication with the communication target fails five consecutive times.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -o 5
```

(3) Example of changing the method of inactivating the standby interface

The following shows an example of using this command to inactivate the standby interface and set "0.0.0.0" as the IP address (using a virtual interface from the shared-IP zone).

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

< Example common to all modes >

(1) Example of executing the status display command

The following shows an example of displaying the settings made using the hanetparam command.

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
```

7.7 hanetpoll Command

[Name]

hanetpoll - Setting, modifying, deleting, and displaying the monitoring destination information for the HUB monitoring function

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetpoll command [args]
```

[Feature description]

The hanetpoll command sets the monitoring destination information required for the HUB monitoring function. This command also modifies, deletes, displays, enables, or disables the settings.

| command | Process outline | Authority |
|---------|--|--------------|
| create | Creates monitoring destination information | Super user |
| copy | Copies monitoring destination information (synchronous switch) | Super user |
| print | Displays monitoring destination information | General user |
| modify | Modifies monitoring destination information | Super user |
| delete | Deletes monitoring destination information | Super user |
| on | Enabling the HUB monitoring function | Super user |
| off | Disabling the HUB monitoring function | Super user |

(1) create command

The operation of the HUB monitoring function requires the definition of monitoring destination information. Use the create command to define monitoring destination information.

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n devicename -p  
polladdress1[,polladdress2] [-b {on | off}]
```

-n devicename:

Specify the name of a virtual interface to be monitored. Specify a virtual interface created using the hanetconfig create command or the hanetconfig copy command. No logical virtual interface name can be specified.

-p polladdress1[,polladdress2]:

Specify the host name or IP address of the monitored HUB.

For single physical interface (single interface bundled by virtual interface):

Set at least one monitoring destination. Up to two can be set.

Specify a host name of the monitoring destination or IP address to polladdress1.

If there is a second monitoring destination, specify a host name of the monitoring destination or IP address to polladdress2.

For dual configurations (multiple interfaces bundled by virtual interface):

It is recommended to set two monitoring destinations. At least set one.

If there are two monitoring destinations, specify a host name of the HUB that the Primary interface connects or IP address to polladdress1. For polladdress2, specify a host name of the HUB that the Secondary interface connects or IP address.

For single monitoring destination, specify a host name of the monitoring destination or IP address to polladdress1.



Note

When setting monitoring location with an IP address, IPv4 address or IPv6 address can be set as an address from.

When setting an IPv6 address, do not specify a prefix value.

When setting an IPv6 address in the environment where the automatic address configuration by an IPv6 router is not performed, set the

link-local address.

Also, when specifying a monitor-to host name, do not use the same name that exists in IPv4 and IPv6.

-b on | off:

If two HUBs are specified as monitoring destinations in NIC switching mode, communication between the primary and secondary HUBs can be monitored.

on: Monitors communication between two HUBs.

off: Does not monitor communication between two HUBs.

(2) copy command

Use this command when copying monitoring target's information to a virtual interface on NIC Switching mode or when synchronizing the switching operation of virtual interface.

This command thus allows monitoring destination information to be automatically created by using the copy source information and without requiring you to specify monitoring destination information and HUB-to-HUB monitoring mode. This command realizes simpler operation than directly executing the hanetpoll create command. The following is the command format for the copy command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n devicename1,devicename2
```



Point

If you have used tagged VLAN interface on NIC Switching mode and created more than one virtual interface, which have disparate network address, you must keep in account that multiple IP address cannot be configured as monitoring target on Switch/HUB running VLAN. In such a case, it is possible to implement synchronous switching in between virtual interfaces using the same physical interface. This allows a virtual interface, which does not have the IP address for monitoring target to perform fail back operation by synchronizing with a virtual interface, which already has the existing monitoring target. In order to synchronize the switching operation of virtual interface, use the "copy" command (it is possible to specify disparate network addresses).

-n devicename1,devicename2:

Specify the names of virtual interfaces from and to which monitoring destination information should be copied.

devicename1:

Specify the name of a virtual interface that is set in monitoring information in the copy source.

devicename2:

Specify the name of a new virtual interface to be monitored. Specify a virtual interface created using the hanetconfig create command or the hanetconfig copy command. No logical virtual interface name can be specified.

(3) print command

Use the print command to display the current monitoring destination information. Use this command to view the current monitoring destination information. The following is the format of the print command.

```
/opt/FJSVhanet/usr/sbin/hanetpoll print [-n  
devicename1[,devicename2,...]]
```


-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces whose monitoring destination information should be displayed. If this option is not specified, the print command displays all the monitoring destination information currently specified.

The following shows an example of displaying information without any option specified.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
[ Standard Polling Parameter ]
    interval(idle)    =    5( 60) sec
    times              =    5 times
    max_retry          =    5 retry
    repair_time        =    5 sec
    link detection     =    NO
    failover mode      =    YES

[ Polling Parameter of each interface ]
Name      Hostname/Polling Parameter
+-----+-----+
sha0      swhub1,swhub2
          hub-hub poll      =    OFF
          interval(idle)    =    5( 60) sec
          times              =    5 times
          max_retry          =    5 retry
          repair_time        =    5 sec
          link detection     =    NO
          failover mode      =    YES

Name      Hostname/Polling Parameter
+-----+-----+
sha1      swhub3,swhub4
          hub-hub poll      =    OFF
          interval(idle)    =    5( 60) sec
          times              =    5 times
          max_retry          =    5 retry
          repair_time        =    5 sec
          link detection     =    NO
          failover mode      =    YES
```

| Item | | Explanation |
|-------------------------------------|----------|--|
| Standard Polling Parameter | | Common monitoring information |
| Polling Parameter of each interface | | Each monitoring information |
| Name | | Displays the name of a virtual interface to be monitored. |
| Hostname | | Displays the host name or IP address to be monitored, in the order of the primary and secondary monitoring destinations. |
| hub-hub poll | | Displays the inter-HUB monitoring status. |
| hub-hub poll | ON | The monitoring function is enabled. |
| | OFF | The monitoring function is disabled. |
| | --- | The monitoring function is not used. |
| interval(idle) | interval | Displays the monitoring interval in the stationary status. |
| | idle | Displays in seconds the wait time that elapses after monitoring starts and before the HUB links up. |
| times | | Displays the monitoring count. |

| Item | | Explanation |
|----------------|-----|---|
| max_retry | | Displays the consecutive failure occurrence count before failure notification. |
| repair_time | | Displays the recovery monitoring interval in seconds. |
| link detection | YES | Detects link-based failures. |
| | NO | Does not detect link-based failures. |
| failover mode | | With or without cluster switching when an error occurred in all transfer routes. |
| failover mode | YES | Node switching is performed when the virtual interface is registered in the cluster resource. |
| | NO | No node switching is performed. |

(4) modify command

Use the modify command to modify the monitoring destination information.

```
/opt/FJSVhanet/usr/sbin/hanetpoll modify -n devicename {[-p
polladdress1[,polladdress2]] [-b {on | off}]}
```

-n devicename:

Specify the name of a virtual interface whose monitoring destination information should be modified.

-p polladdress1[,polladdress2]:

Specify the host names or IP addresses of the monitoring destinations to be modified. See the -p option of (1) create command.

-b on | off:

Set whether or not to use HUB-to-HUB monitoring (Monitoring on/off for). For details, see the -b option of (1) create command.



Note

Changing the number of monitoring target from two targets to one target, verify that HUB-to-HUB monitoring exists, and if the value is set "on", then change it back to "off".

(5) delete command

Use the delete command to delete the monitoring destination information. The following is the format of the delete command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll delete -n
{devicename1[,devicename2,...] | all}
```

-n devicename1[,devicename2,...]:

Specify the names of virtual interfaces (such as sha0 and sha1) whose monitoring destination information should be deleted.

all:

Specify this parameter to delete all the defined monitoring destination information.

(6) on command

To make the created HUB monitoring function valid, and to change an interval to monitor a HUB monitoring function, and a monitoring function of the other end of communication in GS/SURE linkage mode, use the on command:

```
NIC switching mode or GS/SURE linkage mode:
/opt/FJSVhanet/usr/sbin/hanetpoll on [-s sec] [-c times] [-r retry] [-b sec] [-f
{yes | no}] [-p sec] [-l {yes | no}]
NIC switching mode (When a specific virtual interface is specified):
/opt/FJSVhanet/usr/sbin/hanetpoll on -n devicename [-d] | [[-s sec] [-c times]
[-b sec] [-f {yes | no}] [-p sec] [-l {yes | no}]]
```

-n devicename:

Specify the virtual interface name (such as sha0, sha1) used in NIC switching mode for enabling HUB monitoring feature. If this option is not specified, the entire virtual interfaces, which have the monitoring target configured, will be selected.

When specifying the virtual interface with this option, the setting values of the virtual interface will become the setting values of the specific monitoring information regardless of whether the common monitoring information is changed or not. When operating the virtual interface using the same setting value as the common monitoring information, use this option and the -d option to change the information to the common monitoring information.

In addition, the virtual interface which is sharing NIC synchronizes and enables a HUB monitoring function.

-d:

Changes the value of individually modified monitoring information such as monitoring period and monitoring frequency, into the configuration values that are defined in the common monitoring information. However, this option is only available when '-n' option was individually specified for the virtual interface on NIC Switching mode. (For details on common monitoring information, see the display format of (3) print command)

-s sec:

Specify the monitoring time in seconds. A value from 1 to 300 can be specified (note that the product of sec and times must be 300 or less). When HUB-to-HUB monitoring is enabled or when two monitoring destinations are set in a single physical interface configuration, set the monitoring time to 2 seconds or longer. If this option is not specified, the previous setting is enabled. Initially, 5 (seconds) is specified.

-c times:

Specify the monitoring count. A value from 1 to 300 can be specified (note that the product of sec and times must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified.

-b sec:

Specify the monitoring period when a failure is detected by monitoring the remote host by GS/SURE linkage mode. The values which can be specified are from 0 to 300. If this option is not specified, the previous setting is enabled. Initially, 5 (seconds) is specified.

-f yes | no:

Specify the operation used when node switching occurs due to a line failure during cluster operation. If this option is not specified, the previous setting is enabled. Initially, "yes" is specified. (This parameter is enabled only during cluster operation.)

yes: Node switching is performed if a line monitoring failure occurs.

no: No node switching is performed if a line monitoring failure occurs.

-p sec:

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in NIC switching mode and GS/SURE linkage mode. A value from 1 to 300 can be specified. If this option is not specified, the previous setting is enabled. Initially, 60 (seconds) is specified. If the specified value is less than "monitoring interval" multiplied by "monitoring count," the system ignores the specified link-up time and adopts the time calculated by multiplying "monitoring interval" by "monitoring count."

-l yes | no:

Specify whether to detect link-based failures of a physical NIC in NIC switching mode. If this option is not specified, the previous setting is enabled. Initially, "yes" is specified.

yes: Enables detection of link-based failures.

no : Disables detection of link-based failures.

When setting this option to "yes", control the monitoring or switching as follows based on the link status of a physical NIC:

- When activating NIC by using the "strhanet" command, if the status is One-system failure due to the link down of the primary NIC, stop using the primary NIC and activate the secondary NIC.
- If the monitoring fails due to the link down of a physical NIC, it is immediately considered as transfer route failure instead of retrying the monitoring.
- When switching NICs due to the failure of the monitoring, check the status of the NIC to be switched beforehand. If the status is link down and the link down status has continued for 5 seconds or longer (when the standby patrol is set: 2.5 seconds or longer), restrict switching NICs.



Note

NIC link down by the link status monitoring function cannot be detected in the following environments:

- Oracle VM environments where virtual switches (vswX) or virtual network devices (vnetX) are bundled and physical link status is not reflected.
- Environments where the virtual NIC (VNIC) of Solaris 11 or later is used.

This is because the operating system does not notify NIC link down to the interfaces bundled by GLS even if NIC link down is detected on physical NICs. The route is switched after a failure is detected by the HUB monitoring function, not by the link status monitoring function.

Use the `ldm(1M)` command to reflect the physical link status. For details on the `ldm(1M)` command, see Solaris documentation.

(7) off command

Use the off command to disable the HUB monitoring function. The following is the format of the off command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll off [-n devicename]
```

-n devicename:

Specify the virtual interface name (such as sha0, sha1) used in NIC switching mode for disabling HUB monitoring feature. If this option is not specified, the entire virtual interfaces, which have the monitoring target configured, will be chosen. In addition, the virtual interface which is sharing NIC synchronizes and disables a HUB monitoring function.

[Notes]

- Before monitoring destination information can be specified using this command, configuration information must be set using the `hanetconfig` command.
- This command can be specified for a virtual interface in NIC switching mode (operation mode "d" or "e"). (In GS/SURE linkage mode, only the functions of enabling and disabling the monitoring function are available.)

- A virtual interface to be used in the cluster system is monitored only while a userApplication to which the virtual interface belongs is in operation.
- The monitoring of HUBs is not performed when the HUB monitoring function is specified to virtual interface in Fast switching mode. In this case, an error message is output to indicate this fact and the HUB is not monitored.
- The monitoring time and count to be specified using the hanetpoll on command must be specified so that their product does not exceed 300.
- The retry count to be specified using the hanetpoll on command can be set to 0 from 99999. Monitoring continues indefinitely if 0 is specified.
- Use the hanetpoll print command to display the latest user-defined information (result of create, delete, modify, on, and off) but not to display the current status of the HUB monitoring.
- If any valid monitoring destination information exists, monitoring automatically starts when the system is started up.
- Be sure to define in the /etc/inet/hosts file IP addresses and host names to be specified when the monitoring destination information is set or modified.
- When specified a numeric string for a host name, it is dealt with as decimal and converted into an IP address corresponding to its value to work. (For instance, when specified "123456", it is regarded an IP address "0.1.226.64" is specified.)
- When setting the same monitor-to device for the monitor-to information of more than one virtual interface, use a copy command, for setting the second and after.
- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.
- When specified a host name with this command to where a host name or an IP address should be set, it is not possible to change a corresponding host name on the database such as /etc/inet/hosts and /etc/inet/ipnodes files. To change host name information, it is necessary to delete the definition of a Redundant Line Control function that uses a corresponding host name, and to reset.
- Do not use characters other than alphanumeric characters, period, and hyphen for the host name. If characters other than the above are used, re-write the host names in /etc/inet/hosts and /etc/inet/ipnodes so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.

[Examples]

(1) create command

The following shows an example of creating configuration information for monitoring two routers routerA and routerB on virtual interface sha2. The host name is assumed to be associated with the IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha2 -p routerA,routerB
```

(2) copy command

The following is an example of copying monitoring target data defined in virtual interface sha0 for NIC Switching mode into sha1. (By copying the configuration data of sha0 onto sha1, when sha0 performs failover operation, sha1 also fails back along with sha0).

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

(3) print command

The following shows an example of displaying the configuration information list of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
```

(4) modify command

The following shows an example of changing configuration information for monitoring two routers routerA and routerB to routerA and routerC on virtual interface sha2. The host name is assumed to be associated with the virtual IP address in the /etc/inet/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha2 -p routerA,routerC
```

(5) delete command

The following shows an example of deleting the monitoring destination information on virtual interface sha2 from the definition.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll delete -n sha2
```

(6) on command

The following shows an example of starting the HUB monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

The following is an example of starting HUB monitoring function specifying the virtual interface sha0 for NIC Switching mode.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on -n sha0
```

(7) off command

The following shows an example of stopping the HUB monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

The following is an example of stopping HUB monitoring function specifying the virtual interface sha0 for NIC Switching mode.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off -n sha0
```

7.8 dsppoll Command

[Name]

dsppoll - Displaying the monitoring status

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/dsppoll [-n devicename | -c]
```

[Feature description]

The dsppoll command displays the current monitoring status of monitoring information created using the hanetpoll or hanetobserv command.

[Option]

You can specify the following options:

-n devicename:

Specify virtual interface name for NIC Switching modes. If this option is not specified, the entire interface, which has monitoring target configured will be chosen.

-c:

When this option is specified, displays monitoring information in GS/SURE linkage mode (operation mode "c").

[Display format]

The following is a display format example of when specifying or not specifying virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
+-----+
sha0  Polling Status      =      ON
      Primary Target(status) = swhub1(ON)
      Secondary Target(status) = swhub2(WAIT)
      HUB-HUB status      =      OFF
      interval(idle)      =      5( 60)  times      =      5
      repair_time        =      5      retry        =      5
      link detection      =      NO      FAILOVER Status =      YES
+-----+
shal  Polling Status      =      ON
      Primary Target(status) = swhub3(ON)
      Secondary Target(status) = swhub4(WAIT)
      HUB-HUB status      =      OFF
      interval(idle)      =      5( 60)  times      =      5
      repair_time        =      5      retry        =      5
      link detection      =      NO      FAILOVER Status =      YES
+-----+

# /opt/FJSVhanet/usr/sbin/dsppoll -n sha0

Polling Status      =      ON
interval            =      5
idle                =      60
times               =      5
retry               =      5
repair_time         =      5
link detection      =      NO
failover mode       =      YES
Status  Name  Mode  Primary Target/Secondary Target      HUB-HUB
+-----+-----+-----+-----+-----+-----+
ON  sha0  d  swhub1(ON)/swhub2(WAIT)      OFF
```

| Item | | Explanation |
|--|-----|---|
| Polling Status (when -n is specified) | ON | The monitoring function is enabled. |
| | OFF | The monitoring function is disabled. |
| Polling Status (when -n is not specified) | ON | Monitoring is in progress. |
| | OFF | Monitoring is stopped. |
| interval | | Displays in seconds the monitoring interval in the stationary status. |
| idle | | Displays in seconds the wait time that elapses after monitoring starts and before the HUB links up. |
| times | | Displays the monitoring count. |

| Item | | Explanation |
|--|--------|--|
| retry | | Displays the retry count at which router monitoring should be stopped if a failure is detected. This parameter is meaningless for a virtual interface in NIC switching mode (operation mode "d" or "e") because "1" is set for it. |
| repair_time | | Displays the recovery monitoring interval in seconds. |
| link detection | YES | Detects link-based failures. |
| | NO | Does not detect link-based failures. |
| FAILOVER Status or failover mode | | With or without cluster switching when an error occurred in all transfer routes. |
| FAILOVER Status or failover mode | YES | Node switching is performed when the virtual interface is registered in the cluster resource. |
| | NO | No node switching is performed. |
| Status | | Displays the current status of the monitoring function. |
| Status | ON | Monitoring is in progress. |
| | OFF | Monitoring is stopped. |
| Name | | Displays the name of a virtual interface to be monitored. |
| Mode | d | NIC switching mode (logical IP address takeover function) |
| | e | NIC switching mode (physical IP address takeover function) |
| Primary Target(status) Secondary Target(status) | | Displays monitoring status in Primary/Secondary monitor-to IP address or a host name and parenthesis. |
| | | (ON) Monitoring is in progress. |
| | | (WAIT) Waiting is in progress. |
| | | (FAIL) Monitoring failed (monitoring is stopped). |
| | | (STOP) Unused. |
| HUB-to-HUB status | | Displays the status of HUB-to-HUB communication monitoring. |
| HUB-to-HUB status | WAIT | HUB-to-HUB monitoring has stopped. |
| | ACTIVE | HUB-to-HUB monitoring is operating. |
| | FAIL | HUB-to-HUB monitoring has failed. |
| | OFF | HUB-to-HUB monitoring is unused. |
| | ---- | When RIP mode is being used. |

The following is the display format of monitoring status obtained when the -c option is specified.

```

# /opt/FJShanet/usr/sbin/dsppoll -c
Node          VIP          POLL RIP      NIC          Status
-----+-----+-----+-----+-----+
192.13.75.1   192.13.75.13  ON  ON   hahostA      ACTIVE
                192.13.73.12  FAIL
                192.13.72.19  ACTIVE
                192.13.73.19  ACTIVE
hahostB      hahostC      ON  OFF  192.13.72.19  ACTIVE
                192.13.73.19  ACTIVE

```


| | | | | |
|---------|-----|-----|--------------|------|
| hahostB | OFF | OFF | 192.13.72.19 | ---- |
| | | | 192.13.73.19 | ---- |

| Item | | Explanation |
|--------|--------|--|
| Node | | Displays the name of a node to be monitored. |
| VIP | | Displays the name of a virtual interface held by the monitored node. |
| POLL | | Displays the operation mode of a virtual interface to be monitored. |
| POLL | ON | The monitoring function is enabled. |
| | OFF | The monitoring function is disabled. |
| RIP | | Displays if or not a RIP packet is sent from the other device. |
| RIP | ON | RIP sending on (ON) from the other device. |
| | OFF | RIP sending off (OFF) from the other device. |
| NIC | | Displays the hostname or IP address of a real interface to be monitored. |
| Status | | Displays the monitoring status of a virtual interface. |
| Status | ACTIVE | Monitoring is in progress. |
| | FAIL | Monitoring failed (recover monitoring in progress). |
| | ---- | Monitoring is not yet performed. |

[Related commands]

hanetpoll
hanetobserv

[Notes]

- If no option is specified, this command can be specified for a virtual interface in NIC switching mode (operation mode "d" or "e").
- If the "-c" option is specified, this command can be specified for a virtual interface in GS/SURE linkage mode (operation mode "c").

[Examples]

(1) To display all the monitoring statuses NIC Switching mode.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
```

(2) To display polling status of virtual interface sha0 for NIC Switching mode.

```
# /opt/FJSVhanet/usr/sbin/dsppoll -n sha0
```

(3) When the monitoring information on GS/SURE linkage mode is displayed.

```
# /opt/FJSVhanet/usr/sbin/dsppoll -c
```

7.9 hanetnic Command

[Name]

hanetnic - Dynamic addition/deletion/switching of physical interfaces

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetnic command [args]
```

[Feature description]

The hanetnic command can add, delete, or switch physical interfaces to be used dynamically while the relevant virtual interface is active.

| Command | Process outline | Authority |
|---------|---------------------------------|------------|
| add | Adds physical interfaces | Super user |
| delete | Deletes physical interfaces | Super user |
| change | Changes physical interface used | Super user |

Note

When adding, deleting, or switching interfaces dynamically using this command, the virtual interface must be active.

Point

Dynamic addition or deletion of a redundant physical interface is enabled even when a virtual interface of fast switching is set for the network setting of the shared-IP zone.

(1) add command

This command adds physical interfaces bundled by a virtual interface in Fast switching mode and GS/SURE linkage mode (operation mode "c") dynamically. (Physical interfaces are added while the virtual interface is active.) The following is the format of the add command:

```
/opt/FJSVhanet/usr/sbin/hanetnic add -n devicename -i interface [-f]
```

-n devicename:

Specify a virtual interface name to which the physical interface to be added belongs. It is possible to specify only virtual interface names with Fast switching mode (operation mode "t") and GS/SURE linkage mode (operation mode "c") specified.

-i interface:

Specify a name of an interface to be added.

When dynamically adding (which requires to modification of the configuration information) a virtual interface, set a name of a new interface.

Similarly, for actively exchanging an interface (which does not require modification in the configuration information), run the dsphanet command in order to identify the name of the interface to be added. Moreover, within the interface name displayed in "Device" field, specify the interface name displayed as "(CUT)".

Note

The interface name specified in this option is an actual interface name (such as hmeX) for Fast switching. However, specification of the virtual interface (shaX) name used in operation mode "n" is required for GS/SURE linkage mode.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic addition.)

(2) delete command

This command deletes physical interfaces bundled by a virtual interface in Fast switching mode and GS/SURE linkage mode (operation mode "c") dynamically (Physical interfaces are deleted while the virtual interface is active). The following is the format of the delete command:

```
/opt/FJSVhanet/usr/sbin/hanetnic delete -n devicename -i interface [-f]
```

-n devicename:

Specify a virtual interface name to which the physical interface to be deleted belongs. It is possible to specify only virtual interface names with Fast switching mode (operation mode "t") and GS/SURE linkage mode (operation mode "c").

-i interface:

Specify the name of the interface for deletion.

First, run the dsphanet command to identify the name of the interface subjected for deletion. Then, specify the interface name in the "Device" field where virtual interface displayed.

Note

The interface name specified in this option is actual interface name (such as hmeX) for Fast switching. However, specification of the virtual interface (shaX) name used in operation mode "n" is required for GS/SURE linkage mode.

-f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic deletion.)

(3) change command

This command changes physical interfaces used in a virtual interface in NIC switching mode to those of the standby system. The following is the format of the change command:

```
/opt/FJSVhanet/usr/sbin/hanetnic change -n devicename
```

-n devicename:

Specify the virtual interface name of the used physical interface to be changed. It is possible to specify only virtual interface names with NIC switching mode (operation mode "d" or "e") specified.

[Notes]

As for an actual interface to dynamically add for a virtual interface of Fast switching mode (the operation mode is "t"), be sure to define to use in TCP/IP before adding dynamically. (Check if or not there is /etc/hostname.interface file. If not, create it. Then execute "/usr/sbin/ifconfig a name of the actual interface plumb" command, and activate the interface.)

[Examples]

(1) add command

The following example adds hme0 to the bundled physical interfaces in the virtual interface sha0. It is assumed that sha0 has already been defined in Fast switching mode (operation mode "t") and hme0 has been deleted by using the "hanetnic delete" command.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i hme0
```

(2) delete command

The following example deletes hme1 from the bundled physical interfaces in the virtual interface sha0. It is assumed that sha0 has already been defined in Fast switching mode (operation mode "t").

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i hme1
```

(3) change command

The following example replaces physical interfaces used in the virtual interface sha0 with those of the standby system. It is assumed that sha0 has already been defined in NIC switching mode (operation mode "d").

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0
```

7.10 strptl Command

[Name]

strptl - Starting the standby patrol

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/strptl -n devicename1[,devicename2,...]
```

[Feature description]

The strptl command starts the standby patrol in NIC switching mode.

[Option]

You can specify the following option:

-n devicename1[,devicename2,...]

Specify the name of a virtual interface of the standby patrol to be started. You can specify more than one virtual interface by listing them delimited with a comma (.).

[Related commands]

stpctl

[Notes]

The standby patrol is automatically started when the system is started up. Use this command to start the standby patrol manually after the system is started up.

[Examples]

The following shows an example of starting the standby patrol defined in a virtual interface (sha4).

```
# /opt/FJShanet/usr/sbin/strptl -n sha4
```

7.11 stpctl Command

[Name]

stpctl - Stopping the standby patrol

[Synopsis]

```
/opt/FJShanet/usr/sbin/stpctl -n devicename1[,devicename2,...]
```

[Feature description]

The stpctl command stops the standby patrol in NIC switching mode.

[Option]

You can specify the following option:

-n devicename1[,devicename2,...]

Specify the name of a virtual interface of the standby patrol to be stopped. You can specify more than one virtual interface by listing them delimited with a comma (.).

[Related commands]

strptl

[Notes]

The standby patrol is automatically stopped when the system is shut down. Use this command to stop the standby patrol manually after the system is started up.

[Examples]

The following shows an example of stopping the standby patrol defined in a virtual interface (sha4).

```
# /opt/FJShanet/usr/sbin/stpctl -n sha4
```

7.12 hanetbackup Command

[Name]

hanetbackup - Backing up the environment definition files

[Synopsis]

```
/opt/FJShanet/usr/sbin/hanetbackup [-d backupdir]
```

[Feature description]

The hanetbackup command backs up the environment definition files used by Redundant Line Control function. The backup files are named "hanetYYYYMMDD.bk". YYYYMMDD is the information obtained when the command is executed (YYYY, MM, and DD stands for the year, month and day, respectively).

[Option]

You can specify the following option:

-d backupdir

Specify a directory to which backup environment definition files should be saved. If this option is omitted, the backup files will be saved to under /tmp.

[Related commands]

hanetrestore

[Notes]

If the backup command is executed more than once on the same day using the same output destination, the backup file will be overwritten. Before executing this command, save as required the file that has been output using this command.

[Examples]

The following shows an example of outputting environment definition files to under /tmp.

```
# /opt/FJShanet/usr/sbin/hanetbackup
```

7.13 hanetrestore Command

[Name]

hanetrestore - Restoring the environment definition files

[Synopsis]

```
/opt/FJShanet/usr/sbin/hanetrestore -f backupfilename
```

[Feature description]

The hanetrestore command restores the environment definition files used by Redundant Line Control function.

[Option]

You can specify the following options:

-f backupfilename

Specify a file created using the backup command.

[Related commands]

hanetbackup

[Notes]

- After executing this command, be sure to reboot the system.

- Do not execute this command when the environment setting is completed. If executed, there is a possibility that a conflict will occur in the definition information, which makes it not possible to work properly. In this case, delete the definition information by a `resethanet` command and set the environment again. See "[7.15 resethanet Command](#)" for the detail of a `resethanet` command.
- The supported environment files for restoring the environment definition files with this command are the packages (FJSVhanet) with version 2.3 or later. The packages (FJSVhanet) prior to version 2.2 are not supported.

[Examples]

The following shows an example of restoring a file (/tmp/hanet20041129.bk) created using the backup command.

```
# /opt/FJSVhanet/usr/sbin/hanetrestore -f /tmp/hanet20041129.bk
```

7.14 hanethvrsc Command

[Name]

hanethvrsc - Sets the information of a virtual interface to register in the cluster resources.

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanethvrsc command [args]
```

[Feature description]

hanethvrsc command makes it possible to create/delete/display the information of a virtual interface to register in the resources of PRIMECLUSTER.

| Command | Process outline | Authority |
|---------|--|------------|
| create | Creates virtual interface information | Super user |
| delete | Deletes virtual interface information | Super user |
| print | Displays virtual interface information | Super user |

(1) create command

Creates the information of a virtual interface to register in the resources of PRIMECLUSTER. The information of a virtual interface is consisted of a logical virtual interface and a take over IP address. It is possible to create up to 64 logical virtual interfaces. A logical number of a logical virtual interface (a number to add after ":") is automatically numbered from 65.

The following is the command format for creating a virtual interface information:

- When creating a virtual interface information

```
Fast switching mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename -i {takeover-ipv4
| takeover-ipv6/prefix | takeover-ipv4,takeover-ipv6/prefix}
NIC switching mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename
GS/SURE linkage mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename [-i takeover-ipv4]
```

-n devicename:

Specify a name of the virtual interface for Fast switching, NIC switching or GS/SURE linkage mode created with `hanetconfig` command. A multiple take over IP address can be applied to a single virtual interface name for Fast switching mode. For NIC switching mode and GS/SURE linkage mode (operation mode 'c'), one take over IP address can be applied against one virtual interface name.

-i takeover-ipv4[,takeover-ipv6/prefix]:

Specifies a host name used as a take over IP address or an IP address. The host name that can be specified is within 16 characters. This option is necessary when a virtual interface to specify by -n option is Fast switching mode. Not necessary when NIC switching mode. In NIC switching mode, a value specified by -i option of hanetconfig create command is automatically set as a take over IP address. In GS/SURE linkage mode (operation mode 'c'), this option is omissible. When it omits, IP address set as virtual interface is automatically set up as take over IP address.

(2) delete command

Deletes the information of a virtual interface from the cluster resources.

```
/opt/FJSVhanet/usr/sbin/hanethvrsc delete -n  
{devicename1[,devicename2,...] | all}
```

-n devicename:

Specifies a name of a logical virtual interface created by create command (shaXX:YY). However, it is not possible to delete while RMS is working.

(3) print command

Displays a list of the information of a virtual interface to register in the cluster resources.

```
/opt/FJSVhanet/usr/sbin/hanethvrsc print [-n devicename1[,devicename2,...]]
```

An example of a display is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print  
ifname      takeover-ipv4      takeover-ipv6  
+-----+-----+-----+  
sha1:65     takeover-ip1       -  
sha2:65     -                   takeover-ip2  
sha3:65     192.13.70.1        fec0:1::123/64
```

| Item | Explanation |
|---------------|---|
| ifname | A name of a logical virtual interface to register in the cluster resources is displayed. |
| takeover-ipv4 | A host name or an IP address of a take over IP address (IPv4) to add to a logical virtual interface is displayed. |
| takeover-ipv6 | A host name or an IP address of a take over IP address (IPv6) to add to a logical virtual interface is displayed. |
| '-'(hyphen) | Means that neither a hostname nor an IP address is set. |

[Notes]

- When specified a host name to where to set a host name or an IP address with this command, it is not possible to change/delete the corresponding host name on the host database of such as /etc/inet/hosts and /etc/inet/ipnodes files. To change/delete the information of the host name, it is necessary to temporarily delete a definition of a Redundant Line Control function to use the corresponding host name and to set the definition again.
- When creating information of a virtual interface to be registered in the resources of PRIMECLUSTER by using this command, check that the virtual interface to be registered is deactivated before execution.

[Examples]

(1) create command

An example of using create command when setting Fast switching mode (IPv4):

An example of using create command when registering a virtual interface sha0 added a take over IP address (10.1.1.1) in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 10.1.1.1
```

An example of configuring Fast switching mode (IPv6):

The following is an example of registering the virtual interface sha0 in the cluster resource after applying the take over IP address (fec0:1::1/64).

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

An example of configuring Fast switching mode (IPv4/IPv6):

The following is an example of registering the virtual interface sha0 in the cluster resource after applying IPv4 take over IP address (10.1.1.1) and IPv6 take over IP address (fec0:1::1/64).

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 10.1.1.1,fec0:1::1/64
```

An example of using create command when setting NIC switching mode:

An example of using create command when registering a virtual interface sha1 in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

An example of configuring GS/SURE linkage mode:

The following is an example of registering the virtual interface sha1 in the cluster resource.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1 -i 192.168.80.10
```

(2) delete command

An example of using create command when deleting a logical virtual interface sha1:65 from the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n sha1:65
```

(3) print command

An example of displaying a list of the information of a virtual interface to register to the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
```

7.15 resethanet Command

[Name]

resethanet - Initializes the information of virtual interface configuration and reactivates a Redundant Line Control function.

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/resethanet -i | -s
```

[Feature description]

resethanet commands initializes the information of virtual interface configuration and reactivates a Redundant Line Control function. The initialized configuration information is as follows.

- The information of virtual interface configuration (the definition information set by hanetconfig command)
- The monitor-to information (the definition information set by hanetpoll command)

The parameters set by hanetpoll on command, hanetparam command, and hanetobserv command are not initialized.

[Option]

Specify the following options:

-i:

Specify to initialize the information of virtual interface configuration. Do not specify this option except to stop using a Redundant Line Control function during the operation, or to recreate the information of virtual interface configuration.

-s:

Specify to reactivate a Redundant Line Control function. This option validates changed content of the setting without rebooting a system when changed the information of virtual interface configuration.

(1) Initializing the configuration information

Initialize the configuration information of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/resethanet -i
```

-i:

Initializes the configuration information of a virtual interface and makes it the status of no definition. However, if even one virtual interface is registered as cluster resources in the corresponding system, it is not possible to initialize.

(2) Reactivating a Redundant Line Control function

Reactivates a Redundant Line Control function.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

-s:

Reactivates a Redundant Line Control function. However, if RMS is activated at PRIMECLUSTER operation in a corresponding system, it is not possible to reactivate.

[Notes]

- When the configuration information is initialized with the command, it cannot be returned to the original state prior to initialization. Users are recommended to save the information using the hanetbackup command.
- If the shared-IP zone is using the virtual interface, stop the zone then change the network setting before initializing the virtual interface configuration.
- When you execute this command, please stop RMS beforehand.

[Examples]

The following is an example of initialize the configuration information of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/resethanet -i
```

The following is an example of reactivates a Redundant Line Control Function.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

7.16 hanetgw Command

[Name]

hanetgw - Setting, deleting, and displaying a virtual gateway configuration definition of GS/SURE linkage mode.

[Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetgw command [args]
```

[Feature description]

The hanetgw command creates/deletes/displays the virtual gateway required for operating in GS/SURE linkage mode. The virtual gateway is used to communicate in GS/SURE linkage mode. By creating the virtual gateway, the virtual IP address is automatically selected as the local IP address which is used for communication. Moreover, the host route through the virtual gateway for the communication target is automatically registered when a virtual interface is activated.

| Command | Process outline | Authority |
|---------|------------------------------------|--------------|
| create | Creates configuration information | Super user |
| delete | Deletes configuration information | Super user |
| print | Displays configuration information | General user |

(1) create command

Set the virtual gateway address for the virtual interface in GS/SURE linkage mode.

The command format for setting the virtual gateway is as follows.

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n devicename -g gwaddr
```

-n devicename

Specify the virtual interface in GS/SURE linkage mode.

-g gwaddr

Specify the host name or IP address for the virtual gateway information. This host name or IP address should be associated with an IP address in a network database including the /etc/hosts file.

(2) delete command

Use the delete command to delete the virtual gateway information. The command format is as follows.

```
/opt/FJSVhanet/usr/sbin/hanetgw delete -n {devicename1[,devicename2,...] | all}
```

-n devicename1[,devicename2,...]

Specify the name of the virtual interface whose information you want to delete.

-n all

Delete all the defined virtual gateway information.

(3) print command

Displays the contents of the settings for the virtual gateway information. The command format for displaying the virtual gateway information is as follows.

```
/opt/FJSVhanet/usr/sbin/hanetgw print [-n devicename1[,devicename2,...]]
```

Shown below is an example of the displayed virtual gateway information.

```
# /opt/FJSVhanet/usr/sbin/hanetgw print
ifname  GW Address
+-----+-----+
sha0    192.168.80.254
sha10   192.168.90.254
```

| Display | Contents |
|------------|---|
| ifname | Virtual interface on which the virtual gateway is set |
| GW Address | Host name or IP address set for the virtual gateway |

[Notes]

- When you set the virtual gateway information, if you specify a subnet different from the network address information for the virtual interface in GS/SURE linkage mode, communication may not be possible. Be sure to specify the same network address information as the one for the virtual interface in GS/SURE linkage mode.
- If specification of the virtual gateway is omitted, communication using GS/SURE linkage mode is not available on applications. Specify the virtual IP address for the local the local IP address by using the bind function or others.

[Examples]

(1) create command

Shown below is an example of setting the virtual gateway information.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n sha0 --g 192.168.80.254
```

(2) delete command

Shown below is an example of deleting the virtual gateway information.

```
# /opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0
```

Appendix A Messages and corrective actions

This appendix outlines messages and corrective actions to be taken to eliminate errors.

A.1 Messages Displayed by Redundant Line Control function

This section explains the meaning of, and action to take for each message output by Redundant Line Control function regarding such commands as the configuration commands and operation commands.

Each message has the following format:

[Output message]

1. A format for information messages and error output messages:

```
hanet: BBBCC: DDDDD: EEEEE FFFFF
(1)   (3)   (4)   (5)   (6)
```

2. A format for console output messages and internal information output messages:

```
hanet: AAAAA: BBBCC DDDDD: EEEEE FFFFF
(1)   (2)   (3)   (4)   (5)   (6)
```

(1) Component name

Always begins with "hanet".

(2) Error Kind

Included in the console messages and internal information. AAAAA provides the following information:

ERROR:

Error message

WARNING:

Warning message

INFO:

Information message. It is only output when syslog ("[3.2.3 syslog setup](#)") is set.

TRACE:

Internal information

(3) Message number (Displayed in total five digits.)

Outputs an output message with a unique number. Not displayed when output an internal message.

The first three digits (BBB) indicate the message number.

The last two digits (CC) indicate the internal code.

(4) Outline of errors

The output information (DDDDD) is as follows. Not output when it is a console message.

information:

Means that an output message is the information.

warning:

Means that there is an error in the definition information (a process continues).

operation error:

Means that the executed command method has an error.

configuration error:

Means that there is an error in the definition information.

internal error:

Means that there is a fatal error.

(5) Error details

Message may be output as required.

(6) Others

The complimentary information (FFFFF) is occasionally output if necessary.

A.1.1 Information message (number 0)

| Message number | Message | Meaning | Action |
|----------------|-------------|--|--------|
| 000 | normal end. | Execution of the command was successfully completed. | None |

A.1.2 Error output message (numbers 100 to 500)

The meaning of and response to each message output by Redundant Line Control function is listed below.

Table A.1 Message number 1xx, 2xx

| Message number | Message | Meaning | Action |
|----------------|---|--|--|
| 101 | command can be executed only with super-user. | Only a super-user can execute this command. | Please perform by a super-user authority. |
| 102 | this interface is already linked. | The specified virtual device has already been activated. | Execute the dsphanet command to make sure that the virtual interface is in the activated status. |
| 105 | invalid ip_address. | An invalid IP address is specified. | Specify the correct IP address for re-execution. |
| 111 | invalid parameter. | An invalid parameter is specified. | Read the appropriate command reference, and execute the command again. |
| 112 | invalid argument. | An invalid command argument was found. | Read the appropriate command reference, and execute the command again. |
| 114 | -r option value is invalid. | An invalid value is specified. | Read the appropriate command reference to get the correct value, and execute the command again. |
| 115 | -s -c option total value is invalid. | An invalid value is specified. | Specify the values (-s and -c) so that the product of the two values does not exceed 300, and execute the command again. |
| 116 | -s -c option value is invalid. | An invalid value is specified. | The values (-s and -c) must be selected from within a range of 1 to 300. Specify a number |

| Message number | Message | Meaning | Action |
|----------------|---------------------------------|---|--|
| | | | within the range for each value, and execute the command again. |
| 118 | interface is inactive. | The specified virtual interface has been deactivated. | Execute the dsphanet command to check the status of the specified virtual interface. |
| 119 | interface is active. | The specified virtual interface has been activated. | Execute the dsphanet command to check the status of the specified virtual interface. |
| 120 | invalid device name. | An invalid virtual interface name is specified. | Specify the correct virtual interface name, and execute the command again. |
| 121 | directory not found. | The specified directory was not found. | Specify a directory name that already exists, and execute the command again. |
| 122 | backup file not found. | The specified backup file was not found. | Specify a backup file that already exists, and execute the command again. |
| 123 | invalid backup file. | The specified backup file is invalid. | Specify the backup file that was created by the hanetbackup command, and execute the command again. |
| 124 | not directory | Directory name was not found where directory was expected. | Specify a directory, and execute the command again. |
| 125 | interface is Cluster interface. | The specified interface is available in the cluster operation. | Specify an interface that is not being used in the cluster operation, and execute the command again. |
| 126 | shared resource is not found. | An invalid common resource is specified. | Specify a correct common resource name, and execute the command again. |
| 127 | invalid key | An invalid resource key is specified. | Specify a correct resource key, and execute the command again. |
| 128 | invalid logicalIP. | An invalid logical IP address is specified. | Specify a correct logical IP address, and execute the command again. |
| 129 | logicalIP is already defined. | The specified logical IP address has been specified in configuration information. | Specify a different logical IP address, and execute the command again. |
| 130 | logicalIP is not specified. | No logical IP address is specified. | Specify a logical IP address, and execute the command again. |
| 131 | primaryIF is not specified. | No primary interface is specified. | Specify a primary interface, and execute the command again. |
| 132 | invalid primaryIF. | An invalid primary interface is specified. | Specify a correct primary interface, and execute the command again. |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| 133 | physicalIP is not specified. | No physical IP address is specified for the interface. | Specify a physical IP address for the interface, and execute the command again. |
| 134 | invalid physicalIP. | The physical IP address of the interface is invalid. | Specify a correct physical IP address, and execute the command again. |
| 135 | primary polling address is not specified. | No monitoring destination IP address is specified for the primary interface. | Specify a monitoring destination IP address for the primary interface, and execute the command again. |
| 136 | invalid primary polling address. | The monitoring destination IP address of the primary interface is invalid. | Specify a correct monitoring destination IP address, and execute the command again. |
| 137 | secondaryIF is not specified. | No secondary interface is specified. | Specify a secondary interface, and execute the command again. |
| 138 | invalid secondaryIF. | An invalid secondary interface is specified. | Specify a correct secondary interface, and execute the command again. |
| 139 | secondary polling address is not specified. | No monitoring destination IP address of the secondary interface is specified. | Specify a monitoring destination IP address of the secondary interface, and execute the command again. |
| 140 | invalid secondary polling address. | An invalid monitoring destination IP address is specified for the secondary interface. | Specify a correct monitoring destination IP address for the secondary interface, and execute the command again. |
| 141 | HUB-HUB polling flag is not specified. | Whether HUB-to-HUB communication monitoring is performed is not specified. | Specify whether to perform the HUB-to-HUB communication monitoring (ON or OFF), and execute the command again. |
| 142 | invalid HUB-HUB polling flag. | There is an error in the specification indicating whether HUB-to-HUB communication monitoring is performed. | Specify ON or OFF of the HUB-to-HUB communication monitoring, and execute the command again. |
| 143 | logicalIP is defined in physicalIP. | The IP address specified as a logical IP address overlaps the physical IP address. | Specify an IP address that is not specified in the virtual interface as the logical IP address, and execute the command again. |
| 144 | secondaryIF equal primaryIF. | The primary interface and the secondary interface are identical. | Specify different interfaces, and execute the command again. |
| 145 | interface is already defined in another set. | The specified interface is used in another operation set. | Specify an interface that is not used in other operation sets, and execute the command again. |
| 146 | interval is not specified. | No monitoring interval is specified. | Specify a monitoring interval, and execute the command again. |

| Message number | Message | Meaning | Action |
|----------------|---|--|---|
| 147 | invalid interval specified. | The monitoring interval value is invalid. | Specify a correct monitoring interval, and execute the command again. |
| 148 | count is not specified. | No monitoring count is specified. | Specify a monitoring count, and execute the command again. |
| 149 | invalid count specified. | The monitoring count value is invalid. | Specify a correct monitoring count, and execute the command again. |
| 150 | invalid argument. | An invalid option is specified. | Refer to the command reference, and execute the command again. |
| 151 | logicalIP is active. | The specified processing could not be performed because the transfer path monitoring of the specified operation set was operating. | Stop the transfer path monitoring, and execute the command again. |
| 152 | logicalIP is inactive. | The specified processing could not be performed because the transfer path monitoring of the specified operation set was stopped. | Start the transfer path monitoring, and execute the command again. |
| 153 | logicalIP is not defined. | The specified operation set is not defined. | Specify a correct operation set. |
| 154 | logicalIP is registered to cluster resource. | The specified operation set is registered as a cluster resource. | Delete the operation set from the cluster resources. |
| 155 | invalid ping on/off. | HUB-to-HUB communication monitoring information specified in the operation set information is invalid. | Specify correct operation set information. |
| 156 | secondaryIF is not defined. | Because the secondary interface is not specified, interfaces cannot be switched. | Specify an operation set in which the secondary interface is defined. |
| 157 | product of interval and time should be less than 300. | The detection time (product of the monitoring interval and monitoring count) of line failure is too large. | Specify the monitoring interval and monitoring count so that their product does not exceed 300 seconds. |
| 158 | invalid interface count(max 32) | The maximum number of real interfaces that a virtual interface can bundle in GS/SURE linkage mode is exceeded (maximum 32). | Reduce the number of bundled real interfaces, and execute the command again. |
| 159 | MAC address is already defined. | The specified MAC address has already been specified. | Specify a different MAC address, and execute the command again. |
| 160 | specified devicename could not support cluster. | The specified device does not support cluster operation. | Specify an interface name that support cluster operation, and execute the command again. |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| 161 | polling function is defined. | The monitoring function is specified. | Delete a monitoring function with the name of the corresponding virtual interface, and execute again. |
| 162 | invalid MAC address. | An invalid MAC address is specified. | Specify a correct MAC address, and execute the command again. |
| 163 | IP address or Hostname is already defined. | The specified IP address or host name has already been specified. | Specify a different IP address or host name, and execute the command again. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 169, 170 |
| 164 | interface name is already defined. | The specified interface name has already been specified. | Specify a different interface, and execute the command again. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 166 |
| 165 | invalid interface name. | An invalid interface name is specified. | Specify a correct interface name, and execute the command again. When the virtual interface is registered in cluster resource, please execute it again after stopping RMS. |
| 166 | invalid mode. | A virtual interface configured with invalid operation mode or incompatible operation mode was specified. | Specify a virtual interface configured with valid operation mode or compatible operation mode. |
| 167 | parent device name not found. | No virtual interface corresponding to the logical virtual interface was found. | Specify a correct logical virtual interface, and execute the command again. |
| 168 | invalid hostname. | Specified host name or defined host name does not exist in /etc/inet/hostsfile or /etc/inet/ipnodes file. Or, specified host name is invalid. | Check for the existing host name specified in the command argument or hostname specified in configuration settings for Redundant Line Control function, in /etc/inet/hosts or /etc/inet/ipnodes file. If the host name does not exist, create one and try again. If the host name exists in these files, check if the name contains characters other than alphanumeric characters, hyphen, and period. Also make sure it does not use non- |

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| | | | alphanumeric characters for the first and last character. If it contains these characters, change the name and re-execute the command. |
| 169 | physical interface name is already defined. | The specified physical interface name has already been specified. | Specify a different physical interface name, and execute the command again. This message may also be output if the specified physical interface is shared with another virtual interface when changing the configuration definition. In this case, delete another virtual interface in advance, or specify another physical interface that is not shared with another virtual interface. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 166 |
| 170 | invalid physical interface name. | An invalid physical interface name is specified. | Specify the correct name of the physical interface (the name of the virtual interface when the mode is "p" or "q"), and execute again. When setting a standby patrol function, check that two physical interfaces are defined that configure a virtual interface to be monitored. In addition, when a problem cannot be solved by this action, please perform the same action as the following messages. A problem may be solved. Message number: 164 |
| 171 | trunking interface list is not specified. | No interface that operates in trunking mode is specified. | Specify an interface, and execute the command again. |
| 172 | mode p interface is defined. | A virtual interface in mode P is specified. | Delete the interface in mode P, and execute the command again. |
| 173 | mode c interface is activated. | An interface in mode C is activated. | Inactivate the interface in mode C, and execute the command again. |
| 174 | ifname is not defined in hanetconfig. | The specified virtual interface name is not specified in configuration information. | Create configuration information using the hanetconfig command, and execute the command again. |

| Message number | Message | Meaning | Action |
|----------------|--|---|---|
| 175 | same polling addresses are specified. | Primary and Secondary interfaces specified the same monitor-to address. | Specify different monitoring destinations, and execute the command again. |
| 176 | polling target is not alive. | No response is received from the monitoring destination. | Check the monitoring destination, and execute the command again. |
| 177 | polling is active. | The monitoring function is operating. | Stop (OFF) the monitoring function using the hanetpoll command, and execute the command again. |
| 178 | invalid version. | An incorrect version is specified. | Specify the version of the backed up Redundant Line Control function, and execute the command again. |
| 179 | invalid virtual interface count(max 64). | The number of virtual interfaces of the communication target exceeded the maximum number (maximum 64). | Delete unnecessary definitions, and execute the command again. |
| 180 | mode q interface is defined. | An invalid option is specified. | Deactivate an interface of mode q and execute again. |
| 181 | invalid client count(max 128). | An invalid option is specified. | Execute the command again with a correct value. |
| 182 | -p option value is invalid. | An invalid option is specified. | See the command reference and execute the command again with a correct value. |
| 183 | -b option value is invalid. | An invalid option is specified. | See the command reference and execute the command again with a correct value. |
| 184 | shared resource can not be specified. | An invalid option is specified. | See the command reference and execute the command again with a correct value. |
| 185 | function is already defined by another. | An invalid option is specified. | Check the configuration information again, delete unnecessary definitions, and execute again. |
| 186 | could not get information. | Communication between command-daemon failed. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 187 | could not delete last 1 NIC. | It is not possible to delete if a using actual interface is only one when deleting dynamically an actual interface. | After stopped a virtual interface to process, delete or change the specified actual interface. When changing a definition of a virtual interface, delete or change a definition with hanetconfig command. |
| 188 | number of physical interface is already maximum. | The number of the physical interfaces that configures the specified virtual interface has | Review the number of the physical interfaces that configures a virtual interface, |

| Message number | Message | Meaning | Action |
|----------------|--|--|---|
| | | reached the maximum number possible to bundle. Therefore, it is not possible to add an actual interface dynamically. | and change a definition using a hanetconfig command if necessary. |
| 189 | invalid network address. | The specified network address is invalid. | Check if or not the specified network address matches with that of a virtual interface network using hanetconfig print command. Specify a correct network address again. |
| 190 | virtual gateway function is defined. | A virtual gateway function is already set. | Delete a virtual gateway function with the name of the corresponding virtual interface, then execute again. |
| 191 | StandbyIP address function is defined. | A function to specify a standby IP address is already set. | Delete a function to specify a standby IP address with the name of the corresponding virtual interface, and execute again. |
| 192 | resource monitor process for virtual interface is running. | A resource monitor for the virtual interface is working. | Execute hvshut command provided by a cluster system, halt a resource monitor, and execute again. |
| 193 | Specified interface is already linked to IP. | The IP address is already assigned to the specified interface. | Check if or not there is /etc/hostname.interface file. If exists, change a name or delete it. After executed "/usr/sbin/ifconfig interface name unplumb" command, execute the command again. |
| 194 | Specified interface is not bundled by a virtual interface. | The specified interface is not defined as the one to configure a virtual interface. | Check the interface that configures a virtual interface using hanetconfig print command. Specify an interface name displayed in the Interface List, and execute the command again. In addition, when you add the interface which does not exist on a definition, please specify "-f" option of the hanetnic add command, and execute the command again. |
| 195 | Standby patrol function could not started. | It is not possible to execute a standby patrol function. | Check that the system has already recognized all physical interfaces that configure a virtual interface to be monitored by a standby patrol function, and execute again. |
| 196 | Standby patrol function is defined. | A standby patrol function is already set. | Delete a standby patrol function of the corresponding virtual interface name, and execute again. |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| 197 | specified physical interface is already unlinked. | Activation of the specified physical interface is already deleted. | Using dsphanet command, check that the specified physical interface is not used yet. |
| 198 | address family of take over IP address incompatible. | The specified address form of a take over IP address (an address family) is not compatible with that of a setting virtual interface. | Make an address form of a take over IP address compatible with that of a setting virtual interface and execute again. |
| 199 | invalid take over IP address. | The specified take over IP address is invalid. | Check a value of the specified take over IP address and execute again. |
| 200 | invalid hostname or prefix value. | The specified host name or prefix value is invalid. | Check the specified host name or prefix value and execute again. |
| 201 | dual stack interface can not be specified. | It is not possible to specify a virtual interface of dual stack configuration. | Delete a definition of the corresponding virtual interface and define newly. |
| 202 | address family of polling IP address incompatible. | The specified address form of a monitor-to IP address (an address family) is not compatible with that of a setting virtual interface. | Make an address form of a monitor-to IP address compatible with that of a setting virtual interface and execute again. |
| 203 | interfaces defined as cluster resources still exist. | One or more virtual interfaces registered as cluster resources exist. | Delete the cluster resources and execute the command again. |
| 204 | interface defined as cluster resource is still active. | A virtual interface is active as cluster resources. | Stop RMS and execute again. |
| 205 | mode can't be changed for dual stack interface. | Mode can't be changed if the virtual IF is a dual stack. | Temporary delete the configuration information of the virtual interface and reconfigure. |
| 206 | mode can't be changed for IPv6 interface. | Mode cannot be changed if the virtual IF is IPv6. | Temporary delete the configuration information of the virtual interface and reconfigure. |
| 207 | order of physical interface is different or invalid physical interface name. | Order of the interfaces is incorrect or the name of the interface is invalid. | Check the contents of the interface and retry. |
| 208 | configuration is not defined. | Valid configuration information or monitoring target's information is not configured. | Configure the valid configuration information or monitoring target's information. |
| 209 | specified address family is not defined. | The specified address type (address family) of the virtual interface is undefined. | Ensure the specified address matches the address format of configured virtual interface. |
| 210 | invalid address family. | The specified address type (address family) does not match the address type of the virtual interface. | Ensure the specified address matches the address format of configured virtual interface. |

| Message number | Message | Meaning | Action |
|----------------|---|--|---|
| 211 | invalid MAC address(multicast or broadcast). | The specified MAC address is invalid. | Specify a MAC address other than a multicast address or broadcast address. |
| 212 | polling attribute of specified devicename cannot be changed individually. | The monitoring information of the virtual interface cannot be changed individually. | Specify the monitoring configuration value as changeable virtual interface that can be specified individually. |
| 213 | invalid interface name.(same physical interface) | Tagged VLAN interface created on the same physical interface was specified over the same physical interface. | Check the specified operation mode and tagged VLAN name. Then, retry the operation. |
| 214 | invalid interface name.(VLAN-ID is the same) | Identical logical device number of tagged VLAN interface is assigned. | Check the specified operation mode and tagged VLAN name. Then, retry the operation. |
| 215 | invalid interface name.(VLAN-ID different) | Disparate logical device number of tagged VLAN interface is assigned. | Check the specified operation mode and tagged VLAN name. Then, retry the operation. |
| 216 | When polling address is one, HUB-HUB polling flag must be OFF. | When polling address is one, HUB-HUB polling flag must be set OFF. | Set two polling targets or set the flag OFF, then retry the operation. |
| 217 | specified physical interface is inactive. | The specified physical interface is inactive. | Ensure the hostname configuration file (/etc/hostname.interface) for the physical interface exists. If it does no exist, create a new configuration file including physical IP address or hostname and then reboot the system After rebooting the system, execute the command. If the above file exists, run the following command: /usr/sbin/ifconfig [interface name] plumb [physical IP address] netmask + broadcast + up Then, execute the command again. |
| 218 | bundled interface does not exist. | A virtual interface bundling physical interface does not exist or a tagged VLAN interface does not exist. | Ensure virtual interface bundling physical interface or a tagged VLAN interface exists. Then re-execute the command. |
| 219 | invalid interface name.(physical interface is overlapped) | Specified Tagged VLAN interface is overlapped with part of physical interface or Tagged VLAN interfaces which belongs other virtual interface. | Specify un-overlapped or completely corresponding Tagged VLAN interfaces with other virtual interface. |
| 220 | interface is used in zones. | The virtual interface is used in the non-global zone. | Stop the non-global zone then execute the command again. |

| Message number | Message | Meaning | Action |
|----------------|--|---|---|
| 221 | failed to inactivate virtual interface. | Deactivation of the virtual interface failed. | Stop the non-global zone then execute the command again. If the symptom still remains the same, collect troubleshooting information of the redundant line control then contact field engineers. |
| 222 | invalid interface name.(unusable combination) | The physical interface name specified is invalid. | Check that the tagged VLAN interface is unmixed with the physical interface then execute the command again. |
| 223 | failed to activate interface. | Failed to activate a interface. | Activation of the interface failed because the same IP address was specified more than once or system resources are insufficient. Check the interface by executing the /usr/sbin/ifconfig command. If the symptom still remains the same, collect troubleshooting information of the redundant line control then contact field engineers. |
| 224 | operation error: operation is not supported in this environment. | Virtual interfaces in the specified mode are not supported In non-global zones. | Virtual interfaces other than the NIC switching mode are not supported in non-global zones. Review the configuration information. |

Table A.2 Message number 3xx

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| 301 | could not open configuration file. | Failed to open the configuration information file. | Check whether the creation of configuration information has been completed. |
| 302 | invalid interface name. | An invalid virtual interface name was found in configuration information. | Review the configuration information. |
| 303 | hostname is not specified. | The host name is not specified in the configuration information. | Review the configuration information. |
| 304 | invalid hostname. | An invalid host name is specified in configuration information. | Review the configuration information. |
| 305 | trunking interface list is not specified. | The bundled physical interface is not specified in configuration information. | Review the configuration information. |
| 306 | invalid interface count(max 8). | The number of physical interfaces to be bundled exceeds the preset value. | Specify 8 or fewer physical interfaces as the number of interfaces to be bundled. |
| 307 | interface name is already defined. | The virtual interface name you want to specify has already | Specify a virtual interface so that it does not conflict with the |

| Message number | Message | Meaning | Action |
|----------------|---|--|---|
| | | been defined in the configuration information. | other interfaces in the configuration information, and execute the command again. |
| 308 | physical interface name is already defined. | The physical interface name that you want to bundle in a virtual interface has already defined. | Review the configuration information. |
| 309 | interface address is already defined. | The same IP address is specified for more than one virtual interface. | Review the configuration information. |
| 310 | invalid physical interface name. | An invalid physical interface name is specified in the configuration information. | Review the configuration information. |
| 311 | invalid file format. | An invalid file format was found in configuration information. | Execute the check command for the configuration information, and take the appropriate action according to the output message. |
| 312 | parent device name not found. | The configuration information does not contain the virtual interface with the logical virtual interface. | Review the configuration information. |
| 313 | invalid mode. | An invalid operation mode is specified in the configuration information. | Review the configuration information. |
| 314 | target is not defined. | The destination information for monitoring does not contain the address information of the monitoring destination. | Review the destination information for monitoring. |
| 315 | polling device is already defined. | The destination information for monitoring contains multiple specification entries with the same virtual interface name. | Review the destination information for monitoring. |
| 316 | same polling addresses are specified. | Primary/Secondary interfaces specified the same monitor-to address. | Review the destination information for monitoring. |
| 317 | interface name is not defined. | The virtual interface name is not specified in the destination information for monitoring. | Review the destination information for monitoring. |
| 318 | invalid device count(max 64). | The number of specified virtual interfaces exceeds 64. | Review the configuration information or destination information for monitoring. |
| 319 | Invalid logical device count(max 63). | The number of specified logical virtual interfaces exceeds 63 (i.e., the maximum number for one virtual interface). | Review the configuration information. |

| Message number | Message | Meaning | Action |
|----------------|--------------------------------------|--|--|
| 320 | Configuration is invalid. | The configuration information contains invalid data. | Review the configuration information. |
| 321 | Configuration is not defined. | Failed to find valid configuration information or destination information for monitoring. | Define the settings for the configuration information or destination information for monitoring. |
| 322 | invalid define count(max 64). | The total of defined virtual interfaces and defined logical virtual interfaces exceeds 64 (i.e., the maximum number for definition). | Review the configuration information. |
| 323 | LogicalIP is already max. | The number of logical IP addresses exceeded the maximum defined number. | Review the configuration information. |
| 324 | current configuration is invalid. | No operation set can be created because the definition of the created operation set contains invalid information. | Review the operation set information. |
| 325 | invalid ping on/off. | ON/OFF information for monitoring is not specified in the operation set information. | Review the operation set information. |
| 326 | invalid logicalIP. | The logical IP address is invalid. | Review the configuration information. |
| 327 | LogicalIP is already defined. | The logical IP address has already been specified. | Review the configuration information. |
| 328 | logicalIP not found. | The logical IP address was not found. | Review the configuration information. |
| 329 | primaryIF not found. | The primary interface was not found. | Review the configuration information. |
| 330 | invalid primaryIF. | The primary interface is invalid. | Review the configuration information. |
| 331 | physicalIP not found. | The physical IP address was not found. | Review the configuration information. |
| 332 | invalid physicalIP. | The physical IP address is invalid. | Review the configuration information. |
| 333 | primary polling address not found. | No monitoring destination address of the primary interface was found. | Review the monitoring destination information and configuration information. |
| 334 | invalid primary polling address. | The monitoring destination address of the primary interface is invalid. | Review the monitoring destination information and configuration information. |
| 335 | invalid secondaryIF. | The secondary interface is invalid. | Review the configuration information. |
| 336 | secondary polling address not found. | No monitoring destination address of the secondary interface was found. | Review the monitoring destination information and configuration information. |

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| 337 | invalid secondary polling address. | The monitoring destination address of the secondary interface is invalid. | Review the monitoring destination information and configuration information. |
| 338 | HUB-HUB polling flag not found. | Whether HUB-to-HUB communication monitoring is performed is not specified. | Review the monitoring destination information and configuration information. |
| 339 | logicalIP equal physicalIP. | The same value is specified as the logical IP address and physical IP address. | Review the configuration information. |
| 340 | secondaryIF equal primaryIF. | The same value is specified as the primary interface and secondary interface. | Review the monitoring destination information and configuration information. |
| 341 | interface is already defined in another set. | An interface used in another operation set is specified. | Review the configuration information. |
| 342 | invalid HUB-HUB poll on/off. | There is an error in the specification indicating whether HUB-to-HUB communication monitoring is performed. | Review the monitoring destination information and configuration information. |
| 343 | physicalIP is already defined in another set. | A logical IP address used in another operation set is specified. | Review the configuration information. |
| 344 | polling information is different. | Different information is specified in the operation set sharing a physical interface. | Review the operation set information. |
| 345 | cluster configuration is incomplete. | The transfer path monitoring cannot be started because the cluster system settings are incomplete. | Review the setting of a cluster system, and reboot a machine. |
| 346 | invalid client count. | The number of the clients is improper. | Execute the command again with the correct number of the clients. |
| 347 | client address is already defined. | Already defined the specified client address. | See the client definition information, specify an address not redundant, and execute again. |
| 348 | invalid client address. | The specified client address is improper. | Check the client address and execute the command again. |
| 349 | invalid PmgropeID. | The PM group ID is improper. | Check the PM group ID and execute the command again. |
| 350 | invalid network address. | The specified network address is improper. | Check the network address and execute the command again. |
| 351 | observe information is not defined. | Not yet defined the monitoring item information. | Define the monitoring item information by hanetobserv command. |
| 352 | in.routed is not started. | Not yet activated a routing daemon (in.routed). | Enable svc:/network/routing/route service to activate routing daemon (in.routed). |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| 353 | invalid prefix value | A prefix value is invalid. | Check the specified IP address and prefix value. |
| 354 | interface is specified redundantly. | Redundancy was found in the specified virtual interface. The redundancy will be ignored. | Specify the valid virtual interface and re-execute the command again. |
| 356 | could not get polling information. | Failed to obtain polling information. | Configure the polling information and re-execute the command. If the same error occurs after re-executing the command, then collect appropriate logs for Redundant Line Control function and contact our system engineers with the reported error message. |
| 358 | the same network addresses are inappropriate. | The network addresses assigned between the interfaces cannot be the same network address. | Review the assigned IP address (hostname) and network mask (prefix length). The network addresses between must use different network address. Assign the different network addresses between the interfaces. |
| 360 | take over ip address is not defined. | A take over IP address is not set. | Review the setting of Redundant Line Control function and cluster system. |
| 361 | virtual interface is not defined. | A virtual interface is not set. | Review the setting of Redundant Line Control function and cluster system. |
| 363 | IP address is already defined in zones. | The IP address specified is already set in the non-global zone. | Change the IP address in the non-global zone, or specify a different IP address. |
| 364 | interface name is defined in zones. | The virtual interface specified for the non-global zone is deleted. | Change the interface for the non-global zone. |
| 365 | secondaryIF is specified in zones. | The secondary interface specified is already defined in the non-global zone. | Change the interface for the non-global zone to the primary interface. |
| 374 | mac addresses of physical interfaces are not unique. | The MAC addresses of the primary interface and the secondary interface are the same. | Specify an address other than 0:0:0:0:0 for the MAC address of the standby patrol. |

Table A.3 Message number 5xx

| Message number | Message | Meaning | Action |
|----------------|----------------|---|---|
| 501 | socket() fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. After checked there is no mistake, execute a command |

| Message number | Message | Meaning | Action |
|----------------|----------------------------|---|---|
| | | | again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 502 | ioctl(SIOCGIFCONF) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 510 | could not allocate memory. | An error was found in the internal system call. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 511 | could not open file. | An error was found in the internal system call. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 512 | could not read file. | An error was found in the internal system call. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 513 | could not write file. | An error was found in the internal system call. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line |

| Message number | Message | Meaning | Action |
|----------------|-----------------------------|---|--|
| | | | Control function, and then contact field engineers to report the error message. |
| 514 | open() fail. | An error was found in the internal system call. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 515 | ioctl(SHAIOCSETPARAM) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 516 | ioctl(I_PUNLINK) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 517 | ioctl(SHAIOCGETLID) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 518 | ioctl(I_PLINK) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |

| Message number | Message | Meaning | Action |
|----------------|--------------------------------|--|--|
| 519 | ioctl(SHAIOCPLUMB) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 525 | ioctl(SHAIOCGETINFO) fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 538 | total entry is negative value. | An unexpected error occurred during reading configuration information. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 539 | ioctl(SHAIOCNODENAME) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 540 | ioctl(SHAIOCIPADDR) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then |

| Message number | Message | Meaning | Action |
|----------------|-----------------------------|---|--|
| | | | contact field engineers to report the error message. |
| 541 | ioctl(SHAIOSAP) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 542 | ioctl(SHAIOCDEBUG) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 543 | ioctl(SHAIOCWATCHDOG) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 544 | ioctl(SHAIOCDISCARD) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 545 | ioctl(SHAIOCMESSAGE) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line |

| Message number | Message | Meaning | Action |
|----------------|------------------------------|---|--|
| | | | Control function, and then contact field engineers to report the error message. |
| 546 | unexpected error. | An unexpected system call error occurred. | Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 547 | ioctl(SIOCGIFFLAGS) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 548 | ioctl(SIOCGIFNUM) fail. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 549 | polling process is inactive. | An internal process was not executed. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 550 | opendir failed. | An unexpected system call error occurred. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 551 | semaphore lock failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |

| Message number | Message | Meaning | Action |
|----------------|------------------------------|---|---|
| 552 | semaphore unlock failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 553 | shared memory attach failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 554 | shared memory detach failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 555 | IPC key generate failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 556 | get semaphore failed. | An error was found in the internal system call. | <p>The following system resources are required for Redundant Line Control function:</p> <ul style="list-style-type: none"> * semsys:seminfo_semmni (The maximum number of the semaphore identifiers) : One or greater * semsys:seminfo_semmns (The maximum number of the semaphores in a system) : One or greater <p>If the values are not sufficient, edit the kernel parameter file (/etc/system) and add the required value to the original parameter value.</p> <p>If the problem continues to occur after correcting the kernel parameter values, then there is a possibility that the semaphore identifier for the Redundant Line Control function has already been used by another application. In such case, follow the procedure described bellow to use a different identifier:</p> <pre># cd /opt/FJSVhanet/etc/sbin # mv hanetctld hanetctld.org # cp hanetctld.org hanetctld # shutdown -y -i6 -g0</pre> <p>If the problem still remains even after the identifier has been changed, collect</p> |

| Message number | Message | Meaning | Action |
|----------------|--|---|---|
| | | | examination materials of Redundant Line Control function and contact field engineers. |
| 557 | get shared memory segment identifier failed. | An error was found in the internal system call. | <p>The following system resources are required for Redundant Line Control function:</p> <ul style="list-style-type: none"> * shmsys:shminfo_shmmax (The maximum size of the shared memory segment) : 5120 or greater * shmsys:shminfo_shmmni (The maximum number of the shared memory segments) : two or greater <p>If the values are not sufficient, edit the kernel parameter file (/etc/system) and add the required value to the original parameter value.</p> <p>Additionally, do not specify shmsys:shminfo_shmmin(minimum size of the shared memory segment).</p> <p>If the problem continues to occur after correcting the kernel parameter values, then there is a possibility that the shared memory identifier for the Redundant Line Control function has already been used by another application. In such case, follow the procedure described below to use a different identifier:</p> <pre># cd /opt/FJSVhanet/etc/sbin # mv hanetselect hanetselect.org # cp hanetselect.org hanetselect</pre> <p>If the problem still remains even after the identifier has been changed, collect examination materials of Redundant Line Control function and contact field engineers.</p> |
| 558 | control semaphore failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 559 | internal error. | An internal error occurred. | Collect materials for examination of Redundant Line Control function, and then |

| Message number | Message | Meaning | Action |
|----------------|---------------------------------|---|---|
| | | | contact field engineers to report the error message. |
| 560 | control shared memory failed. | An error was found in the internal system call. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 561 | daemon process does not exist. | An internal error occurred. | If not rebooted after the installation, first reboot, then execute again. There is a possibility that the command of Redundant Line Control function was executed after Redundant Line Control function stops when this message is output at the time of shutting down. Please review the execution timing of the command by the user. If the same message is still output, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 562 | failed to alloc memory. | Failed to acquire memory. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 563 | failed to activate logicalIP. | An internal error occurred. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 564 | failed to inactivate logicalIP. | An internal error occurred. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 565 | ioctl(SHAIOCPATROLL) fail. | An error was found in the internal system call. | Execute the command again. If the same error message is output, contact field engineers to report the error message. |
| 566 | ether_aton() fail. | An error was found in the internal system call. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function, and then |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| | | | contact field engineers to report the error message. |
| 567 | ioctl(SIOCGIFADDR) fail. | An error occurred in the internally used system call. | Check there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute the command again. If the same phenomenon still occurs, collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 568 | ioctl(SIOCGIFNETMASK) fail. | An error occurred in the internally used system call. | Check there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute the command again. If the same phenomenon still occurs, collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 569 | could not communicate with daemon process. | Failed to communicate between a command and a daemon. | Ensure the system is running as multi-user mode. If the system is running as single user mode, change it to multi-user mode and re-execute the command. If this error occurs while running the system as multi-user mode, collect the error logs and contact our system engineer. |
| 570 | failed to get socket. | An error occurred in the internally used system call. | Collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 571 | failed to send request. | An error occurred in the internally used system call. | Collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 572 | failed to receive response. | An error occurred in the internally used system call. | Collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 573 | request timeout. | An error occurred in the internally used system call. | Collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |

| Message number | Message | Meaning | Action |
|----------------|-------------------------------------|---|--|
| 574 | failed to delete virtual interface. | Failed to delete a virtual interface. | Execute the command again. If the same phenomenon still occurs, collect the examination materials of Redundant Line Control function and contact field engineers to report the error message. |
| 575 | failed to restart hanet. | Failed to reactivate the Redundant Line Control function. | Execute the command again. If the same phenomenon still occurs, collect the examination materials of Redundant Line Control function and contact field engineers to report the error message. |
| 576 | failed to enable configuration. | An error has occurred while processing the configured values. | Restart the Redundant Line Control function; (/opt/FJSVhanet/usr/sbin/resethanet -s) and review the reflected configuration values. If the same error occurs after rebooting the system, then collect appropriate logs for Redundant Line Control function and contact our system engineers with the reported error message. |
| 588 | failed to generate mac address. | Failed to automatically generate the MAC address of the standby patrol. | Execute a command again. If the same phenomenon occurs, set the MAC address manually or collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |

A.1.3 Console output messages (numbers 800 to 900)

The following describes the messages output on the console by Redundant Line Control function, explanation, and operator response.

The following table shows facilities and priorities for the message numbers output to the syslog file.

| Facility | Priority | Message number |
|----------|----------|--|
| kern | notice | 800, 801, 990, 991, 992 |
| user | info | 856, 888, 889, 890, 891, 892, 893, 894, 895, 903 |
| user | warning | 805, 814, 823, 832, 902, 924 |
| user | error | other than those above |

Facilities and priorities for the message number 805, 814, and 823 may be output as user.error.

Table A.4 Message number 8xx

| Message number | Message | Meaning | Action |
|----------------|---|--|---|
| 800 | line status changed: Link Down at TRUNKING mode (interface on devicename, target=host_name) | An error occurred in the communication with the remote host system (host_name) using the physical interface (interface) controlled by the virtual interface (devicename) that is operating in the Fast switching mode. | Check whether an error has occurred on the communication path to the remote host system. |
| | line status changed: Link Down at RIP mode (target=host_name) | An error occurred in the communication with the remote host system (host_name). | Check whether an error has occurred on the communication path to the remote host system. |
| 801 | line status changed: Link Up at TRUNKING mode (interface on devicename, target=host_name) | The communication with the remote host system (host_name) using the physical interface (interface) controlled by the virtual interface (devicename) is recovered. | No action is required. |
| | line status changed: Link Up at RIP mode (target=host_name) | The communication with the remote host system (host_name) is recovered. | No action is required. |
| 802 | file open failed. | Failed to open the file. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 803 | file read failed. | Failed to read the file. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 804 | pipe create failed. | Failed to create the internal communication pipe. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 805 | internal error. (cause code) | An internal error occurred. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 806 | cannot get my process id | Failed to obtain the local process ID. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 814 | cannot up interface. | Failed to up the virtual interface. | Collect materials for examination of Redundant Line Control function, and then |

| Message number | Message | Meaning | Action |
|----------------|--------------------------------|---|--|
| | | | contact field engineers to report the error message. |
| 815 | sha device open failed. | Failed to open the "sha" driver. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 816 | ioctl(SHAIOCSETRSCMON) failed. | Failed to send the monitor start request. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 817 | CIOpen failed. | The connection to the cluster failed. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 822 | no data in cluster event. | No data was found in the cluster event. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 823 | CISetStat failed. | The cluster resource status could not be set. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system. |
| 824 | directory open failed. | Failed to open the directory. | Collect materials for examination of Redundant Line Control function, and then |

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| | | | contact field engineers to report the error message. |
| 825 | signal send failed. | Failed to send the signal. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 826 | command can be executed only with super-user. | The execution-time authority is invalid. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 827 | could not allocate memory. | Failed to obtain the memory. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 828 | fork failed. | The fork () failed. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 829 | child process execute failed. | Failed to generate the child process. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 830 | getmsg failed. | Failed to receive the data from the "sha" driver. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 831 | shared library address get failed. | Failed to obtain the shared library address. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 832 | poll failed. | The poll () failed. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 833 | ioctl(SHAIOCSETIPADDR) failed. | Failed to notify the IP address. | Collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 840 | polling device name is not defined in configuration information. polling is not started. ifname=interface(details) | The transmission line monitoring cannot be started because the definition information of the virtual interface is disabled. | The host name that is defined as the IP address of the virtual interface may be deleted from / etc/inet/hosts file. Check the |

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| | | Interface: Interface name details: Error details | defined information of /etc/ inet/hosts file. |
| 845 | could not restart in.routed. | Failed to restart the routing daemon. The router monitoring function is stopped and cluster switching is performed. | Check that there is no mistake in the setting of a system, Redundant Line Control function, and cluster system. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual as to the materials necessary for examining a cluster system. |
| 846 | could not restart in.rdisc. | Failed to restart the router discovery daemon. The router monitoring function is stopped and cluster switching is performed. | Check that there is no mistake in the setting of a system, Redundant Line Control function, and cluster system. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual as to the materials necessary for examining a cluster system. |
| 850 | cannot down interface. | Failed to inactivate the physical interface. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 851 | primary polling failed. lip=logicalIP, target=pollip. | An error of path to the primary monitoring destination was detected in the initial check of the physical interface. LogicalIP: Logical IP Pollip: Monitoring destination IP | Check for any failure on the communication path to the monitoring destination. |
| 852 | secondary polling failed. lip=logicalIP, target=pollip. | An error of path to the secondary monitoring destination was detected in the initial check of the physical interface. LogicalIP: Logical IP, pollip: Monitoring destination IP | Check for any failure on the communication path to the monitoring destination. |
| 853 | physical interface up failed. | Failed to activate a physical interface. | Check that there is no mistake in the setting of Redundant Line |

| Message number | Message | Meaning | Action |
|----------------|---|--|--|
| | | | Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 854 | logical interface up failed. | Failed to activate a logical interface. | Check that there is no mistake in the setting of Redundant Line Control function and cluster system. If there is no mistake, collect materials for examination of Redundant Line Control function, and then contact field engineers to report the error message. |
| 855 | cluster logical interface is not found. | The logical interface registered with the cluster was not found. | Check that there is no mistake in the setting of a system, Redundant Line Control function, and cluster system. If the same phenomenon occurs, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. See the manual as to the materials necessary for examining a cluster system. |
| 856 | cluster configuration is incomplete. | The logical IP address cannot be activated because the cluster settings are incomplete. | Review the cluster system settings, and reboot the system |
| 857 | polling information is not defined. | Monitoring destination information is not defined. | Define monitoring destination information using the hanetpoll command. |
| 858 | observe information is not defined. | Monitoring destination information is not defined. | Define monitoring destination information using the hanetobserv command. |
| 859 | in.routed is not started. | Routing daemon is not started. | Enable svc:/network/routing/route service to activate routing daemon (in.routed). |
| 870 | polling status changed: Primary polling failed. (ifname,target=pollip) | Line monitoring on the primary side failed. ifname: Interface name, pollip: Monitoring destination address | Check for any failure on the communication path to the monitoring destination. |
| 871 | polling status changed: Secondary polling failed. (ifname,target=pollip) | Line monitoring on the secondary side failed. ifname: Interface name, pollip: Monitoring destination address | Check for any failure on the communication path to the monitoring destination. If monitoring stopped after checking the recovery of the communication path, make the |

| Message number | Message | Meaning | Action |
|----------------|--|--|--|
| | | | HUB monitoring function invalid and valid using the hanetpoll command. If monitoring fails even though possible to communicate normally, tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command. |
| 872 | polling status changed: PrimaryHUB to SecondaryHUB polling failed. (ifname,target=pollip) | An error in the secondary HUB was detected by HUB-to-HUB communication monitoring from the primary interface. ifname: Interface name, pollip: Monitoring destination address | Check for any failure on the communication path to the monitoring destination. If monitoring fails even though possible to communicate normally, tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command. |
| 873 | polling status changed: SecondaryHUB to PrimaryHUB polling failed. (ifname,target=pollip) | An error in the primary HUB was detected by HUB-to-HUB communication monitoring from the secondary interface. ifname: Interface name, pollip: Monitoring destination address | Check for any failure on the communication path to the monitoring destination. If monitoring fails even though possible to communicate normally, tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command. |
| 874 | polling status changed: HUB repair (target=pollip) | Line failure in HUB-to-HUB communication monitoring was repaired. pollip: Monitoring destination address | No action is required. |
| 875 | standby interface failed.(ifname) | An error involving standby interface was detected in the standby patrol. ifname: Interface name | Check that there is no error in a transfer route of the standby side. When it takes long time to link up, occasionally a recovery message is output immediately after this message is output. In this case, a transfer route of the standby side is normal. Therefore, not necessary to deal with. |
| 876 | node status is noticed. (sourceip:status) | A node status change was notified from the remote system. sourceip: Source address, status: Notified status | Check the status of the source. |
| 877 | route error is noticed.(sourceip) | A communication path failure was notified from the remote system. sourceip: Source address | Check for any failure on the communication path to the source. |

| Message number | Message | Meaning | Action |
|----------------|---|--|---|
| 878 | route error is detected. (target=IP) | A communication path failure was detected from the remote system. IP: Remote system address | Check for any failure on the communication path to the source. |
| 879 | message received from unknown host.(srcaddr) | A message was received from an unregistered remote system. srcaddr: Source address | Register the corresponding remote host using the hanetobserve command. |
| 880 | failed to send node down notice by time out. (dstip) | Node status notification failed due to timeout. dstip: Destination address | Check for any failure of the remote system and on the communication path to the remote system. |
| 881 | semaphore is broken. (errno) | Creates a semaphore again because it is deleted. | Not necessary to deal with. |
| 882 | shared memory is broken. (errno) | Creates a shared memory again because it is deleted. | Not necessary to deal with. |
| 883 | activation of a wrong interface has been detected. (ifname) | Since the interface was unjustly activated by the user, the state of an interface is restored. ifname: interface name | Check that the interface has been recovered correctly. In addition, when this message is displayed to the user operating nothing, please investigate the cause of the abnormality occurred. |
| 884 | unexpected interface deactivation has been detected. (ifname) | Since the interface was unjustly deactivated by the user, the state of an interface is restored. ifname: interface name | Check that the interface has been recovered correctly. In addition, when this message is displayed to the user operating nothing, please investigate the cause of the abnormality occurred. |
| 885 | standby interface recovered. (ifname) | It detected that the route by the side of standby was recovered by standby patrol. ifname: interface name of standby patrol | Not necessary to deal with. |
| 886 | recover from route error is noticed.(ifname) | The recovery was notified from the remote system. ifname: Interface name | Not necessary to deal with. |
| 887 | recover from route error is detected. (target=IP) | The recovery of the remote system was detected. IP: Remote system address | Not necessary to deal with. |
| 888 | interface is activated. (ifname) | The physical interface was activated. ifname: Interface name | Not necessary to deal with. |
| 889 | interface is inactivated. (ifname) | The physical interface was inactivated. ifname: Interface name | Not necessary to deal with. |
| 890 | logical IP address is activated. (logicalIP) | The logical IP address was activated. logicalIP: Logical IP | Not necessary to deal with. |

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| 891 | logical IP address is inactivated. (logicalIP) | The logical IP address was inactivated. logicalIP: Logical IP | Not necessary to deal with. |
| 892 | logical virtual interface is activated. (ifname) | The logical virtual interface was activated. ifname: Interface name | Not necessary to deal with. |
| 893 | logical virtual interface is inactivated. (ifname) | The logical virtual interface was inactivated. ifname: Interface name | Not necessary to deal with. |
| 894 | virtual interface is activated. (ifname) | The virtual interface was activated. ifname: Interface name | Not necessary to deal with. |
| 895 | virtual interface is inactivated. (ifname) | The virtual interface was inactivated. ifname: Interface name | Not necessary to deal with. |
| 896 | path to standby interface is established. (ifname) | Monitoring by standby patrol started normally. Ifname: A name of a standby patrol interface. | Not necessary to deal with. |
| 897 | immediate exchange to primary interface is canceled. (ifname) | Restrained prompt failback to the primary interface by standby patrol. ifname: A name of an interface. This message is output when the monitor-to information to set by a hanetpoll create command is other than HUB. | Not necessary to deal with. |
| 899 | route to polling address is inconsistent. | The network address defined to virtual interface and monitoring target is not the same, or since inappropriate routing information was registered into routing table, the mistaken monitoring is performed. | Please correct, when you check monitoring target address and there is an error. When there is no error in monitoring target address, please check whether inappropriate routing information is registered into the routing table. When using tagged VLAN interface, please confirm whether a virtual interface is a setting of NIC switching mode (operation mode "d"). If the setting of a virtual interface is NIC switching mode (operation mode "e"), please change the setting of corresponding monitoring information. |

Table A.5 Message number 9xx

| Message number | Message | Meaning | Action |
|----------------|--|---|--|
| 901 | failed to takeover logical interface used in zone. | Takeover of the logical interface for the non-global zone failed. | The following causes are suspected: * The number of logical |

| Message number | Message | Meaning | Action |
|----------------|---|---|--|
| | | | <p>interfaces reaches the maximum.</p> <p>* The same IP address is used for two or more interfaces in the system.</p> <p>* The same IP address is used for the other node and IPv6.</p> <p>Check the network interface and network environment in the system.</p> |
| 902 | logical interface of zone was added to a secondaryIF. | The logical interface for the non-global zone was added to the secondary interface. | The secondary interface is set to the network interface of the non-global zone. Changing the interface to the primary interface is highly recommended. However, this will not affect ongoing operations because the logical interface for the non-global zone will automatically be taken over to the primary interface. |
| 903 | succeeded in takeover logical interface used in zone. | The logical interface for the non-global zone was succeeded. | Not necessary to deal with. |
| 908 | hanetctld restarted. | The control daemon of GLS was started again. | Not necessary to deal with. |
| 909 | failed to restart daemon. | Stop of the daemon was detected and restart was tried, but failed. | Collect materials for examination of Redundant Line Control function, and contact field engineers to report the error message. |
| 924 | physical interface is not running. (ifname) | An interface is not linked up. ifname: Interface name | Check whether NIC or HUB failures occur. |
| 925 | exchange interface is canceled. (ifname) | Stops switching NICs because the interface of the switching target is not linked up. ifname: Interface name | Check whether NIC or HUB failures occur. |
| 931 | hangup of ping command has been detected. (target=pollip) | A hang-up of the ping command for the monitoring destination is detected. pollip: Monitoring destination IP address | Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message. |
| 932 | cannot send fhsp message. (dest=hostip, code) | The message of Fujitsu Hot Standby Protocol failed to be sent. hostip: Destination IP address code: Detailed code | <p>Check if the setting to pass through the firewall is correctly set for Fujitsu Hot Standby Protocol (UDP: port number 1807).</p> <p>If no problem has been found, collect materials for the examination of the Redundant Line Control function and</p> |

| Message number | Message | Meaning | Action |
|----------------|---|--|--|
| | | | contact field engineers to report the error message. |
| 973 | failed to startup self-checking. | The self-checking function failed to start. | Follow the instructions of the previously displayed message. |
| 974 | sha driver error has been detected. | GLS driver error has been detected. | Follow " 2.3.6 Self-checking function " to take the appropriate action. |
| 976 | hanetctld error has been detected. | GLS daemon error has been detected. | If a recovery message of 977 is displayed, no action is required. If not displayed, follow " 2.3.6 Self-checking function " to take the appropriate action. |
| 977 | hanetctld recovery has been detected. | GLS daemon recovery has been detected. | No action is required. |
| 979 | failed to execute a shell script. | User script execution has failed. | Check that the user script file is present. Also, check whether the system resources are running out by checking the message output time. |
| 980 | sha driver does not exist. | The virtual driver is not installed. | Check whether the GLS package (FJSVhanet) is installed. Also, check that the system has been rebooted after installation. |
| 981 | hanetctld does not exist. | The control daemon is not running. | Check whether the GLS package (FJSVhanet) is installed. Also, check that the system has been rebooted after installation. |
| 982 | svc:/system/filesystem/local:default service was not changed to online state. (details) | The state of the local file system service (svc:/system/filesystem/local:default) was not changed to online. details: Error details | Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message. |
| 983 | failed to mount a file system. (details) | Mounting of the file system failed. details: Error details | Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message. |
| 984 | file system is inconsistent. (details) | The inconsistency of the file system occurred. details: Error details | Make sure that the system startup is completed and /opt is mounted. After that, perform one of the following actions: <ul style="list-style-type: none"> - Starting the system again - Starting GLS service <pre># svcadm clear fjsvhanet</pre> If the operation is not started normally after starting GLS service, the TCP/IP application that uses Redundant Line |

| Message number | Message | Meaning | Action |
|----------------|---|---|---|
| | | | Control function may be failed. Start the system again. |
| 990 | line status changed: all lines disabled: (devicename: interface1=Down, interface2=Down, ...) | In fast switching mode, it is not possible to continue communicating with the other end host because all physical interfaces (interfaceN) bundled by a virtual interface in operation (devicename) became Down. | Check if or not there is any error in a transfer route of communication to the other end host for all physical interfaces. |
| 991 | line status changed: some lines in operation: (devicename: interface1=[Up Down], interface2=[Up Down], ...) | In fast switching mode, part of the physical interfaces (interfaceN) bundled by a virtual interface in operation (devicename) became Down (or Up). | Check if or not there is any error in a transfer route of communication to the other end host for physical interfaces in Down status. |
| 992 | line status changed: all lines enabled: (devicename: interface1=Up, interface2=Up, ...) | In fast switching mode, all physical interfaces (interfaceN) bundled by a virtual interface in operation (devicename) became Up and communication with the other end host recovered. | No action is required. |
| 993 | link down detected: Primary polling failed. (ifname,target=pollip) | The line monitoring failed because link down of the primary interface was detected. ifname: Interface name pollip: Monitoring target address | Check whether an error has occurred in the communication path to the monitoring target. If any failure occurs in the communication path, follow "4.6 Recovery Procedure from Line Failure" to take the appropriate action. After that, use the "dspoll" command to check the monitoring state. If the monitoring stopped, use the "hanetpoll" command to disable the HUB monitoring function once, and then enable it. |
| 994 | link down detected: Secondary polling failed. (ifname,target=pollip) | The line monitoring failed because link down of the secondary interface was detected. ifname: Interface name pollip: Monitoring target address | Check whether an error has occurred in the communication path to the monitoring target. If any failure occurs in the communication path, follow "4.6 Recovery Procedure from Line Failure" to take the appropriate action. After that, use the "dspoll" command to check the monitoring state. If the monitoring stopped, use the "hanetpoll" command to disable the HUB monitoring |

| Message number | Message | Meaning | Action |
|----------------|--|---|------------------------------------|
| | | | function once, and then enable it. |
| 996 | polling status changed: Primary polling recovered. (ifname, target=pollip) | Line monitoring on the primary side recovered. ifname: Interface name pollip: Monitoring target address | No action necessary. |

GLS: Global Link Services

A.1.4 Internal information output messages (no message number)

The following describes the messages to output the internal information of Redundant Line Control function to /var/adm/messages, and their meaning.

| Message number | Message | Meaning | Action |
|----------------|----------------------------------|--|------------------------|
| - | update cluster resource status. | To update the state of the cluster resources. | No action is required. |
| - | receive message from sha driver. | Received a message from an SHA driver. | No action is required. |
| - | receive event from cluster: | Received an event from the cluster management. | No action is required. |
| - | polling | To control a monitoring function. | No action is required. |
| - | in.routed killed. | To terminate an in.routed daemon process. | No action is required. |
| - | in.rdisc killed. | To terminate an in.rdisc daemon process. | No action is required. |
| - | child proc exit. | A monitoring process terminated. | No action is required. |

A.1.5 DR connection script error output messages

In a DR connection script of the Redundant Line Control function, a message is output when not possible to continue communication by disconnecting the corresponding virtual interface and the actual interface due to a certain reason, or when failed to disconnect or connect detecting an error in the workings of a DR connection script. The messages displayed in a DR connection script of the Redundant Line Control function are as follows:

| Code | Message | Meaning | Action |
|------|---|---|---|
| 0001 | When the DR processing is executed for this NIC, the communication is disconnected. The DR processing is stopped. devicename=XX interface=YY | When executed a DR process to an interface YY that a virtual interface XX bundles, the communication is disconnected. Stops the DR process. | Deactivate a virtual interface XX, delete a definition of a virtual interface XX, and execute a DR process again. |
| 0002 | The interface is Cluster interface. The DR processing is stopped. action=ZZ devicename=XX interface=YY | A virtual interface XX that bundles an interface YY is already registered as the cluster resource. Stops a DR process. | Delete a definition of the cluster environment and execute a DR process again. |

| Code | Message | Meaning | Action |
|------|---|--|---|
| 0003 | hanetnic command abnormal end. action=ZZ devicename=XX interface=YY | Ended abnormally by a hanetnic command (ZZ subcommand) while having a DR process to an interface YY that is bundled into a virtual interface XX. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a DR process again. If the same phenomenon occurs, contact field engineers to report the error message. |
| 0004 | strptl command abnormal end. devicename=XX interface=YY | Ended abnormally by an strptl command while executing a DR process to an interface YY that is bundled into a virtual interface XX. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a strptl command again. If the same phenomenon occurs, contact field engineers to report the error message. |
| 0005 | stpptl command abnormal end. devicename=XX interface=YY | Ended abnormally by an stpptl command while executing a DR process to an interface YY that is bundled into a virtual interface XX. | Check that there is no mistake in the setting of Redundant Line Control function. After checked there is no mistake, execute a DR process again. If the same phenomenon occurs, contact field engineers to report the error message. |
| 0006 | hanetpoll on command abnormal end. | Ended abnormally by hanetpoll on command. | After processed DR, check that the settings of Redundant Line Control function have no mistake, and execute hanetpoll on command. If an error occurred even after that, check how to deal with the displayed error in a manual and follow the instructions. |
| 0007 | hanetconfig modify command abnormal end. devicename=XX NIC_list=YY | While processing DR to the interface XX that is bundled into a virtual interface YY, ended abnormally by hanetconfig modify command. | Check that the settings of Redundant Line Control function have no mistake. After checked there is no mistake, execute a DR process again. If the same phenomenon occurred even after that, contact field engineers to report the error message. |
| 0008 | Is the DR processing continued ? | Do you continue to process DR? | Input "YES" to continue, "NO" to end. Inputting "YES" into this message to continue DR processing is recommended. |
| 0009 | The interface is IPv6 interface. The DR processing is stopped. action=delete interface=YYYY | A virtual interface that uses an IPv6 address in an interface YYYY exists. Stops DR processing. | Delete the configuration information that uses an IPv6 address and execute the DR processing again. |

A.2 Messages Displayed in the Cluster System Logs

This section explains the meaning and the action to take for each message output by Redundant Line Control function if startup of the cluster system fails.

Cluster system logs are stored in the following directories:

For details on each log file (switchlog, appX.log), see "PRIMECLUSTER Reliant Monitor Services (RMS) with Wizard Tools Configuration and Administration Guide."

```
/var/opt/SMAWRrms/log
```

| Message number | Message | Meaning | Action |
|----------------|---|--|--|
| - | (Gls): ERROR: virtual interface resource not found. | There is no resource setting. | Pay attention to the following points and check that there is no mistake in the settings of Redundant Line Control function and cluster system. |
| - | (Gls): ERROR: GdBegin failed. (rsc_name, host_name) | Failed to activate the Gls detector. rsc_name: Resource name of the cluster host_name: Takeover virtual IP address (host name) | - Ensure that the setting of the take over IP address is identical in each node of the cluster which takes over the IP address. Execute "hanethvrsc print" to check it. |
| - | online request failed.(errno) | Failed to activate the Gls resource in the online or standby state. 19: An appropriate is not recognized by GLS. 203: Failed to activate the takeover virtual interface. | - If a host name is used in GLS, ensure that host name is already recorded in /etc/hosts. - Ensure that the IP address setting of RMS Wizard is identical to that of the GLS take over IP address. If those settings are not correct, see the following sections to configure the settings correctly. After that, reboot the system or execute resethanet -s. "3.3 Additional system setup" "3.4 Changing system setup" "3.5 Deleting configuration information" "5.2 Adding configuration for Cluster System" If those settings are correct or the same phenomenon still occurs after configuring the settings, collect materials for examination of Redundant Line Control function and cluster system, and then contact field engineers to report the error message. |

GLS: Global Link Services

Appendix B Examples of configuring system environments

This appendix explains how to configure the system environment with redundant network control.

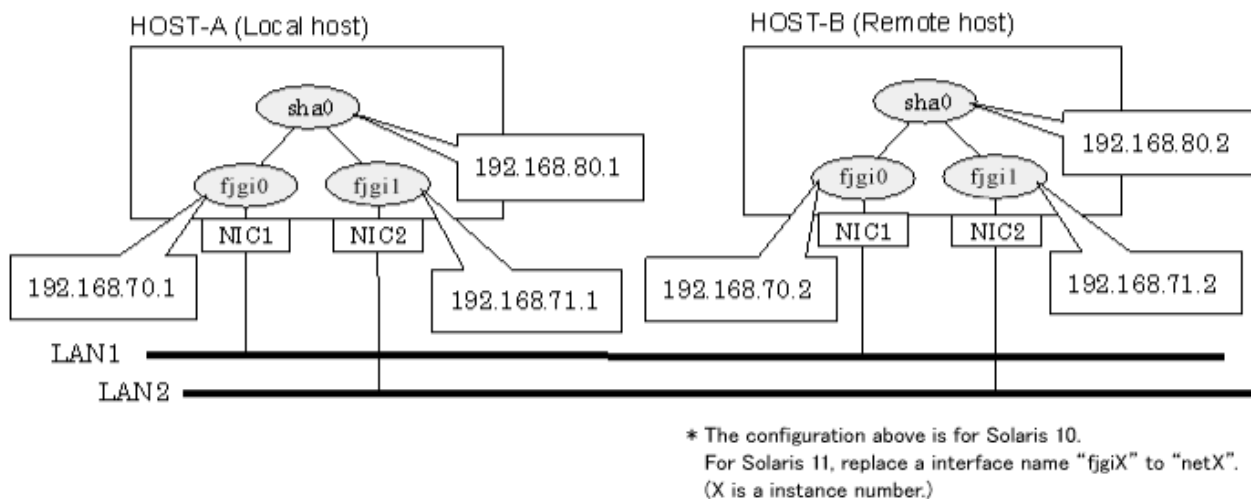
IP addresses used in examples of configuring system environments are all local IP addresses. You can specify these IP addresses with host names.

Moreover, interface names listed in examples of configuring system environments vary depending on the environment. Replace interface names according to the environment. For Solaris 11 or later, the default interface name is netX (X means the instance number).

B.1 Example of configuring Fast Switching mode (IPv4)

B.1.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJVSChanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJVSChanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJVSChanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

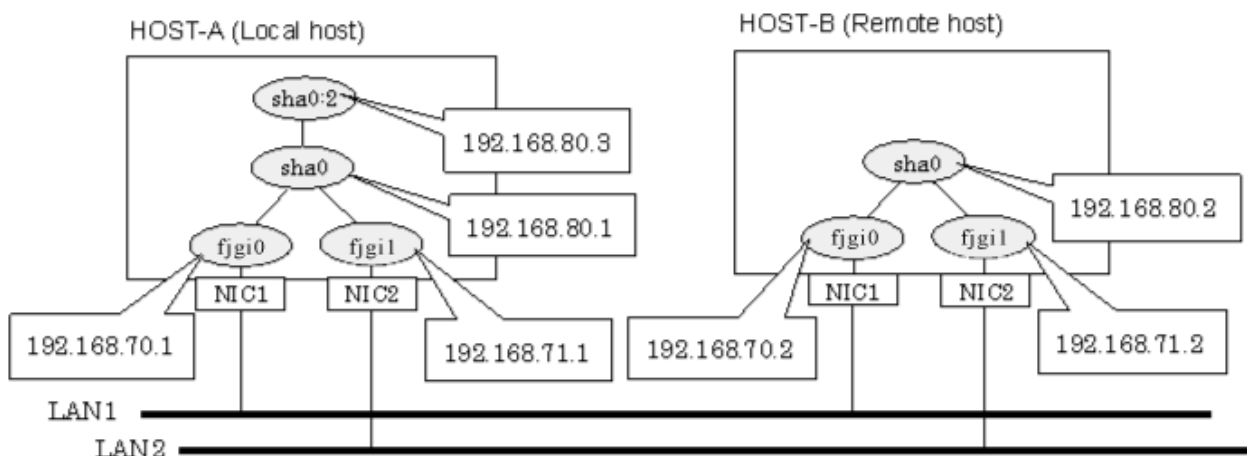
```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSSVhanet/usr/sbin/strhanet
```

B.1.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.80.3    hosta1 # HOST-A Logical virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Creation of logical virtual interface


```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
```

5) Activation of virtual interface and logical virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

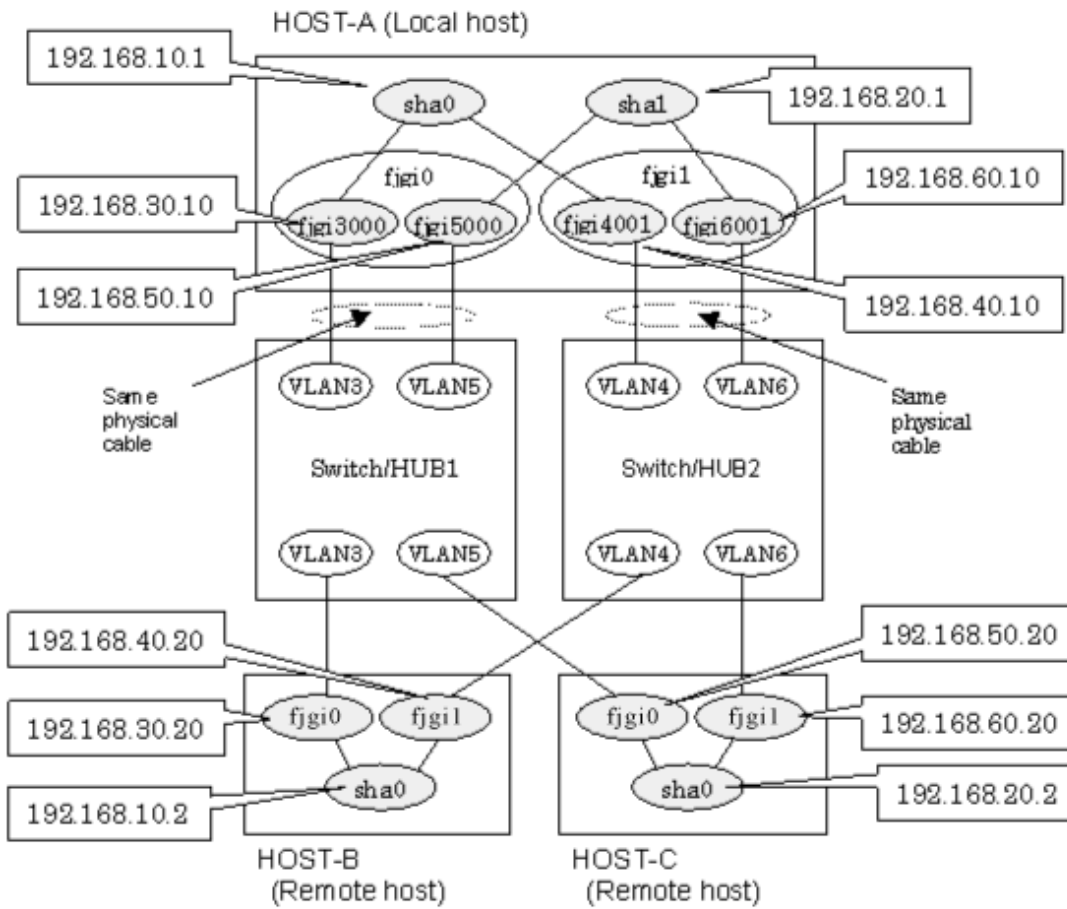
```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

B.1.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.10.1    hosta1    # HOST-A Virtual IP
192.168.20.1    hosta2    # HOST-A Virtual IP
192.168.30.10   hosta3    # HOST-A Physical IP (Tagged VLAN interface)
192.168.40.10   hosta4    # HOST-A Physical IP (Tagged VLAN interface)
192.168.50.10   hosta5    # HOST-A Physical IP (Tagged VLAN interface)
192.168.60.10   hosta6    # HOST-A Physical IP (Tagged VLAN interface)
192.168.10.2    hostb1    # HOST-B Virtual IP
192.168.30.20   hostb3    # HOST-B Physical IP
192.168.40.20   hostb4    # HOST-B Physical IP
192.168.20.2    hostc2    # HOST-C Virtual IP
192.168.50.20   hostc5    # HOST-C Physical IP
192.168.60.20   hostc6    # HOST-C Physical IP
    
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi3000

```
hosta3
```

- Contents of /etc/hostname.fjgi4001

```
hosta4
```

- Contents of /etc/hostname.fjgi5000

```
hosta5
```

- Contents of /etc/hostname.fjgi6001

```
hosta6
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a hosta3/24 net3000/v4
```

- Interface net4001

```
# /usr/sbin/dladm create-vlan -l net1 -v 4
# /usr/sbin/ipadm create-ip net4001
# /usr/sbin/ipadm create-addr -T static -a hosta4/24 net4001/v4
```

- Interface net5000

```
# /usr/sbin/dladm create-vlan -l net0 -v 5
# /usr/sbin/ipadm create-ip net5000
# /usr/sbin/ipadm create-addr -T static -a hosta5/24 net5000/v4
```

- Interface net6001

```
# /usr/sbin/dladm create-vlan -l net1 -v 6
# /usr/sbin/ipadm create-ip net6001
# /usr/sbin/ipadm create-addr -T static -a hosta6/24 net6001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.10.0    255.255.255.0
192.168.20.0   255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi3000, fjgi4001, fjgi5000 and fjgi6001 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t
fjgi3000,fjgi4001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t
fjgi5000,fjgi6001
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t net3000,net4001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t net5000,net6001
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hostb3
```

- Contents of /etc/hostname.fjgi1

```
hostb4
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostb3/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a hostb4/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hostc5
```

- Contents of /etc/hostname.fjgi1

```
hostc6
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a hostc5/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1  
# /usr/sbin/ipadm create-addr -T static -a hostc6/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure hme0 and hme1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

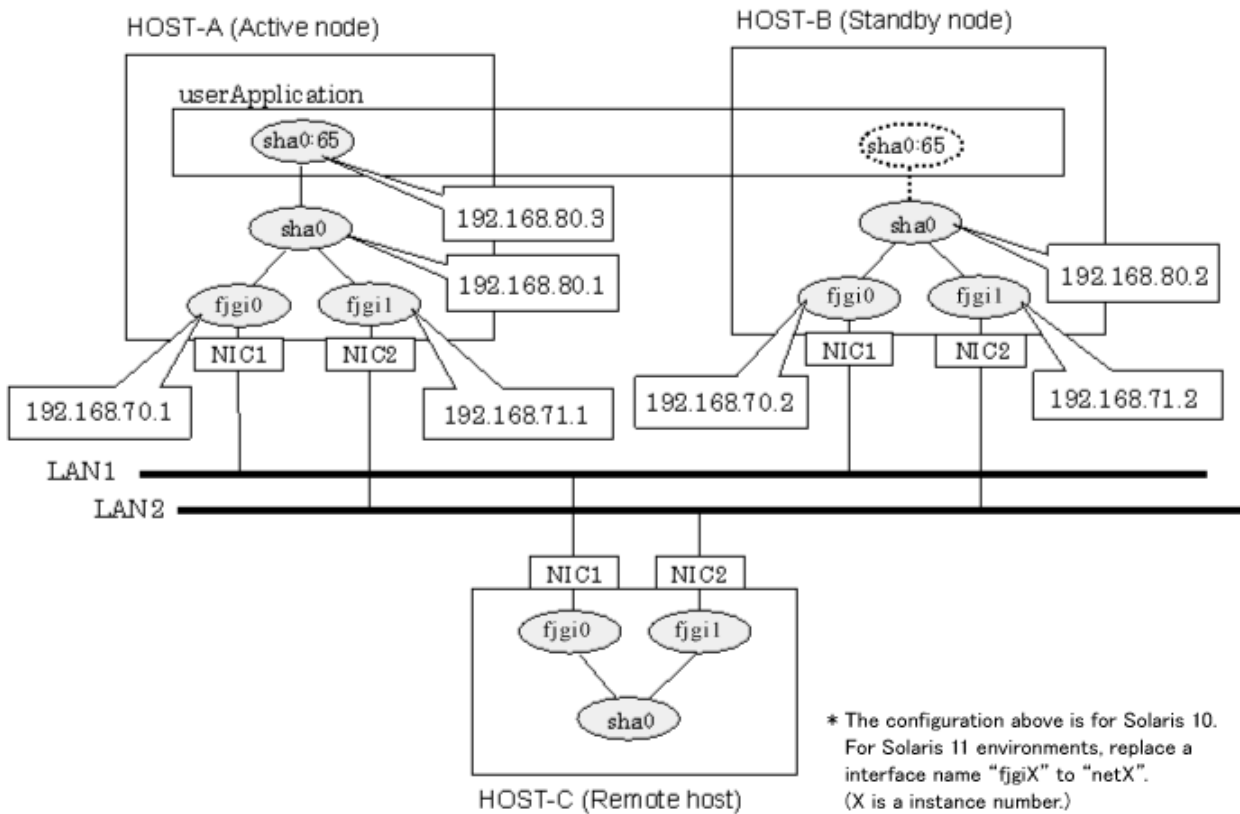
B.1.4 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.3    hosta1 # Takeover virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.3".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

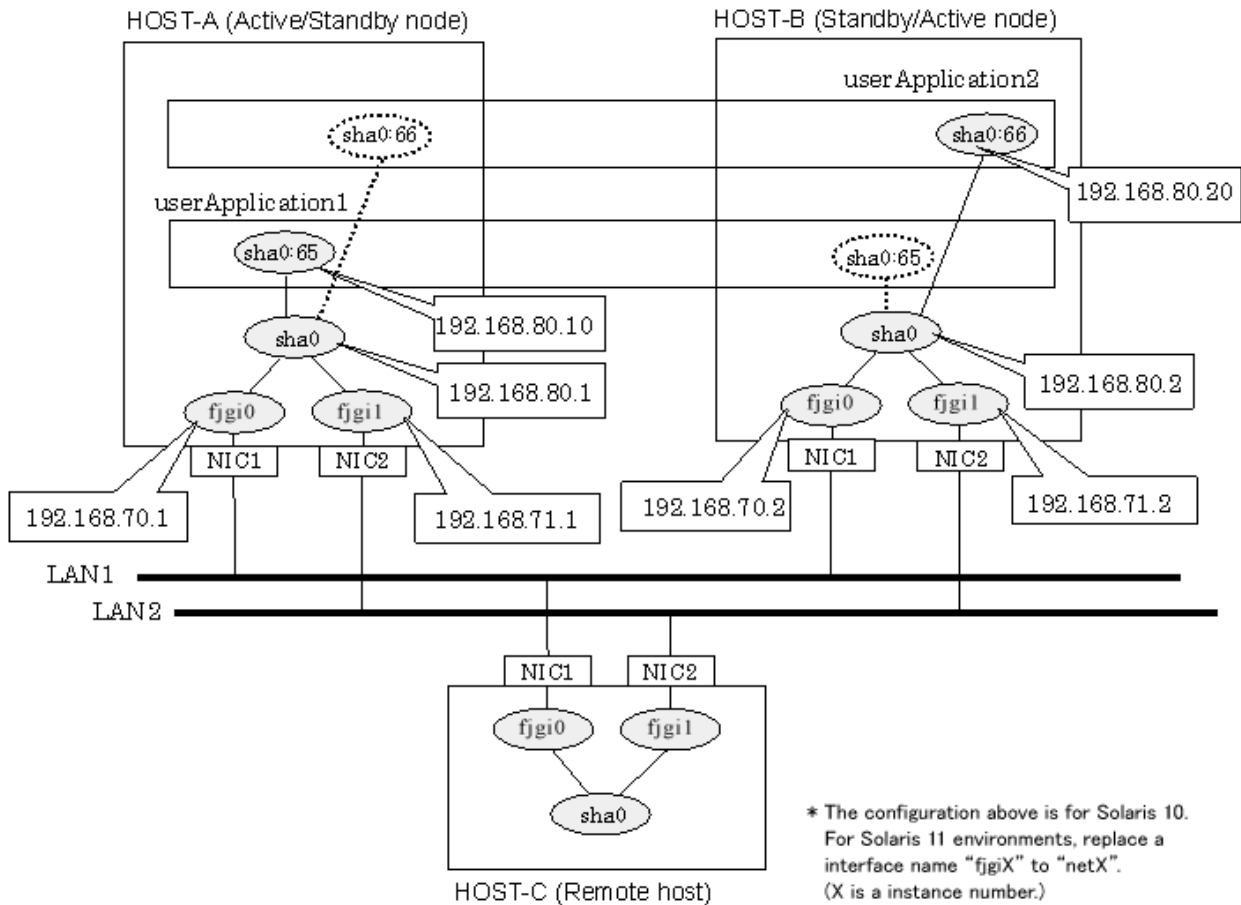
B.1.5 Example of the Cluster system (Mutual Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/inet/hosts` file.

```

192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.10   hosta1 # Takeover virtual IP (1)
192.168.80.20   hostb1 # Takeover virtual IP (2)

```

1-2) For Solaris 10

Write the hostnames defined above in `/etc/hostname.fjgi0` file and `/etc/hostname.fjgi1` file. If a file does not exist, create a new file.

- Contents of `/etc/hostname.fjgi0`

```
host11
```

- Contents of `/etc/hostname.fjgi1`

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the `ipadm(1M)` command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.3" and "192.168.80.10".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

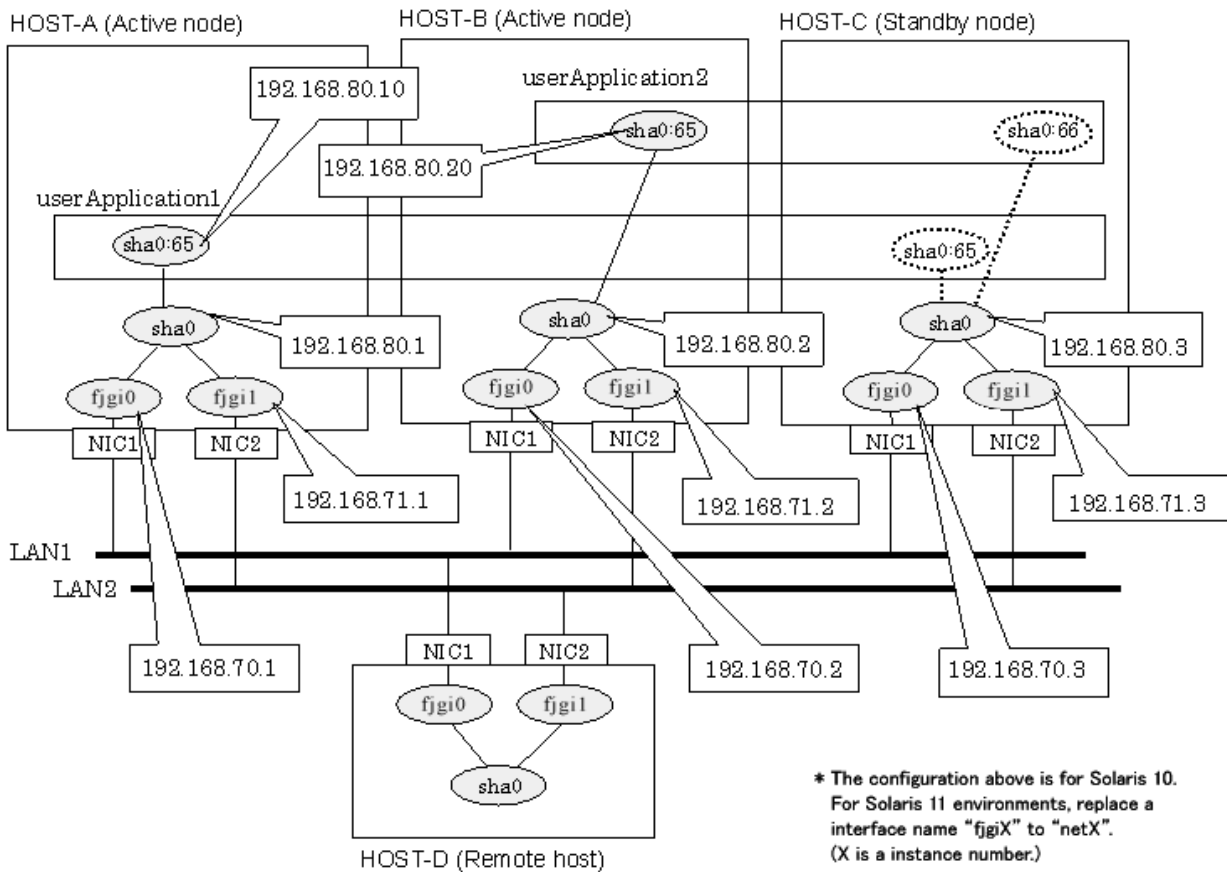
B.1.6 Example of the Cluster system (N:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1      host11 # HOST-A Physical IP (1)
192.168.71.1      host12 # HOST-A Physical IP (2)
192.168.80.1      hosta  # HOST-A Virtual IP
192.168.70.2      host21 # HOST-B Physical IP (1)
192.168.71.2      host22 # HOST-B Physical IP (2)
192.168.80.2      hostb  # HOST-B Virtual IP
192.168.70.3      host31 # HOST-C Physical IP (1)
192.168.71.3      host32 # HOST-C Physical IP (2)
192.168.80.3      hostc  # HOST-C Virtual IP
192.168.80.10     hosta1 # Takeover virtual IP (1)
192.168.80.20     hostb1 # Takeover virtual IP (2)

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host31
```

- Contents of /etc/hostname.fjgi1

```
host32
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host32/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.3" and "192.168.80.10".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

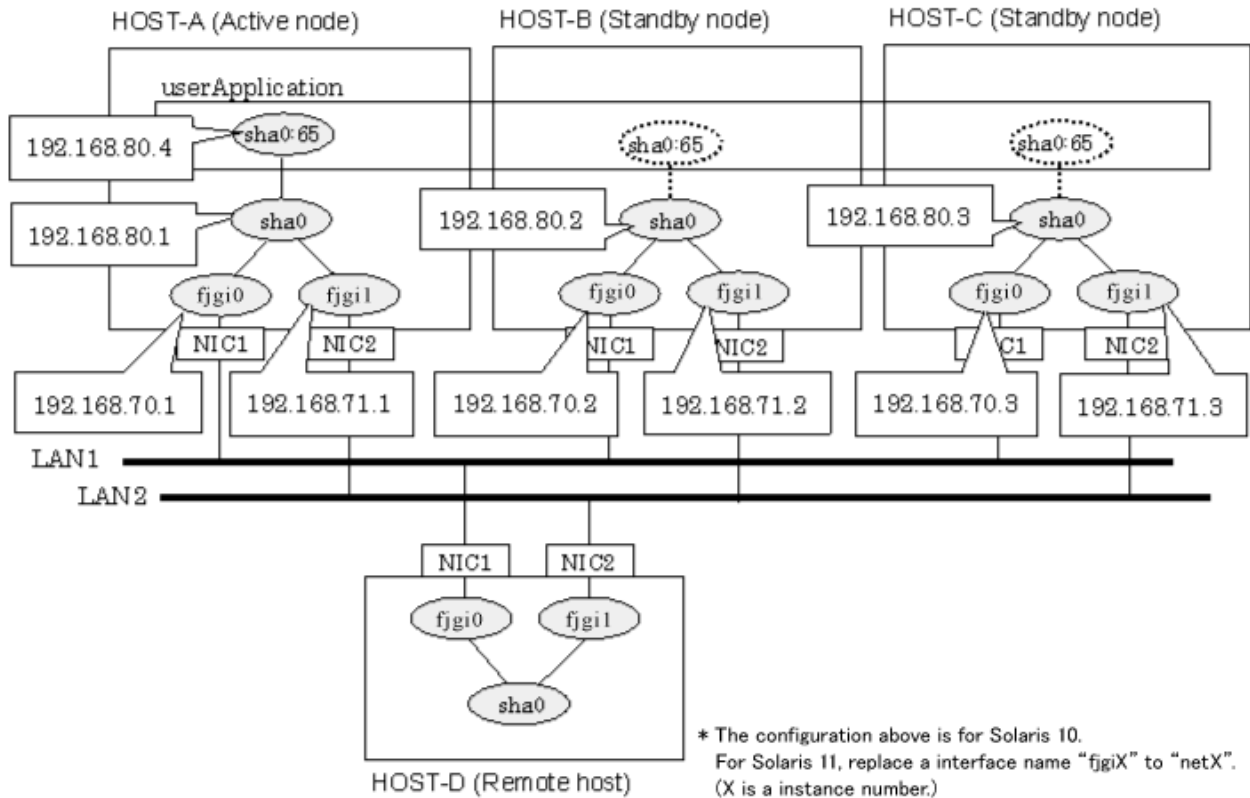
B.1.7 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP (1)
192.168.71.3    host32 # HOST-C Physical IP (2)
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.4    hosta1 # Takeover virtual IP

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0


```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot(For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host31
```

- Contents of /etc/hostname.fjgi1

```
host32
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host32/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create Gls resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once Gls is created, register the two Gls resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.4".

2) Starting of userApplication

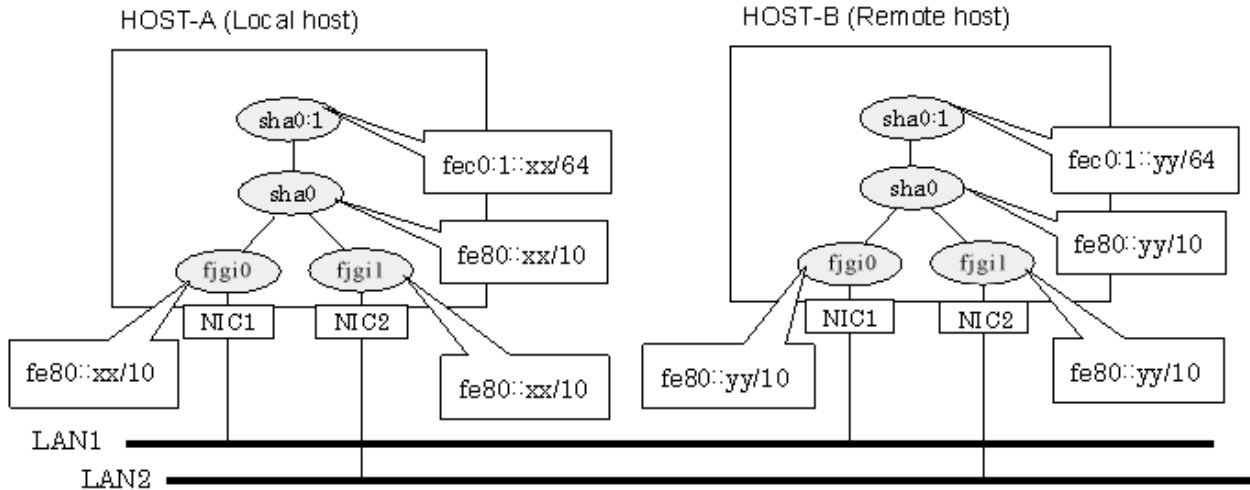
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2 Example of configuring Fast Switching mode (IPv6)

B.2.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 file as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1  
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

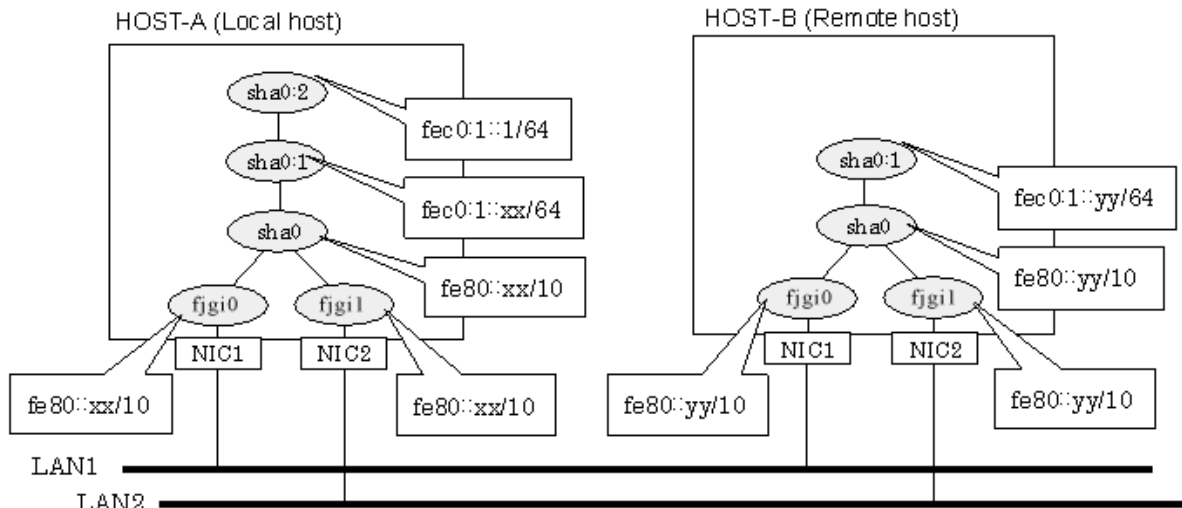
4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.2.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router
advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta1 # Logical virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of logical virtual interface

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::1/64
```

5) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define logical virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

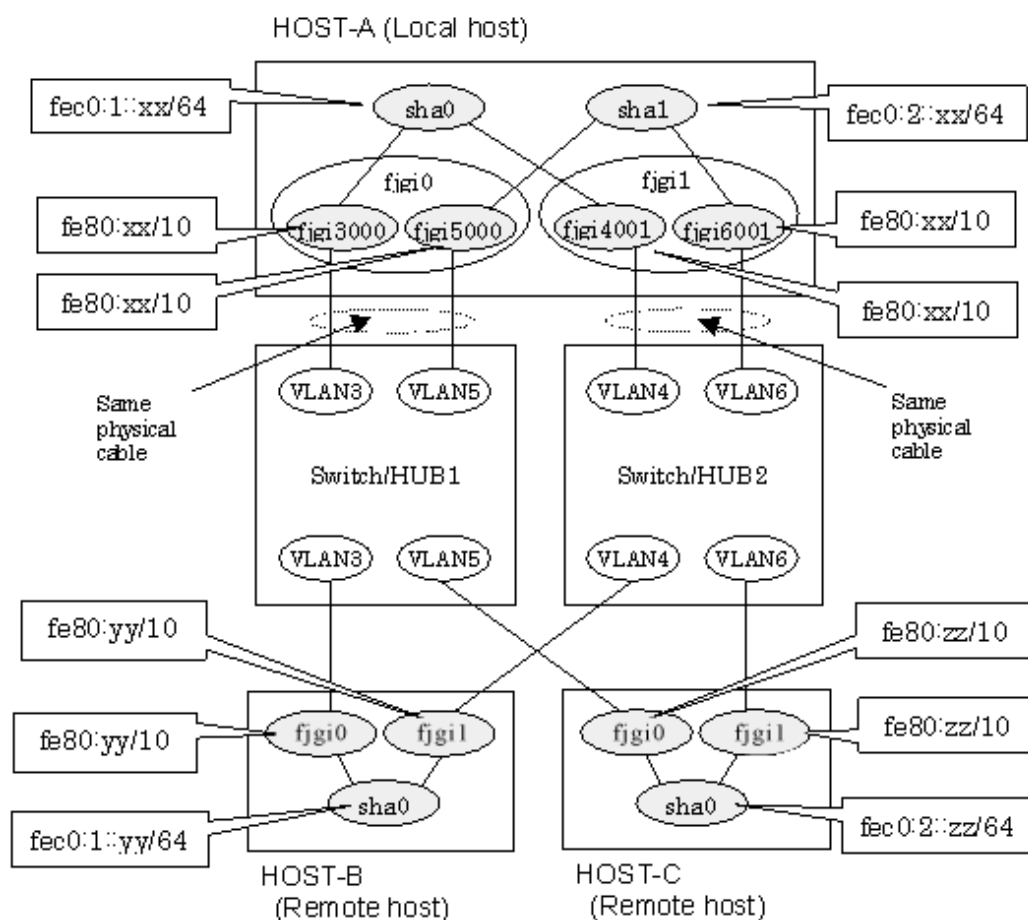
4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

B.2.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 sha1 # sha1 sends Prefix "fec0:2::0/64".
```


Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

1-2) For Solaris 10

Create `/etc/hostname6.fjgi3000`, `/etc/hostname6.fjgi4001`, `/etc/hostname6.fjgi5000` and `/etc/hostname6.fjgi6001` files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the `dladm(1M)` command and the `ipadm(1M)` command.

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

- Interface net4001

```
# /usr/sbin/dladm create-vlan -l net1 -v 4
# /usr/sbin/ipadm create-ip net4001
# /usr/sbin/ipadm create-addr -T addrconf net4001/v6
```

- Interface net5000

```
# /usr/sbin/dladm create-vlan -l net0 -v 5
# /usr/sbin/ipadm create-ip net5000
# /usr/sbin/ipadm create-addr -T addrconf net5000/v6
```

- Interface net6001

```
# /usr/sbin/dladm create-vlan -l net1 -v 6
# /usr/sbin/ipadm create-ip net6001
# /usr/sbin/ipadm create-addr -T addrconf net6001/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure `fjgi3000`, `fjgi4001`, `fjgi5000` and `fjgi6001` are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi3000,fjgi4001
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t fjgi5000,fjgi6001
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net3000,net4001
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t net5000,net6001
```

4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1  
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot(For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-C]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:2::0/64 sha0 # sha0 sends Prefix "fec0:2::0/64".
```

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.2.4 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

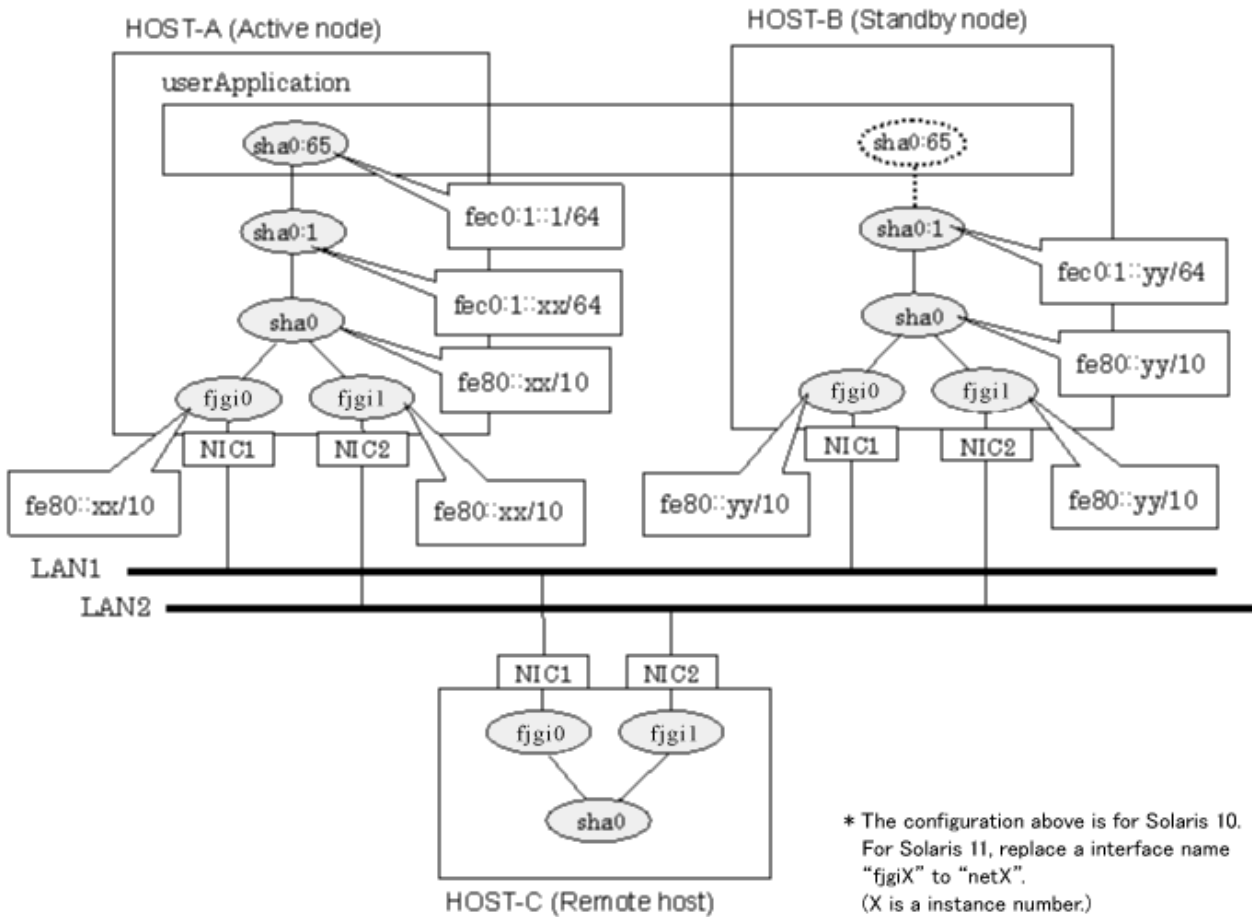
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



[HOST-A]

1) Setting up the system

Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1    # Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resource, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.5 Example of the Cluster system (Mutual standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

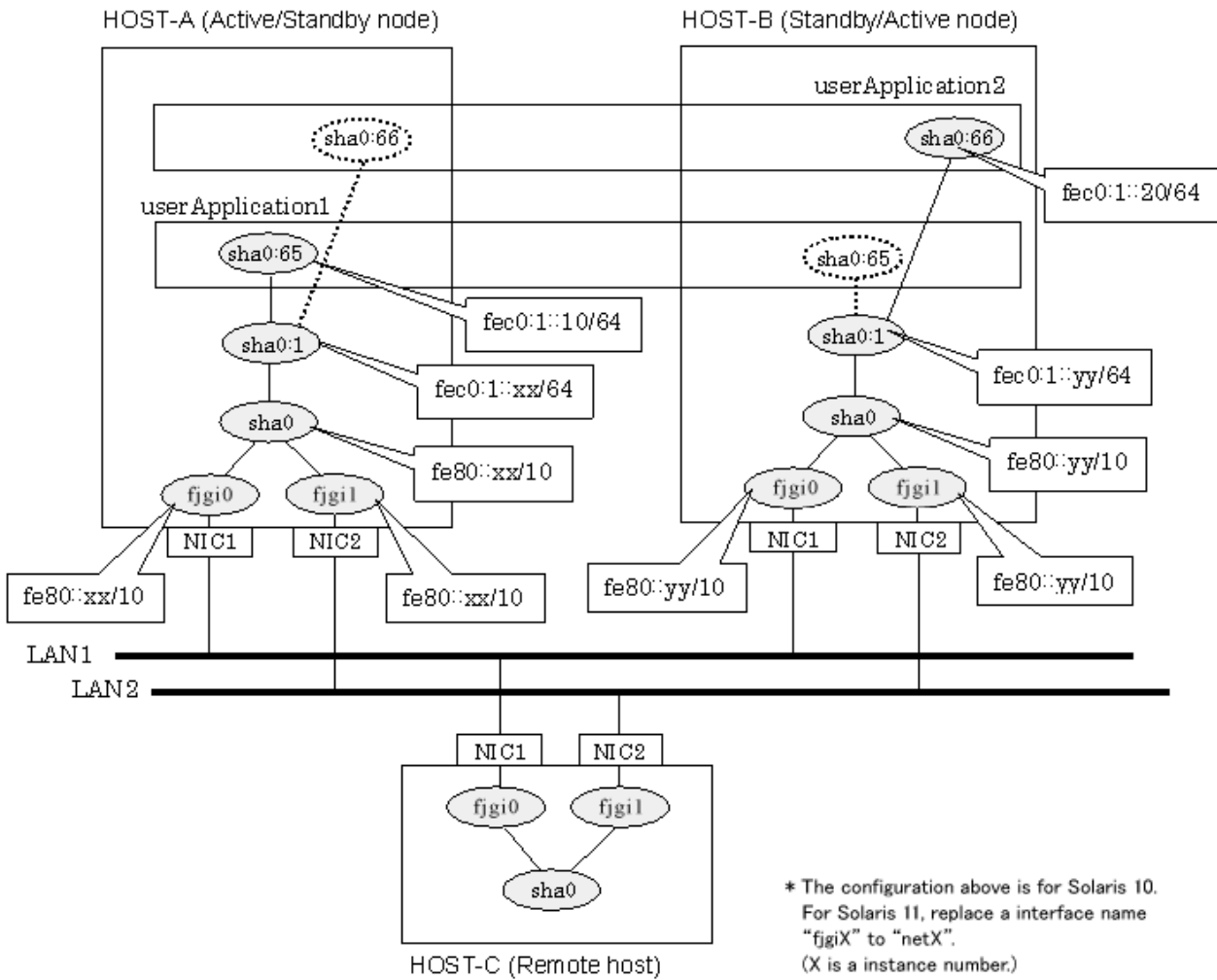
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



[HOST-A]

1) Setting up the system

1-1) Create `/etc/inet/ndpd.conf` file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

1-2) For Solaris 10

Create `/etc/hostname6.f吉i0` and `/etc/hostname6.f吉i1` files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the `ipadm(1M)` command.

- Interface `net0`

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10      v6hosta1  # Takeover virtual IP (1)
fec0:1::20      v6hostb1  # Takeover virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64  
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::10" and "fec0:1::20".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.6 Example of the Cluster system (N:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The values for xx, yy and zz in the IP address of the figure below are assigned automatically by the automatic address configuration.

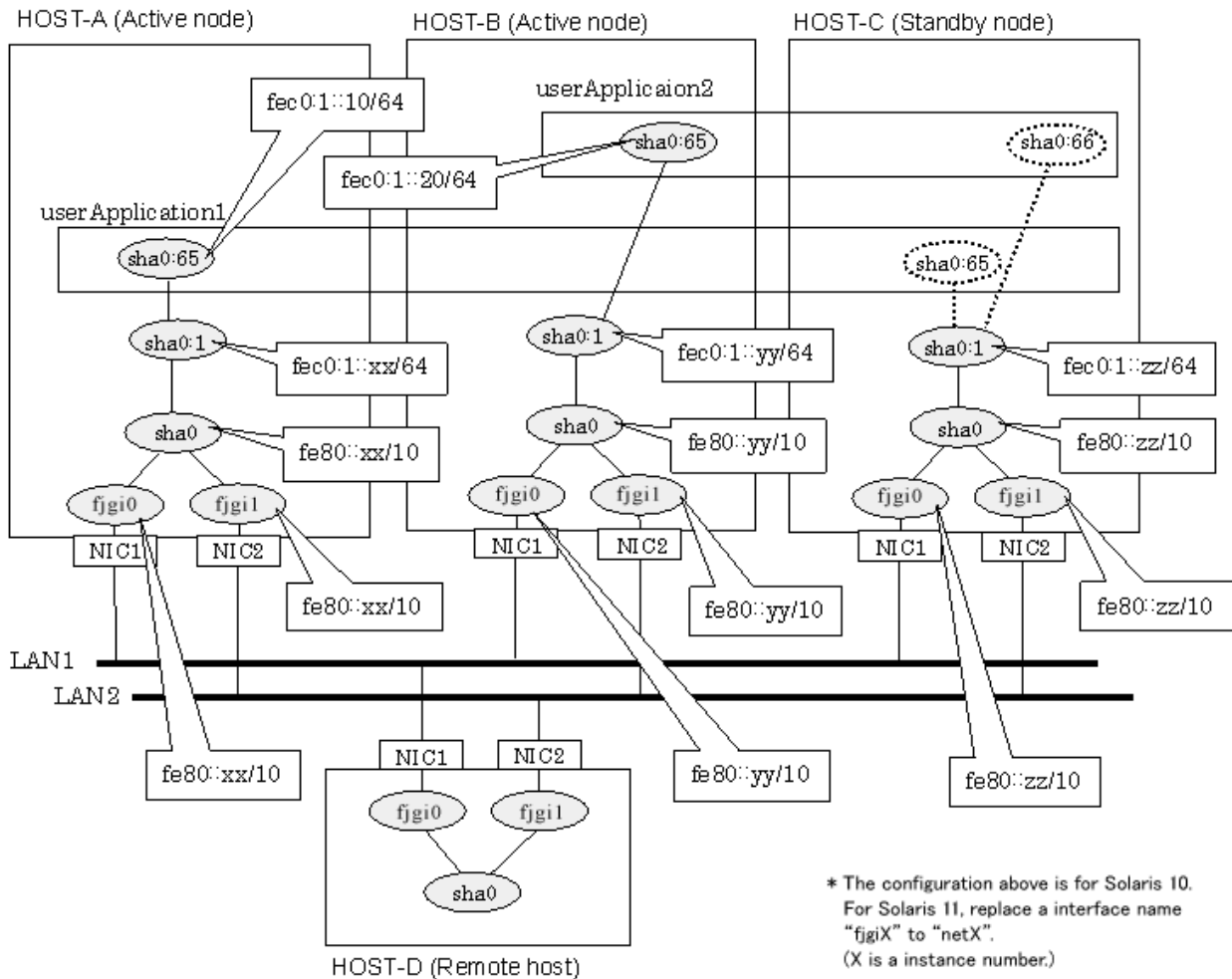
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10      v6hosta1  # Takeover virtual IP (1)
fec0:1::20      v6hostb1  # Takeover virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

[HOST-C]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::10" and "fec0:1::20".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.2.7 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

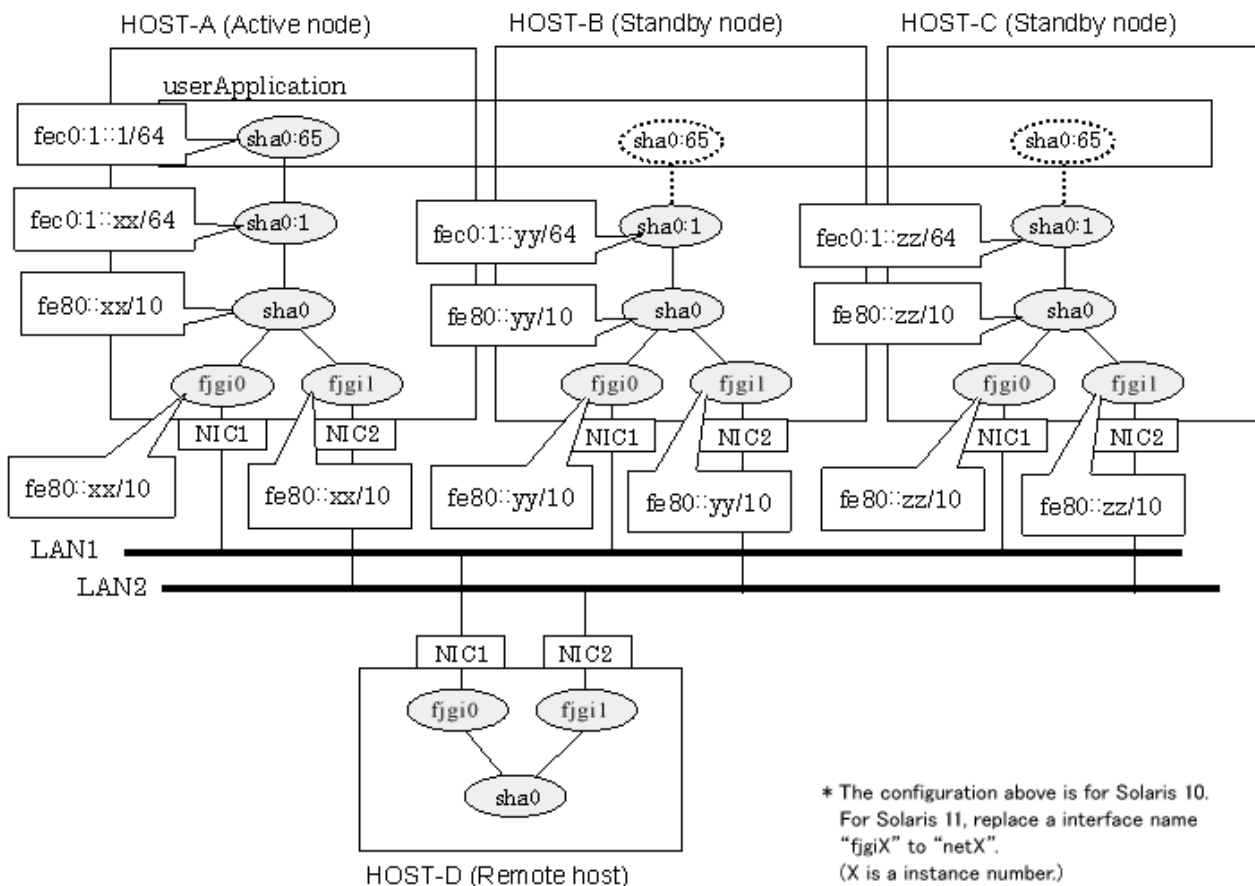
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1  
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta1 # Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

[HOST-C]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-3) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1".

2) Starting of userApplication

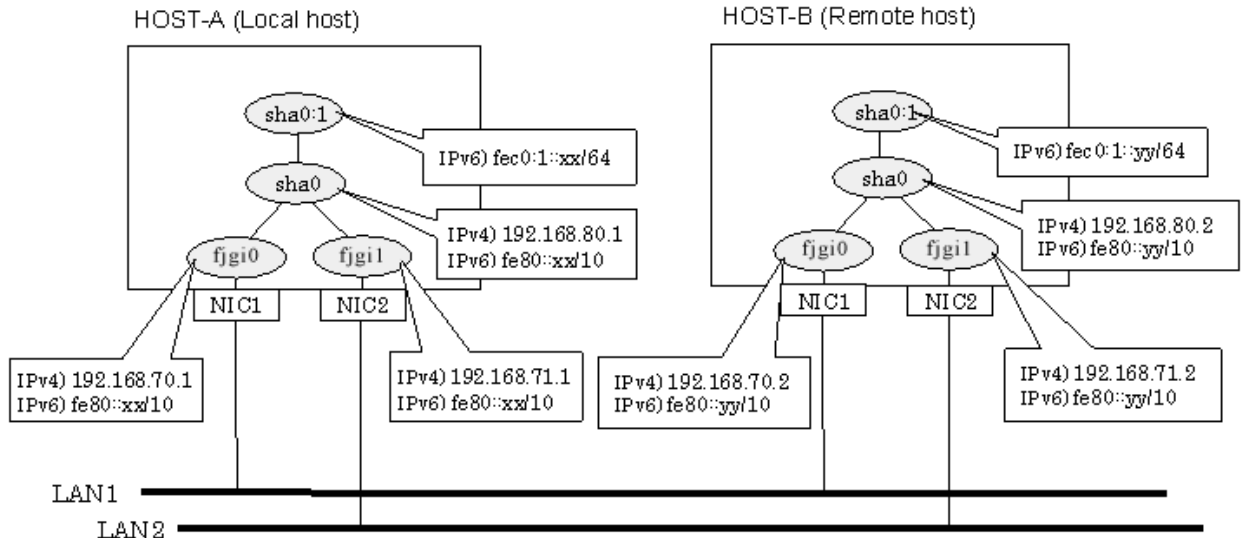
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3 Example of configuring Fast Switching mode (IPv4/IPv6)

B.3.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

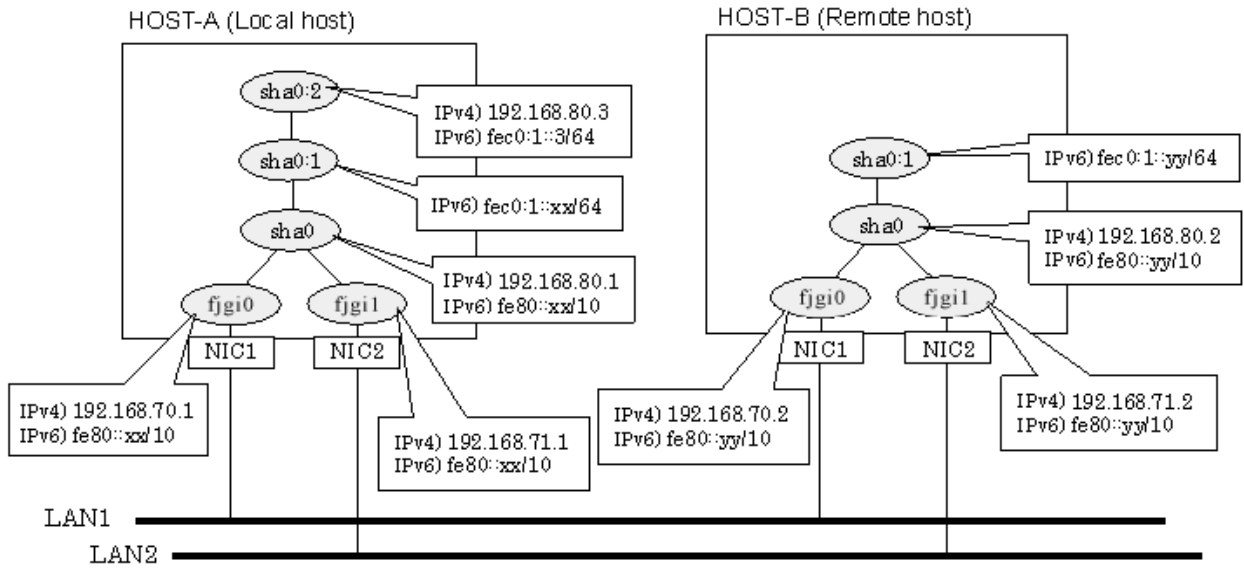
4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.3.2 Example of the Single system in Logical virtual interface

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.80.3    hosta1 # HOST-A Logical virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::3      v6hosta1 # Logical virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of logical virtual interface

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::3/64
```

5) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

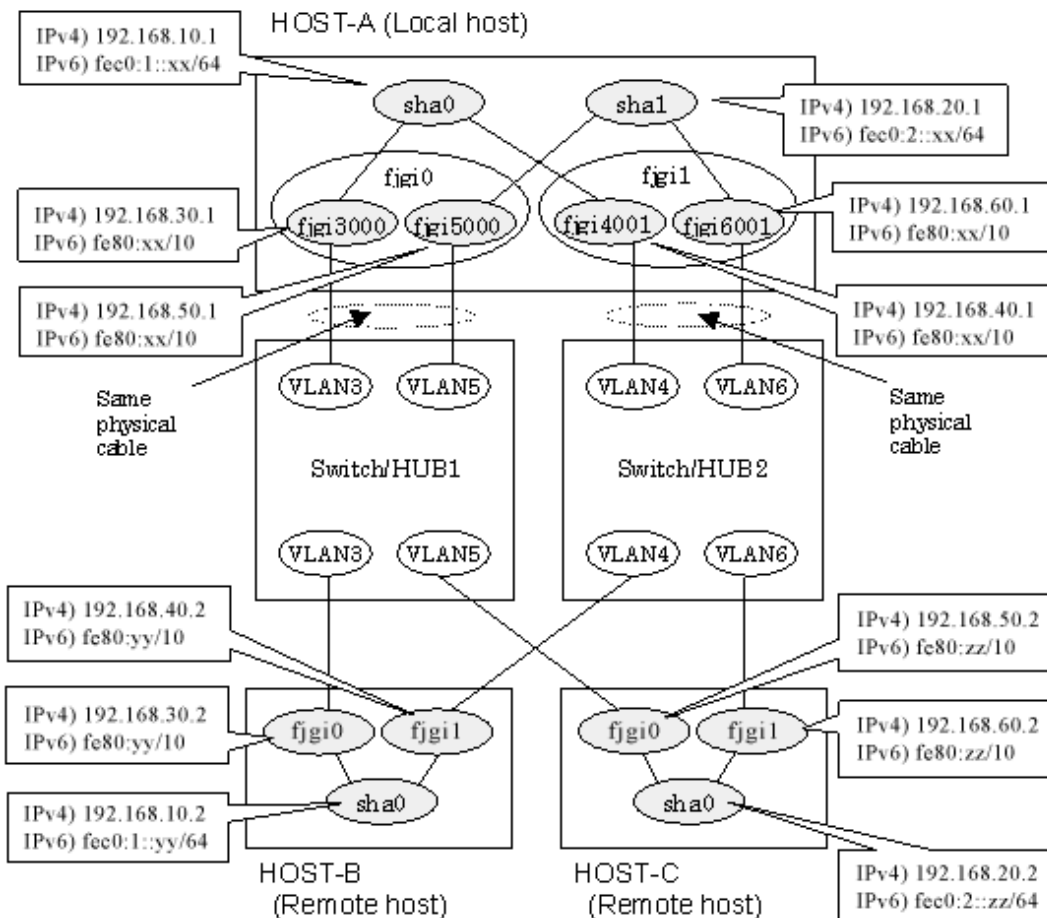
4) Activation of virtual interface

```
# /opt/FJSSVhanet/usr/sbin/strhanet
```

B.3.3 Configuring virtual interfaces with tagged VLAN

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.10.1    hosta1    # HOST-A Virtual IP
192.168.20.1    hosta2    # HOST-A Virtual IP
192.168.30.1    hosta3    # HOST-A Physical IP (Tagged VLAN interface)
192.168.40.1    hosta4    # HOST-A Physical IP (Tagged VLAN interface)
192.168.50.1    hosta5    # HOST-A Physical IP (Tagged VLAN interface)
192.168.60.1    hosta6    # HOST-A Physical IP (Tagged VLAN interface)
192.168.10.2    hostb1    # HOST-B Virtual IP
192.168.30.2    hostb3    # HOST-B Physical IP
192.168.40.2    hostb4    # HOST-B Physical IP
192.168.20.2    hostc2    # HOST-C Virtual IP
192.168.50.2    hostc5    # HOST-C Physical IP
192.168.60.2    hostc6    # HOST-C Physical IP

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname."interface-name" files. If a file does not exist, create a new file.

- Contents of /etc/hostname.fji3000


```
hosta3
```

- Contents of /etc/hostname.fjgi4001

```
hosta4
```

- Contents of /etc/hostname.fjgi5000

```
hosta5
```

- Contents of /etc/hostname.fjgi6001

```
hosta6
```

1-2) For Solaris 11 or later

Set the host by the interface used with the `dladm(1M)` command and the `ipadm(1M)` command and also by the host name defined above.

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a hosta3/24 net3000/v4
```

- Interface net4001

```
# /usr/sbin/dladm create-vlan -l net1 -v 4
# /usr/sbin/ipadm create-ip net4001
# /usr/sbin/ipadm create-addr -T static -a hosta4/24 net4001/v4
```

- Interface net5000

```
# /usr/sbin/dladm create-vlan -l net0 -v 5
# /usr/sbin/ipadm create-ip net5000
# /usr/sbin/ipadm create-addr -T static -a hosta5/24 net5000/v4
```

- Interface net6001

```
# /usr/sbin/dladm create-vlan -l net1 -v 6
# /usr/sbin/ipadm create-ip net6001
# /usr/sbin/ipadm create-addr -T static -a hosta6/24 net6001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.10.0    255.255.255.0
192.168.20.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi3000, /etc/hostname6.fjgi4001, /etc/hostname6.fjgi5000 and /etc/hostname6.fjgi6001 files as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the `dladm(1M)` command and the `ipadm(1M)` command.

- Interface net3000

```
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

- Interface net4001

```
# /usr/sbin/ipadm create-addr -T addrconf net4001/v6
```

- Interface net5000

```
# /usr/sbin/ipadm create-addr -T addrconf net5000/v6
```

- Interface net6001

```
# /usr/sbin/ipadm create-addr -T addrconf net6001/v6
```

1-5) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".  
prefix fec0:2::0/64 sha1 # sha1 sends Prefix "fec0:2::0/64".
```



In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi3000, fjgi4001, fjgi5000 and fjgi6001 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t fjgi3000,fjgi4001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t fjgi5000,fjgi6001
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t net3000,net4001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t net5000,net6001
```

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi3000,fjgi4001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t fjgi5000,fjgi6001
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net3000,net4001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t net5000,net6001
```

5) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hostb3
```

- Contents of /etc/hostname.fjgi1

```
hostb4
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostb3/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a hostb4/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-5) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hostc5
```

- Contents of /etc/hostname.fjgi1

```
hostc6
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostc5/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a hostc6/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.hfjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-5) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:2::0/64 sha0 # sha0 sends Prefix "fec0:2::0/64".
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t fjgi0,fjgi1
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t net0,net1
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJJSVhanet/usr/sbin/strhanet
```

B.3.4 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

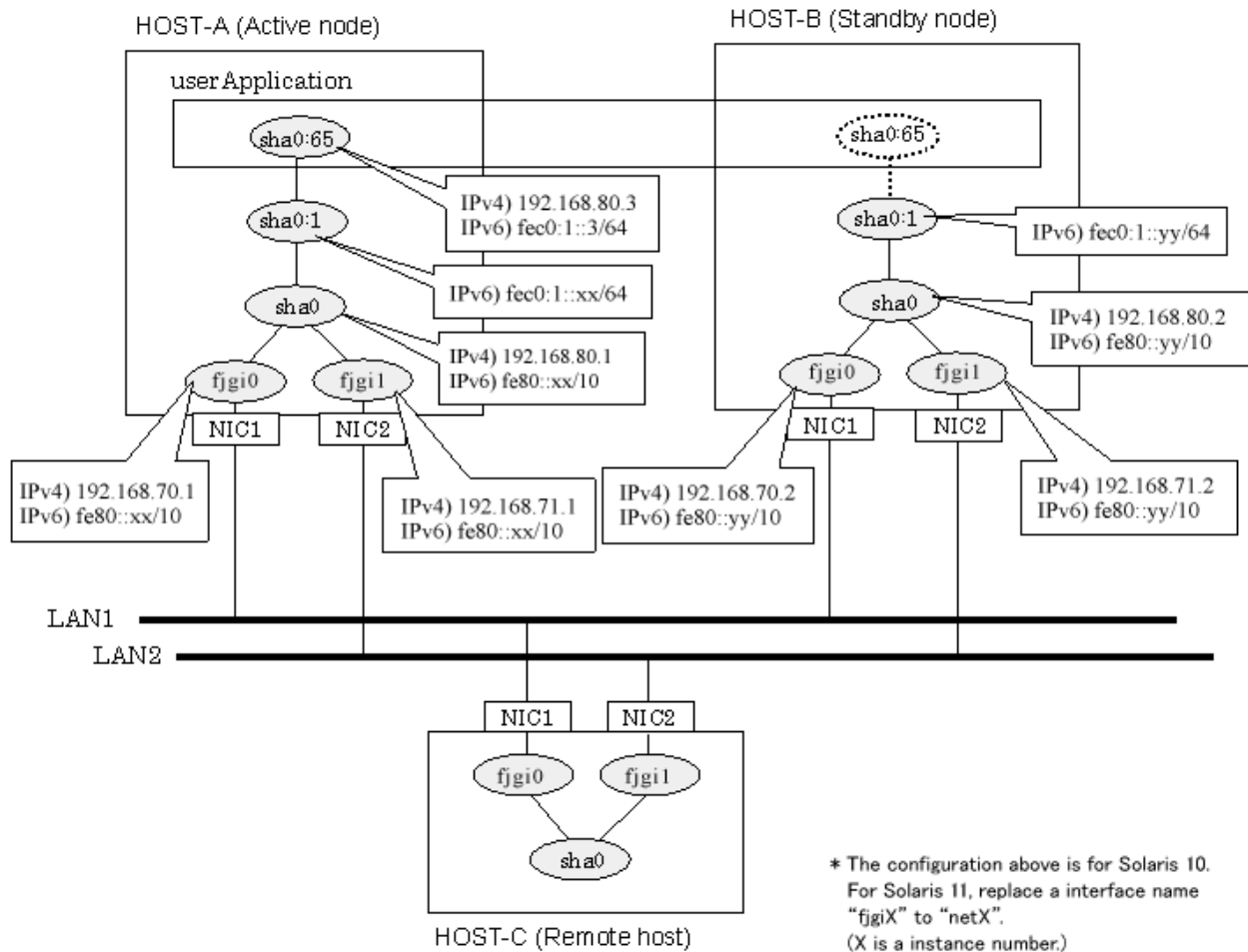
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.3    hosta1 # Takeover virtual IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::3      v6hosta1 # Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3, fec0:1::3/64
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.


```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgil  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3, fec0:1::3/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.3 - fec0:1::3".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.5 Example of the Cluster system (Mutual standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

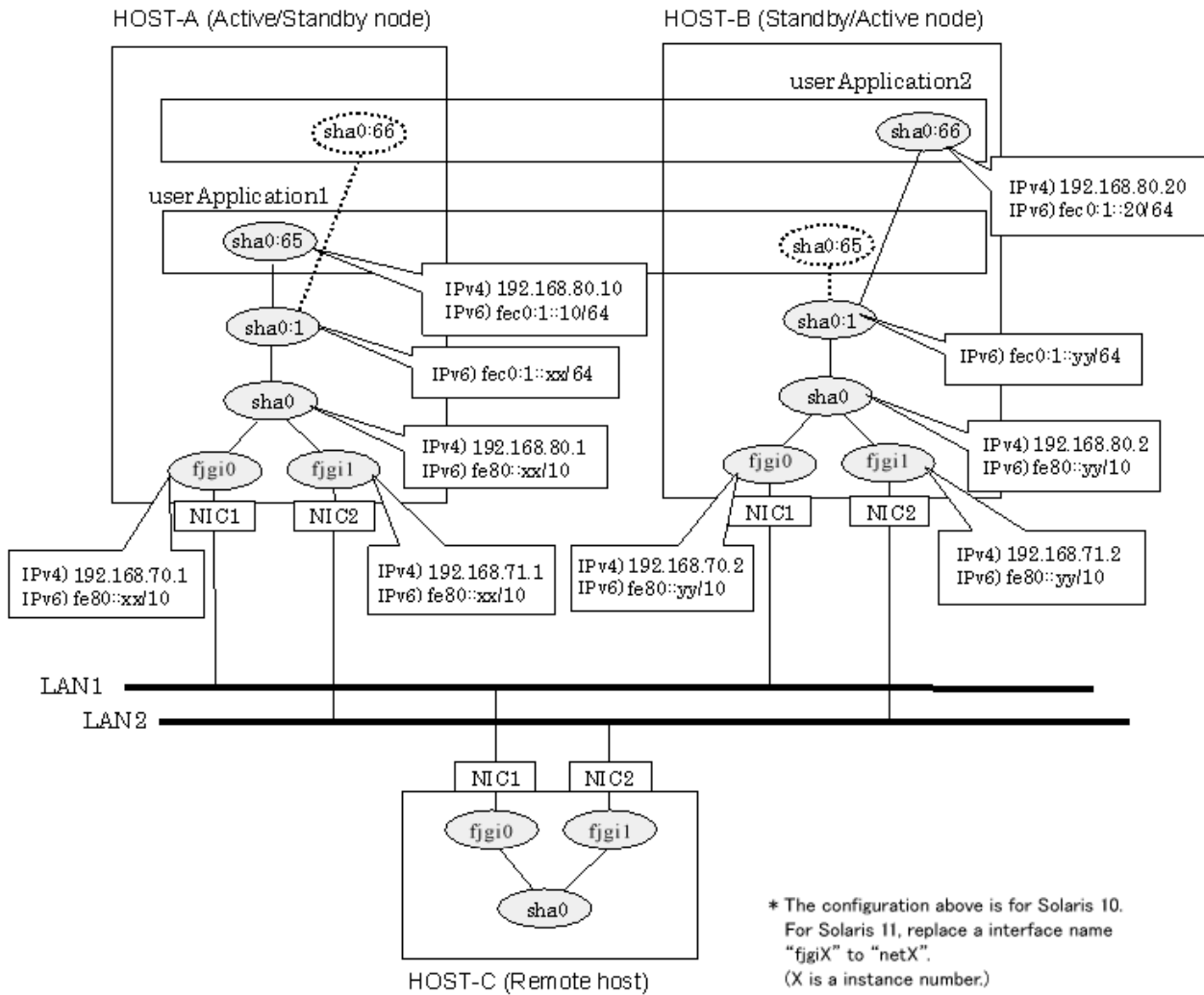
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.10  hosta1 # Takeover virtual IP (1)
192.168.80.20  hostb1 # Takeover virtual IP (2)

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```

host11

```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10     v6hosta1 # Takeover virtual IP (1)
fec0:1::20     v6hostb1 # Takeover virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10, fec0:1::10/64
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20, fec0:1::20/64
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10, fec0:1::10/64
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20, fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.10 - fec0:1::10" and "192.168.80.20 - fec0:1::20".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.6 Example of the Cluster system (N:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The values for xx, yy and zz in the IP address of the figure below are assigned automatically by the automatic address configuration.

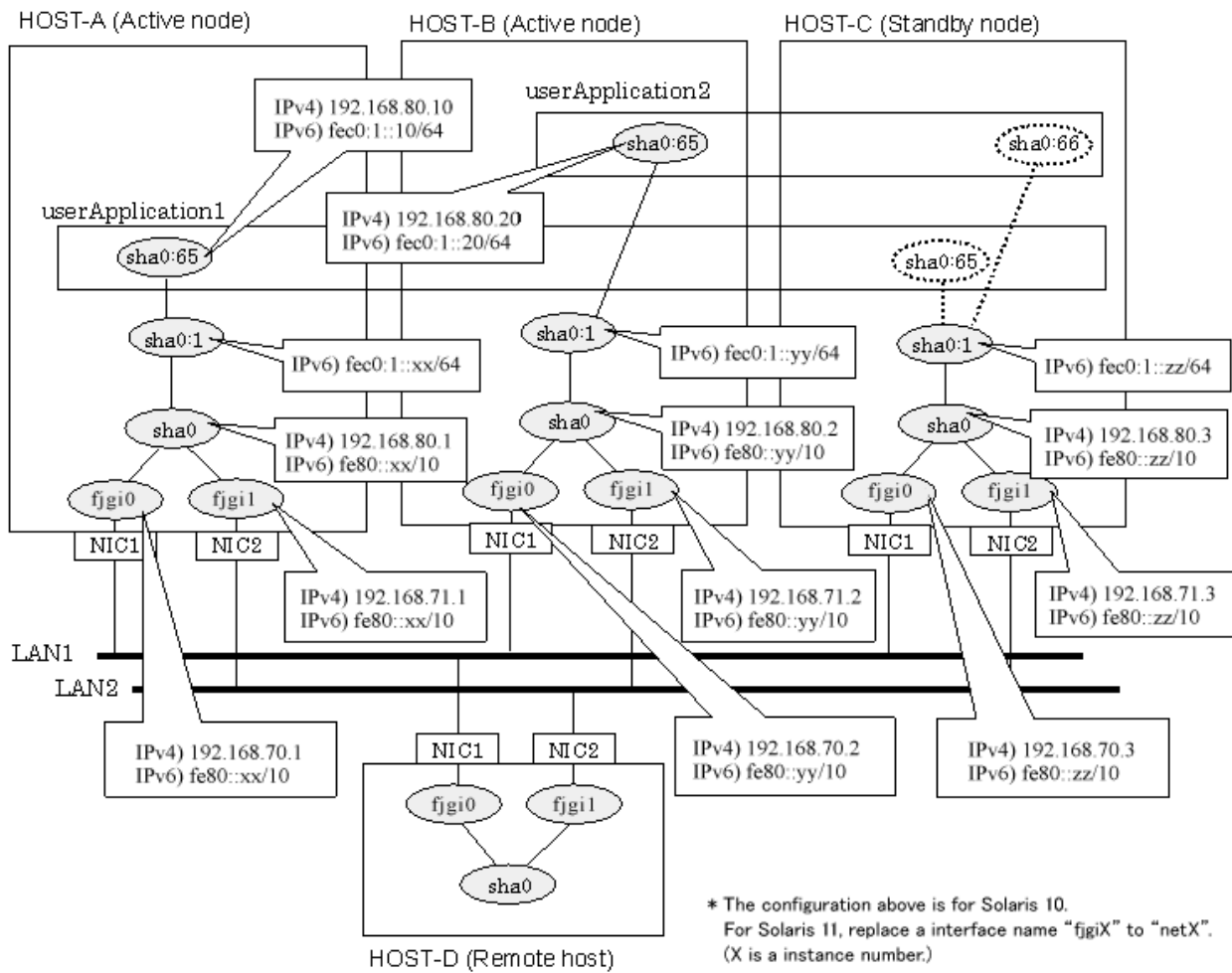
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1      host11 # HOST-A Physical IP (1)
192.168.71.1     host12 # HOST-A Physical IP (2)
192.168.80.1     hosta  # HOST-A Virtual IP
192.168.70.2     host21 # HOST-B Physical IP (1)
192.168.71.2     host22 # HOST-B Physical IP (2)
192.168.80.2     hostb  # HOST-B Virtual IP
192.168.70.3     host31 # HOST-C Physical IP (1)
192.168.71.3     host32 # HOST-C Physical IP (2)
192.168.80.3     hostc  # HOST-C Virtual IP
192.168.80.10    hosta1 # Takeover virtual IP (1)
192.168.80.20    hostb1 # Takeover virtual IP (2)

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::10      v6hosta1 # Takeover virtual IP (1)
fec0:1::20      v6hostb1 # Takeover virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgil
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10, fec0:1::10/64
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```


- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20, fec0:1::20/64
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host31
```

- Contents of /etc/hostname.fjgi1

```
host32
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host32/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10, fec0:1::10/64
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20, fec0:1::20/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of HOST-A, HOST-B, and HOST-C connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.10 - fec0:1::10" and "192.168.80.20 - fec0:1::20".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.3.7 Example of the Cluster system (Cascade)

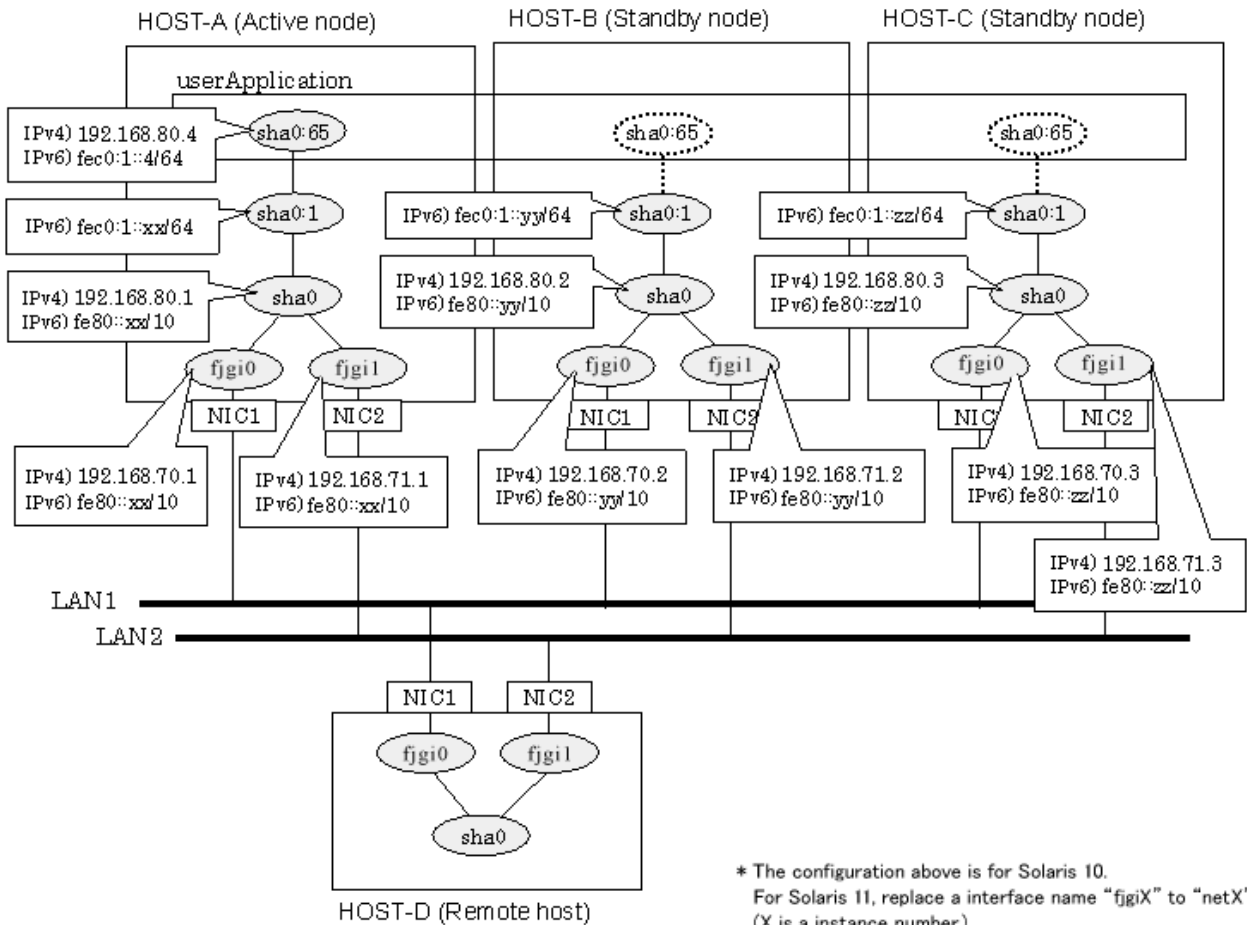
This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.
 In this section, description of private LAN is omitted.
 The dotted line indicates that the interface is inactive.

 **Note**

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Physical IP (1)
192.168.71.1    host12 # HOST-A Physical IP (2)
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP (1)
192.168.71.2    host22 # HOST-B Physical IP (2)
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP (1)
192.168.71.3    host32 # HOST-C Physical IP (2)
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.4    hosta1 # Takeover virtual IP
  
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::4      v6hosta1    # Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4,fec0:1::4/64
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1  
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1  
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4, fec0:1::4/64
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host31
```

- Contents of /etc/hostname.fjgi1

```
host32
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host32/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

1-6) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4, fec0:1::4/64
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 4) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.4 - fec0:1::4".

2) Starting of userApplication

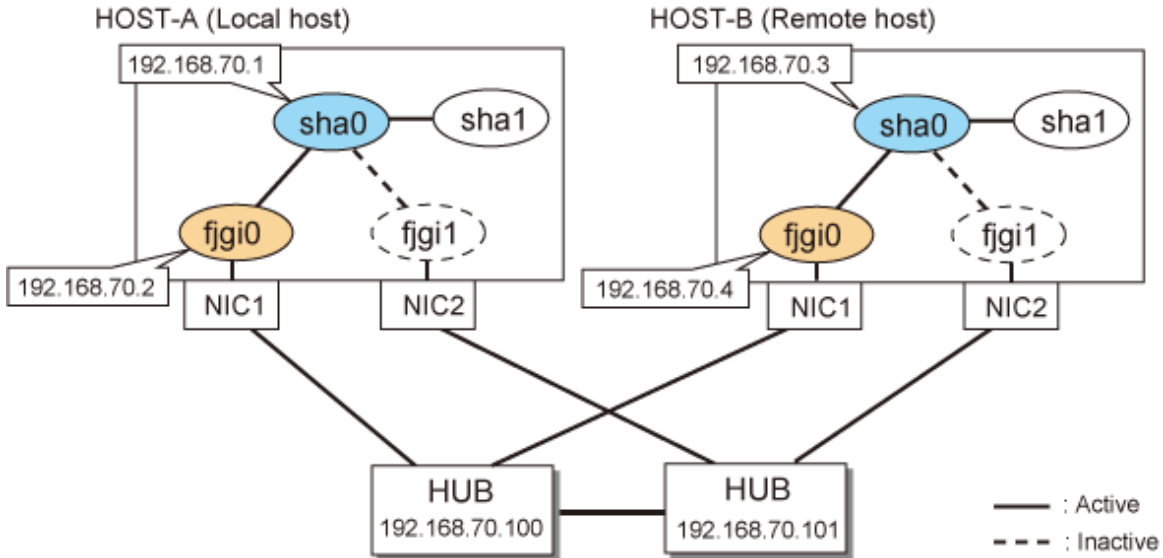
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4 Example of configuring NIC switching mode (IPv4)

B.4.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    hostb    # HOST-B Virtual IP
192.168.70.4    host21   # HOST-B Physical IP
192.168.70.100  swhub1  # Primary HUB IP
192.168.70.101  swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.


```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t
fjgi0,fjgi1
```

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

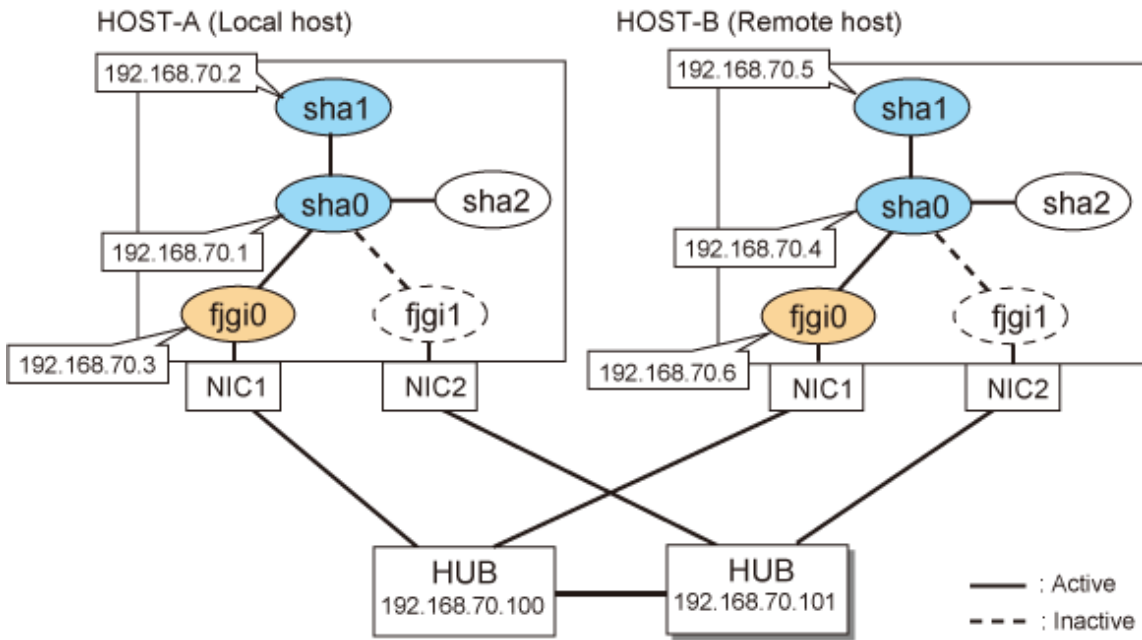
7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

B.4.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta1 # HOST-A Virtual IP (1)
192.168.70.2    hosta2 # HOST-A Virtual IP (2)
192.168.70.3    host11 # HOST-A Physical IP
192.168.70.4    hostb1 # HOST-B Virtual IP (1)
192.168.70.5    hostb2 # HOST-B Virtual IP (2)
192.168.70.6    host21 # HOST-B Physical IP
192.168.70.100  swhub1 # Primary HUB IP
192.168.70.101  swhub2 # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(IM) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t
fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.5
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t
net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.5
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

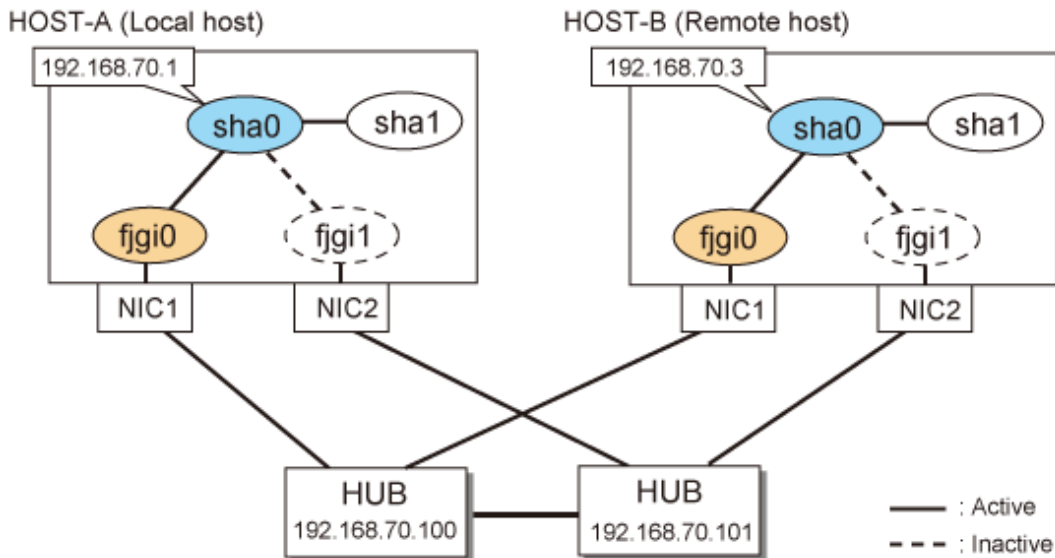
7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

B.4.3 Example of the Single system in Physical IP address takeover function

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    hostb    # HOST-B Virtual IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hosta
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hosta/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net0,net1
```



Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.fjgi0 with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
hostb
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostb/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t net0,net1
```



Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.fjgi0 with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

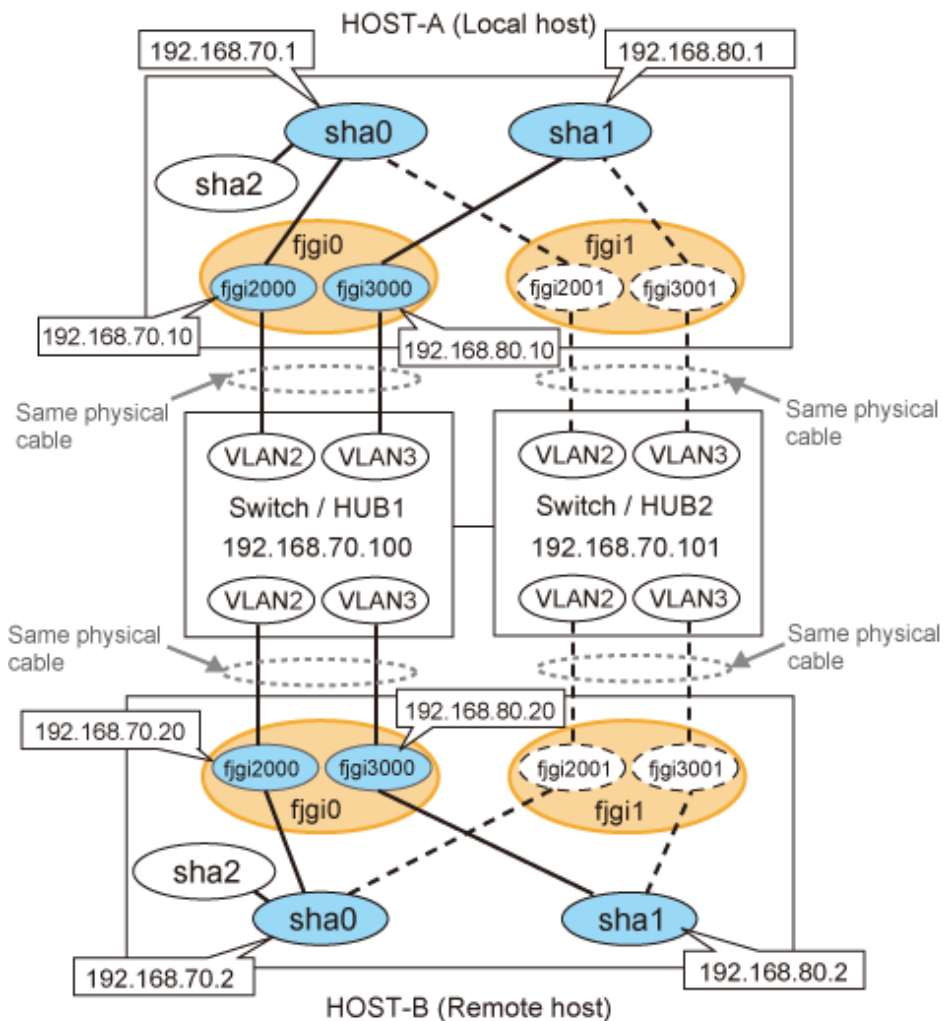
```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

B.4.4 Configuring virtual interfaces with tagged VLAN (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.10  host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.10  host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
192.168.70.20  host72   # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2    hostd    # HOST-B Virtual IP
192.168.80.20  host82   # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100  swhub1   # Primary Switchi/HUB IP
192.168.70.101  swhub2   # Secondary Switch/HUB IP

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3000 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host71
```

- Contents of /etc/hostname.fjgi3000

```
host81
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host71/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a host81/24 net3000/v4
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
fjgi2000,fjgi2001
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
net2000,net2001
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3000, or with the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the ifconfig command after rebooting the system: fjgi2000 and fjgi3000 for Solaris 10; net2000 and net3000 for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3000 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host72
```

- Contents of /etc/hostname.fjgi3000

```
host82
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l neti0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host72/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a host82/24 net3000/v4
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, /etc/hostname.fjgi3000, or with the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

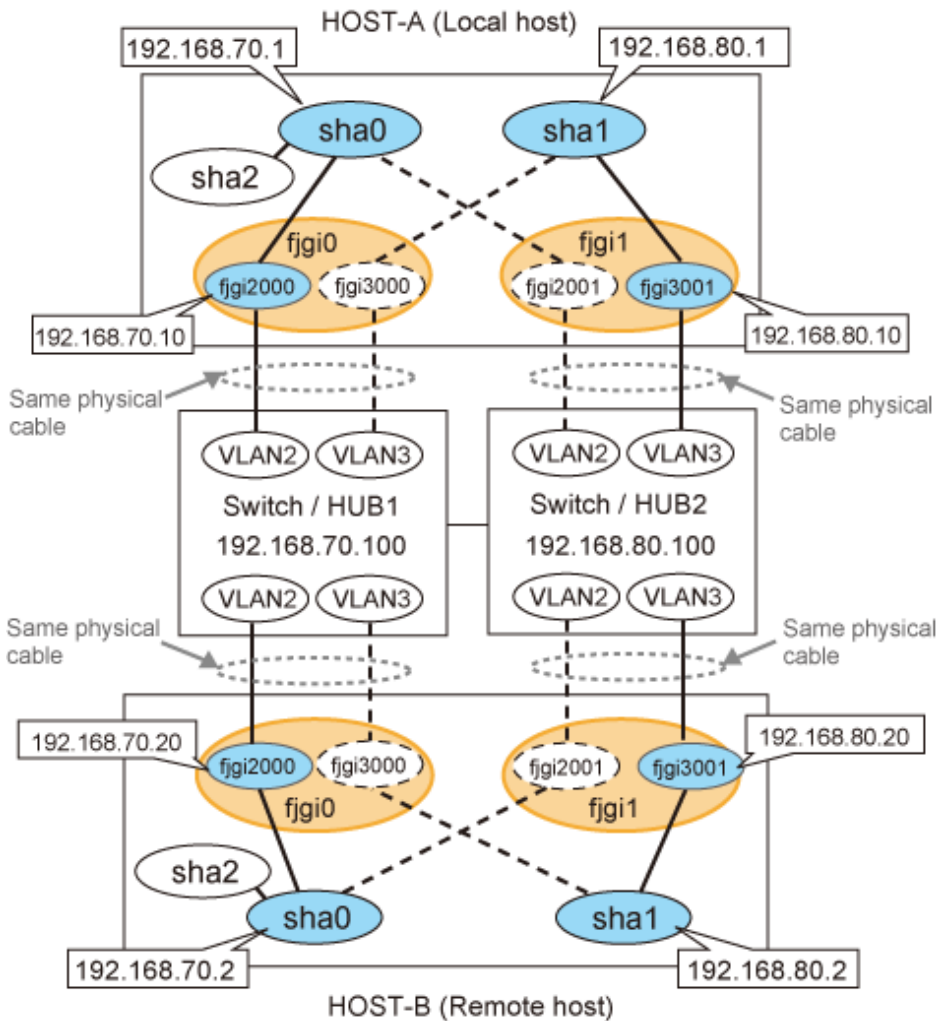
6) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the ifconfig command after rebooting the system: fjgi2000 and fjgi3000 for Solaris 10; net2000 and net3000 for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

B.4.5 Configuring virtual interfaces with tagged VLAN (asynchronous switching)

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.10  host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.10  host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
192.168.70.20  host72   # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2    hostd    # HOST-B Virtual IP
192.168.80.20  host82   # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100  swhub1   # Switch/HUB1 IP
192.168.80.100  swhub2   # Switch/HUB2 IP

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3001 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host71
```

- Contents of /etc/hostname.fjgi3001

```
host81
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host71/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T static -a host81/24 net3001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
net3001,net3000
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3001, or with the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

5) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the ifconfig command after rebooting the system: fjgi2000 and fjgi3001 for Solaris 10; net2000 and net3001 for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3001 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host72
```

- Contents of /etc/hostname.fjgi3001

```
host82
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host72/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T static -a host82/24 net3001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
net3001,net3000
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3001, or with the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

5) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the ifconfig command after rebooting the system: fjgi2000 and fjgi3001 for Solaris 10; net2000 and net3001 for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

B.4.6 Example of the Cluster system (1:1 Standby)

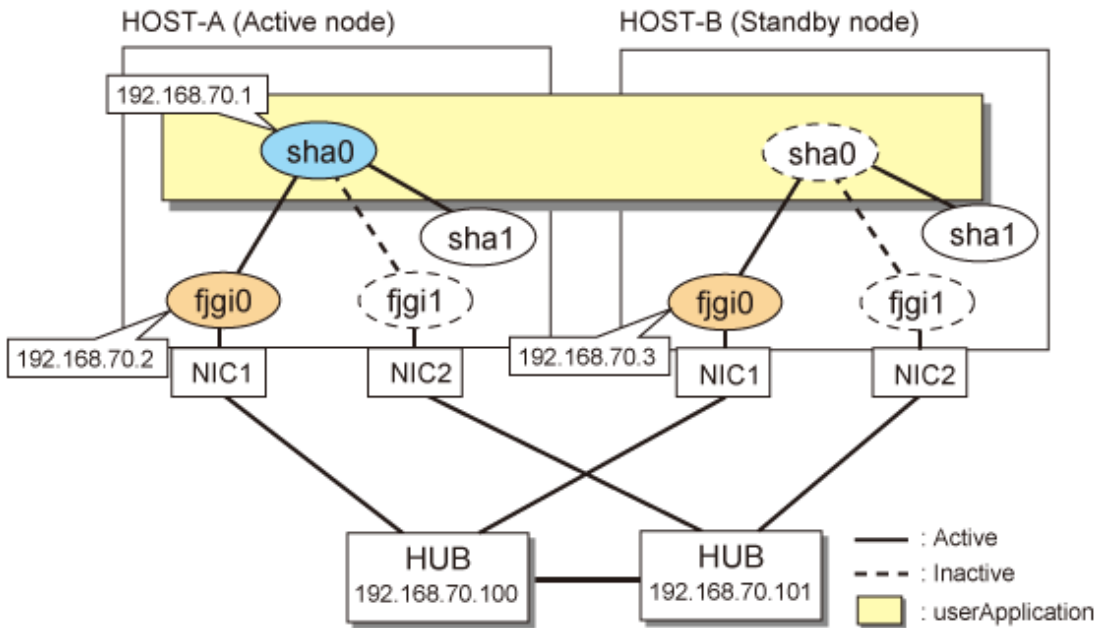
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX."
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100  swhub1  # Primary HUB IP
192.168.70.101  swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t  
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t  
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GLs resource, select the SysNode for HOST-A and HOST-B. Once GLs is created, register it on the userApplication.
 When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4.7 Example of the Cluster system (Mutual standby) without NIC sharing

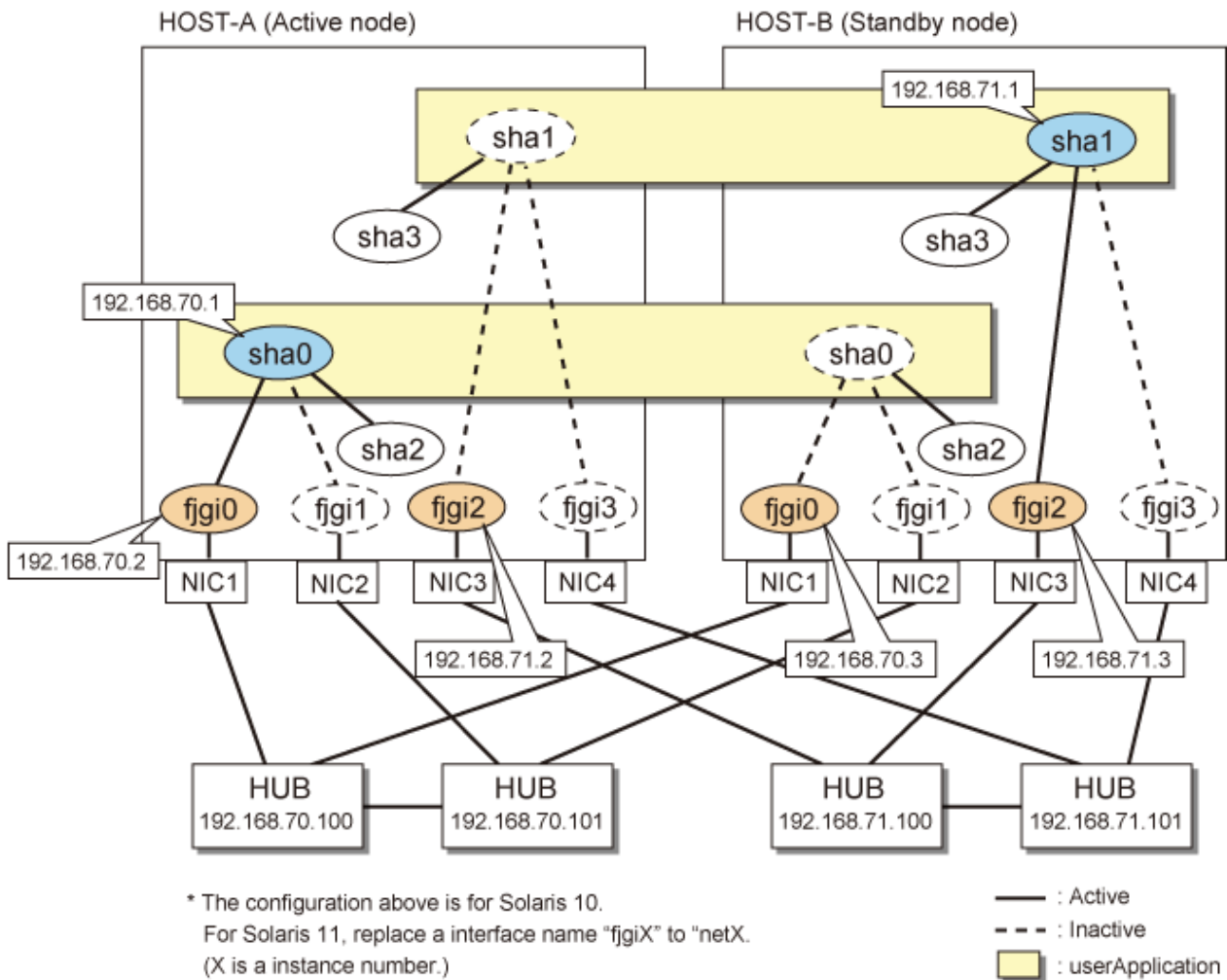
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address1)
192.168.70.2    host11   # HOST-A Physical IP (1)
192.168.70.3    host21   # HOST-B Physical IP (1)
192.168.71.1    hostb    # HOST-A/B Virtual IP (Take over IP address2)
  
```

```
192.168.71.2    host12 # HOST-A Physical IP (2)
192.168.71.3    host22 # HOST-B Physical IP (2)
192.168.70.100  swhub1 # Primary HUB IP (1)
192.168.70.101  swhub2 # Secondary HUB IP (1)
192.168.71.100  swhub3 # Primary HUB IP (2)
192.168.71.101  swhub4 # Secondary HUB IP (2)
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi2 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi2

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2
# /usr/sbin/ipadm create-addr -T static -a host12/24 net2/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t
fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t
net2,net3
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0, in /etc/hostname.fjgi2, or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi2 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi2

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2
# /usr/sbin/ipadm create-addr -T static -a host22/24 net2/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t
fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t
net2,net3
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0, in /etc/hostname.fjgi2, or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1" and "192.168.71.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4.8 Example of the Cluster system (Mutual standby) with NIC sharing

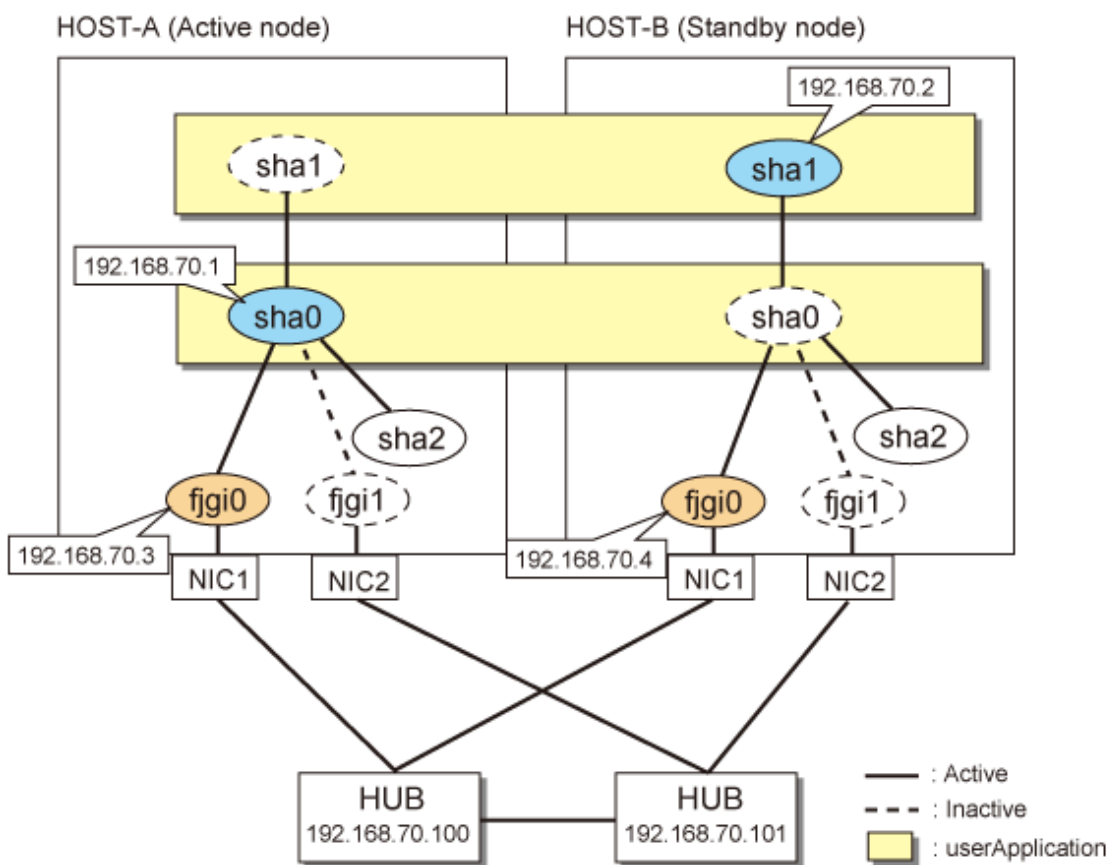
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.


```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address1)
192.168.70.2    hostb    # HOST-A/B Virtual IP (Take over IP address2)
192.168.70.3    host11   # HOST-A Physical IP
192.168.70.4    host21   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgil
# /opt/FJShanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
# /opt/FJShanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJShanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0  
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t  
fjgi0,fjgil  
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t  
net0,net1  
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1" and "192.168.70.2".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4.9 Example of the Cluster system in Physical IP address takeover function I

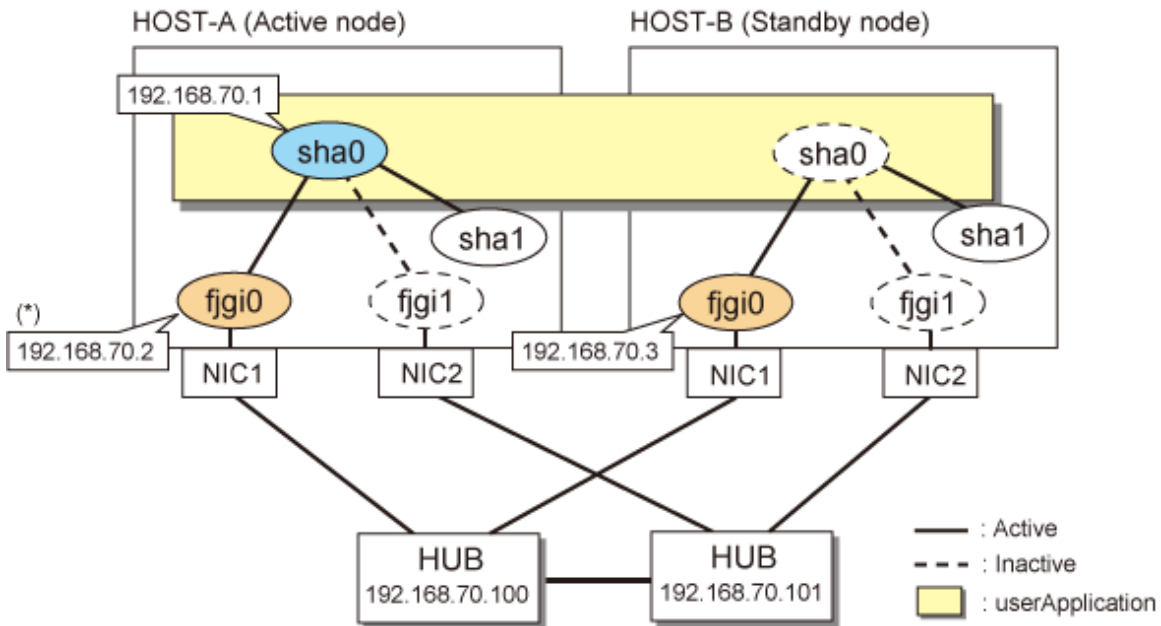
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for enabling physical interface on a standby node.)

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



*) Physical IP address (192.168.70.2) is inactivated when takeover IP address (192.168.70.1) is activated.

* The configuration above is for Solaris 10. For Solaris 11, replace a interface name "fjgiX" to "netX". (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100  swhub1  # Primary HUB IP
192.168.70.101  swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.2 -t  
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.2 -t  
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4.10 Example of the Cluster system in Physical IP address takeover function II

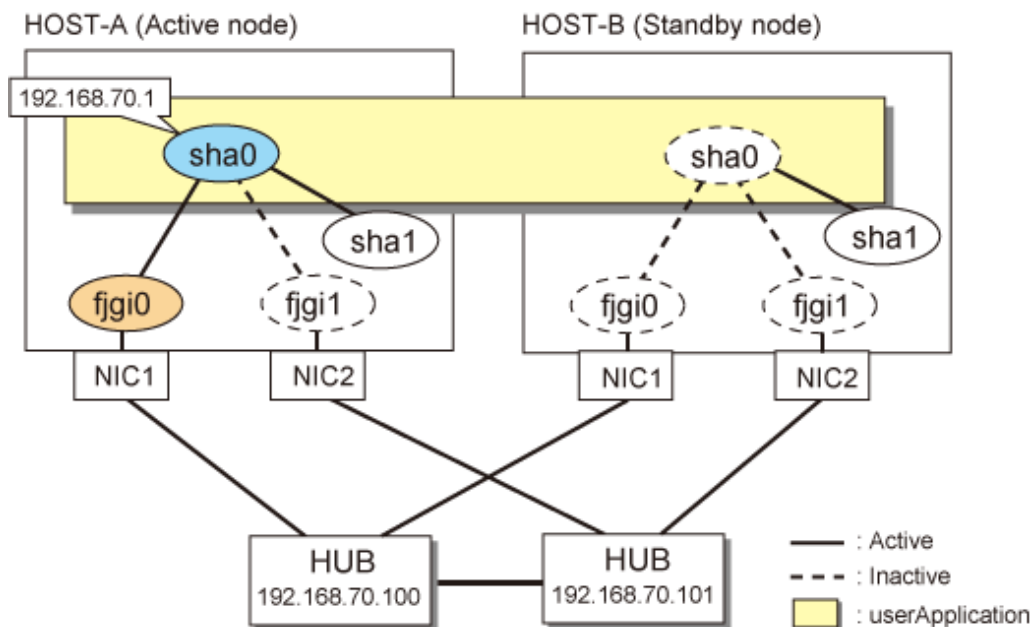
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for not enabling physical interface on a standby node.)

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 4) and 7) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address)
192.168.70.100  swhub1  # Primary HUB IP
192.168.70.101  swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Check that nothing is written in /etc/hostname.fjgi0 file.

- Contents of /etc/hostname.fjgi0

1-2) For Solaris 11 or later

Check that no IP address is set in the interface used with the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm show-addr net0
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t fjgi0,fjgil
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net0,net1
```



Note

For Solaris 10, create /etc/hostname.fjgi0 as an empty file.

If the physical IP address (take over IP address) is written in /etc/hostname.fjgi0 to be specified for the option 'i', IP addresses may duplicate when switching the cluster.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

4) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

7) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Check that nothing is written in /etc/hostname.fjgi0 file. Defined information is the same as for HOST-A.

1-2) For Solaris 11 or later

Check that no IP address is set in the interface used with the ipadm(1M) command.

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t fjgi0,fjgil
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net0,net1
```



Note

For Solaris 10, create /etc/hostname.fjgi0 as an empty file.

If the physical IP address (take over IP address) is written in /etc/hostname.fjgi0 to be specified for the option 'i', IP addresses may duplicate when switching the cluster.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

4) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

7) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 7) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.4.11 Example of the Cluster system (Cascade)

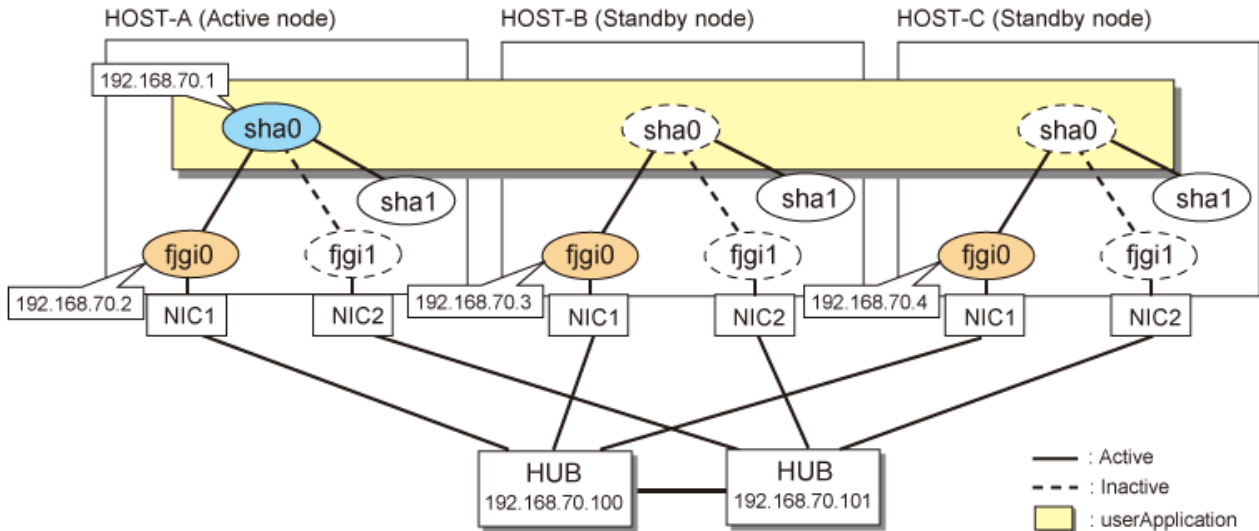
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B/C Virtual IP (Take over IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.4    host31   # HOST-C Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
Host31
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 8) of both HOST-B and HOST-C, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

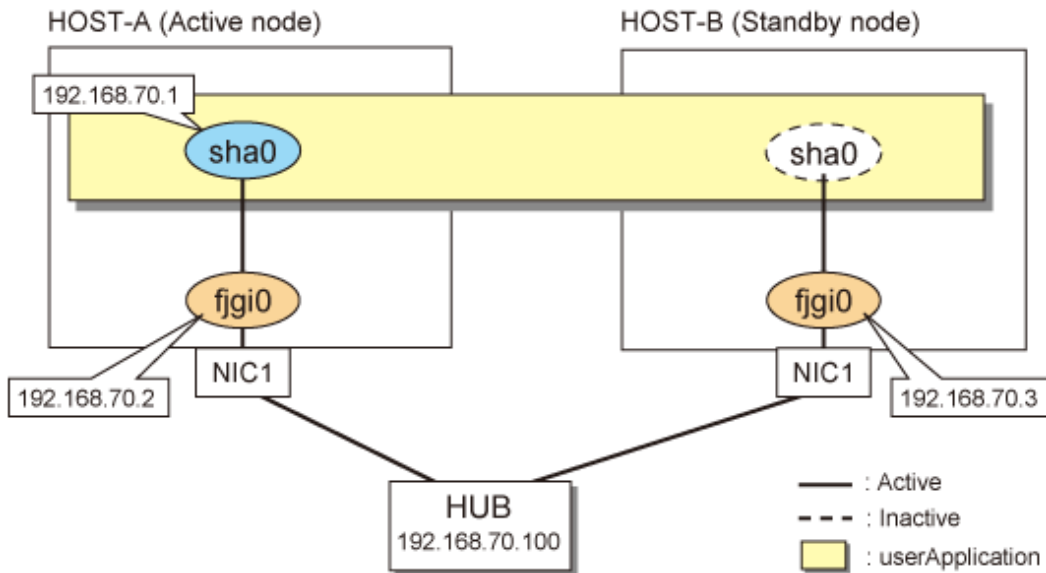
B.4.12 Example of the Cluster system (NIC non-redundant)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
fjgi0
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
net0
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
```

5) Creation of takeover virtual interface

```
# /opt/FJShanet/usr/sbin/hanethvrsc create -n sha0
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
```

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```


6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[Configuration by RMS Wizard]

1) Configuration of userApplication

After completing step 6) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

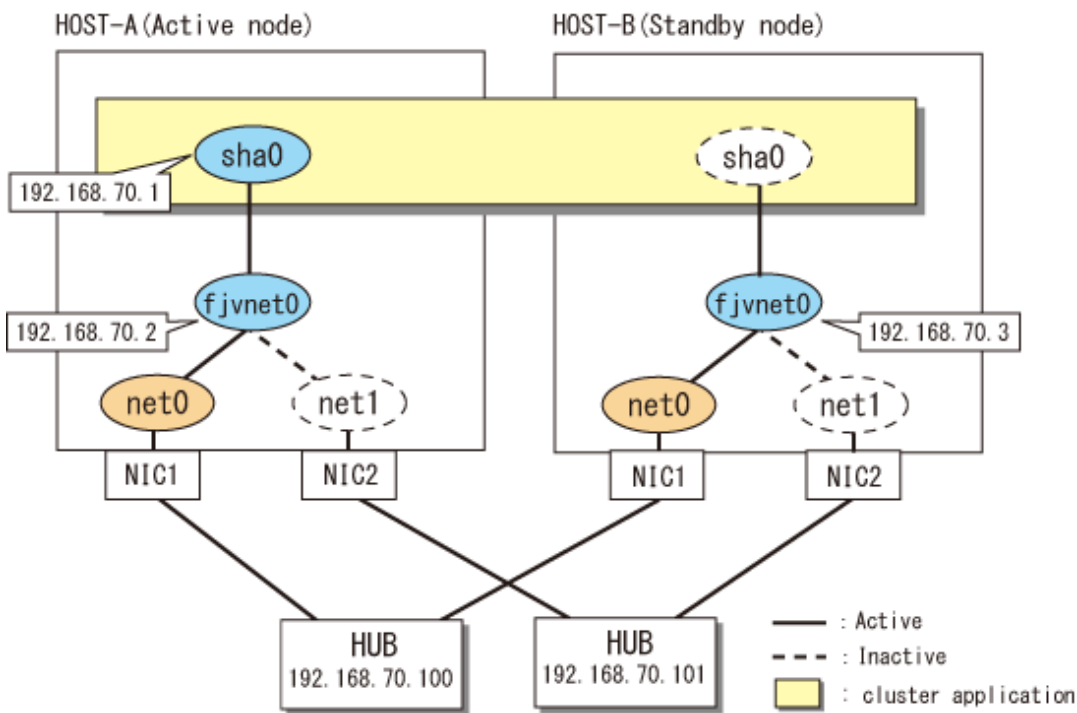
B.4.13 Example of the Cluster system (Virtual NIC)

This section describes an example configuration procedure of the network shown in the diagram below. However, this manual only supports Solaris 11.1 or later environment.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
```

```
192.168.70.100 swhub1 # Primary HUB IP
192.168.70.101 swhub2 # Secondary HUB IP
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0 255.255.255.0
```

2) Creation of virtual NIC

2-1) Create virtual NIC using rvnetadm create command.

```
# /opt/FJSVrvnet/bin/rvnetadm create -n fjvnet0 -i net0,net1
```

2-2) Use rvnetadm start-observ command and enable network monitoring function of virtual NIC.

```
# /opt/FJSVrvnet/bin/rvnetadm start-observ
```

2-3) Set the host by the virtual NIC used with the ipadm(1M) command and also by the host name defined above.

```
# /usr/sbin/ipadm create-ip fjvnet0
# /usr/sbin/ipadm create-addr -T static -a host11/24 fjvnet0/v4
```

3) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2
-t fjvnet0
```



Ensure that the physical IP address specified using option '-e' is the same physical IP address configured with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101
```

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual NIC

2-1) Create virtual NIC using rvnetadm create command.

```
# /opt/FJSVrvnet/bin/rvnetadm create -n fjvnet0 -i net0,net1
```

2-2) Use `rvnetadm start-observ` command and enable network monitoring function of virtual NIC.

```
# /opt/FJSVrvnet/bin/rvnetadm start-observ
```

2-3) Set the host by the virtual NIC used with the `ipadm(1M)` command and also by the host name defined above.

```
# /usr/sbin/ipadm create-ip fjvnet0
# /usr/sbin/ipadm create-addr -T static -a host21/24 fjvnet0/v4
```

3) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3
-t fjvnet0
```



Ensure that the physical IP address specified using option '-e' is the same physical IP address configured with the `ipadm(1M)` command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101
```

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[Configuration by RMS Wizard]

1) Configuration of cluster environment

After completing step 6) of both HOST-A and HOST-B, connect to the administration server using RMS Wizard, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the cluster application.

When registering on the cluster application, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1".

2) Starting cluster application

After completing the configuration, start the cluster application to activate the takeover virtual interface on the operation node.

B.5 Example of configuring NIC switching mode (IPv6)

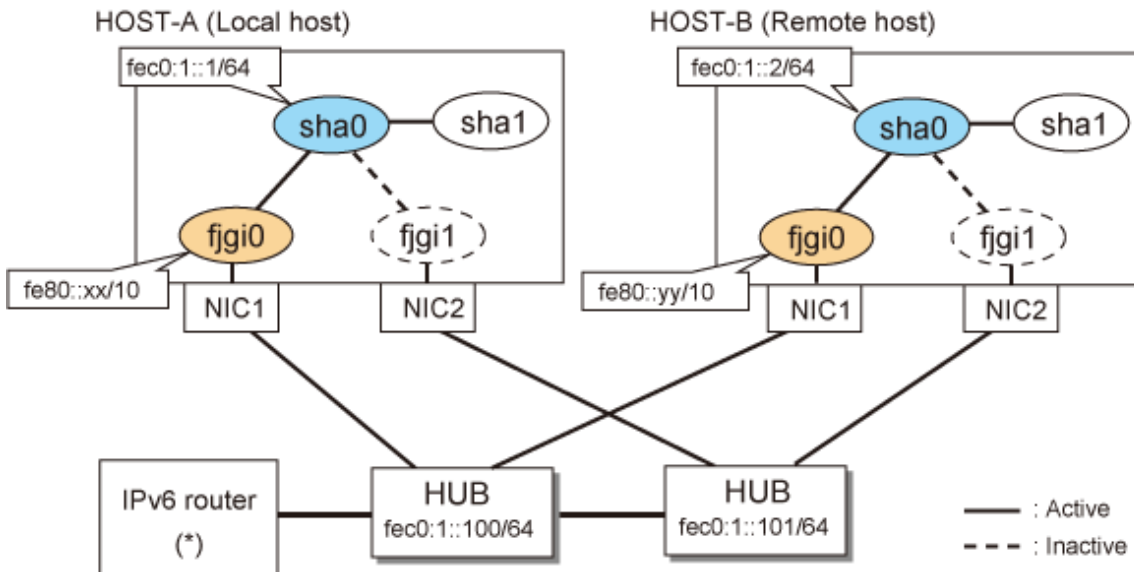
When using IPv6 address, it is required to set an IPv6 router on the same network. Also, specify the same prefix and prefix length of IPv6 address for redundant control line function configured in the IPv6 router.

B.5.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring `/etc/inet/ndpd.conf` to use Solaris server as an IPv6 router is described below:
For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0            # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

- 1-1) For Solaris 10

Create `/etc/hostname6.fjgi0` file as an empty file.

- 1-1) For Solaris 11 or later

Set the interface to be used by using the `ipadm(1M)` command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- 1-2) Define IP addresses and hostnames in `/etc/inet/ipnodes` file.

```
fec0:1::1      v6hosta      # HOST-A Virtual IP
fec0:1::2      v6hostb      # HOST-B Virtual IP
```

```
fec0:1::100    swhub1      # Primary HUB IP
fec0:1::101    swhub2      # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

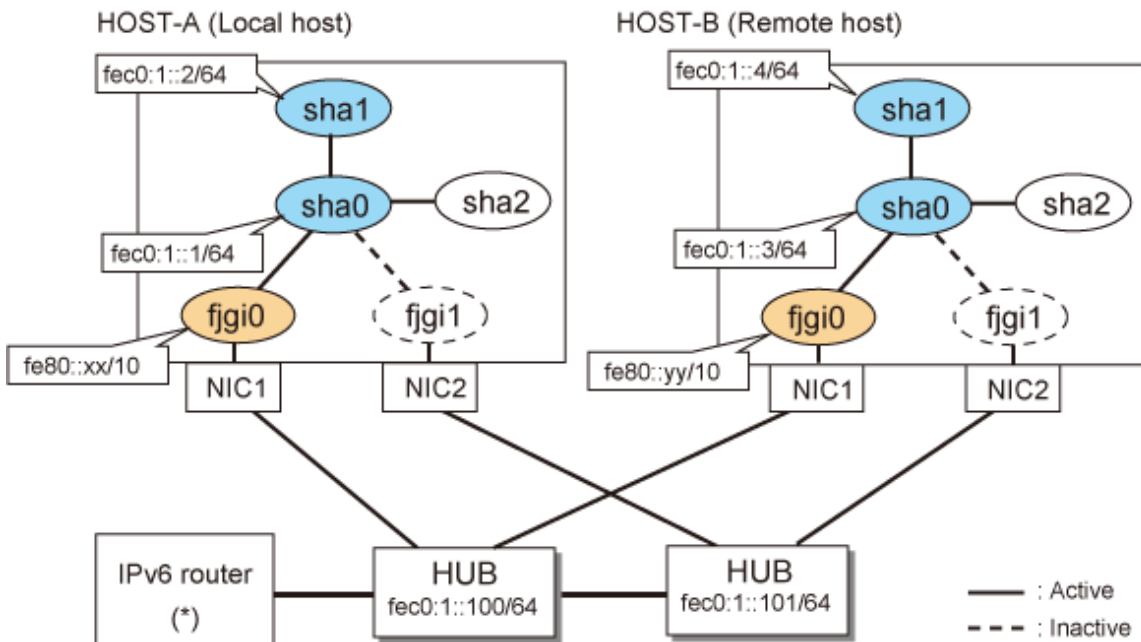
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

B.5.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64"
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64"
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta1 # HOST-A Virtual IP (1)  
fec0:1::2 v6hosta2 # HOST-A Virtual IP (2)  
fec0:1::3 v6hostb1 # HOST-B Virtual IP (1)  
fec0:1::4 v6hostb2 # HOST-B Virtual IP (2)  
fec0:1::100 swhub1 # Primary HUB IP  
fec0:1::101 swhub2 # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1  
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1  
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```


6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

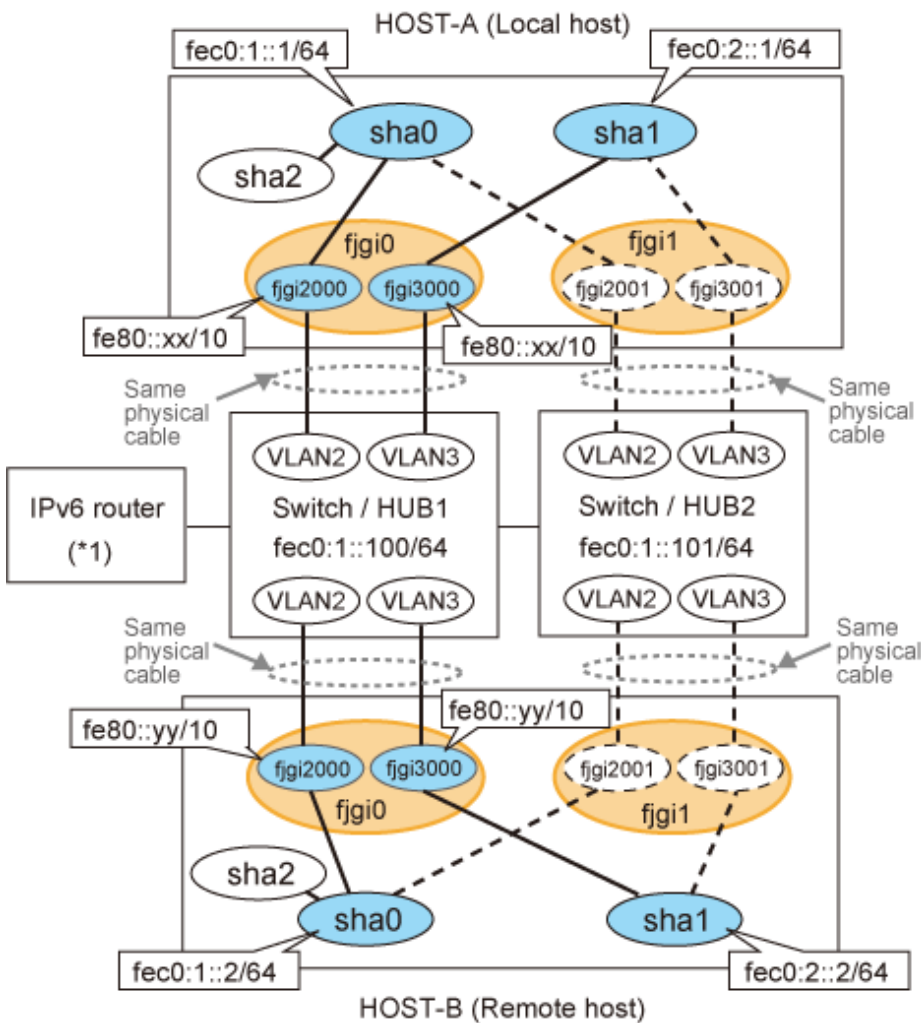
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

B.5.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

Note

An example of configuring `/etc/inet/ndpd.conf` to use Solaris server as an IPv6 router is described below:
For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi2000 # fjgi2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi3000 # fjgi3000 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net2000 # net2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net3000 # net3000 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create `/etc/hostname6.fjgi2000` and `/etc/hostname6.fjgi3000` file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the `dladm(1M)` command and the `ipadm(1M)` command.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-2) Define IP addresses and hostnames in `/etc/inet/ipnodes` file.

```
fec0:1::1 v6hosta1 # HOST-A Virtual IP(1)
fec0:2::1 v6hosta2 # HOST-A Virtual IP(2)
fec0:1::2 v6hostb1 # HOST-B Virtual IP(1)
fec0:2::2 v6hostb2 # HOST-B Virtual IP(2)
fec0:1::100 swhub1 # primary HUB IP
fec0:1::101 swhub2 # secondary HUB IP
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t
net3000,net3001
```

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3000 for Solaris 10, net2000 and net 3000 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjgi3000 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the dladm(1M) command and the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t  
fjgi2000,fjgi2001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t  
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t  
net2000,net2001  
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t  
net3000,net3001
```

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3000 for Solaris 10, net2000 and net 3000 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

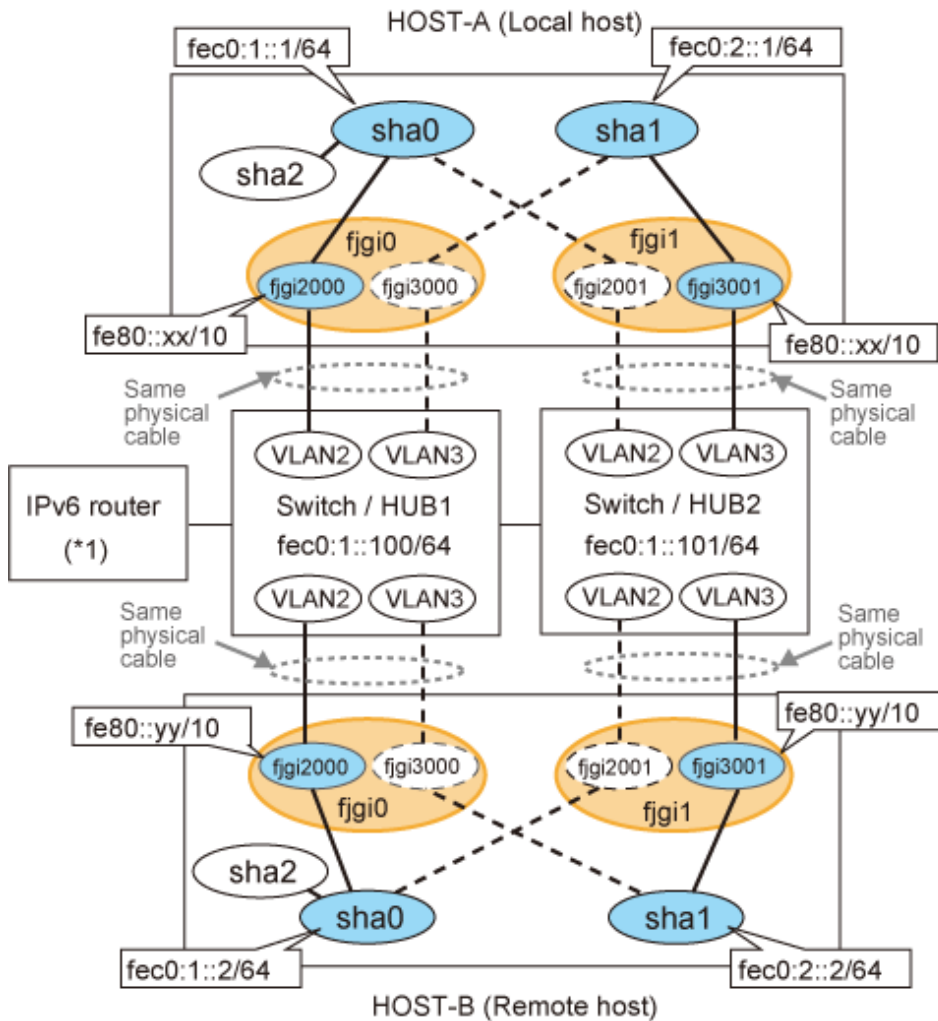
```
# /usr/sbin/shutdown -y -i6 -g0
```

B.5.4 Configuring virtual interfaces with tagged VLAN (asynchronous switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 4) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
 For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi2000 # fjgi2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi3001 # fjgi3001 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net2000 # net2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net3001 # net3001 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjgi3001 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the dladm(1M) command and the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T addrconf net3001/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1    # HOST-A Virtual IP(1)
fec0:2::1      v6hosta2    # HOST-A Virtual IP(2)
fec0:1::2      v6hostb1    # HOST-B Virtual IP(1)
fec0:2::2      v6hostB2    # HOST-B Virtual IP(2)
fec0:1::100    swhub1      # Switch/HUB1 IP
fec0:2::100    swhub2      # Switch/HUB2 IP
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t
net3001,net3000
```

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100 -b off
```

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

5) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3001 for Solaris 10, net2000 and net 3001 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjgi3001 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the dladm(1M) command and the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T addrconf net3001/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t
net3001,net3000
```

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100 -b off
```

4) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

5) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3001 for Solaris 10, net2000 and net 3001 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

B.5.5 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

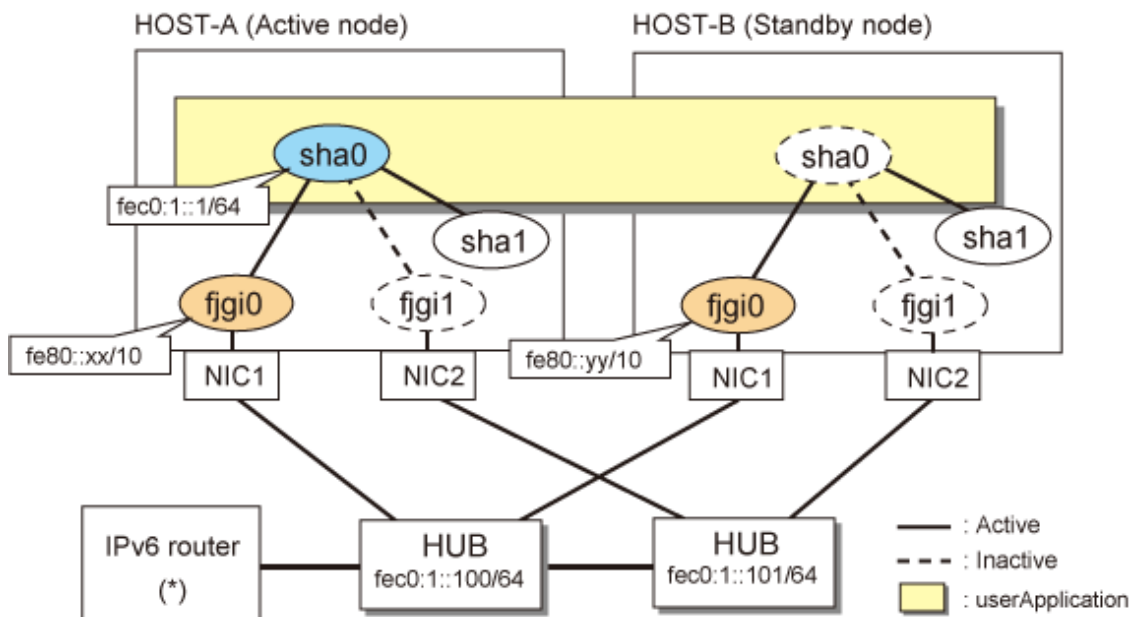
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta # HOST-A/B Takeover virtual IP
fec0:1::100 swhub1 # Primary HUB IP
fec0:1::101 swhub2 # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resource, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.5.6 Example of the Cluster system (Mutual standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

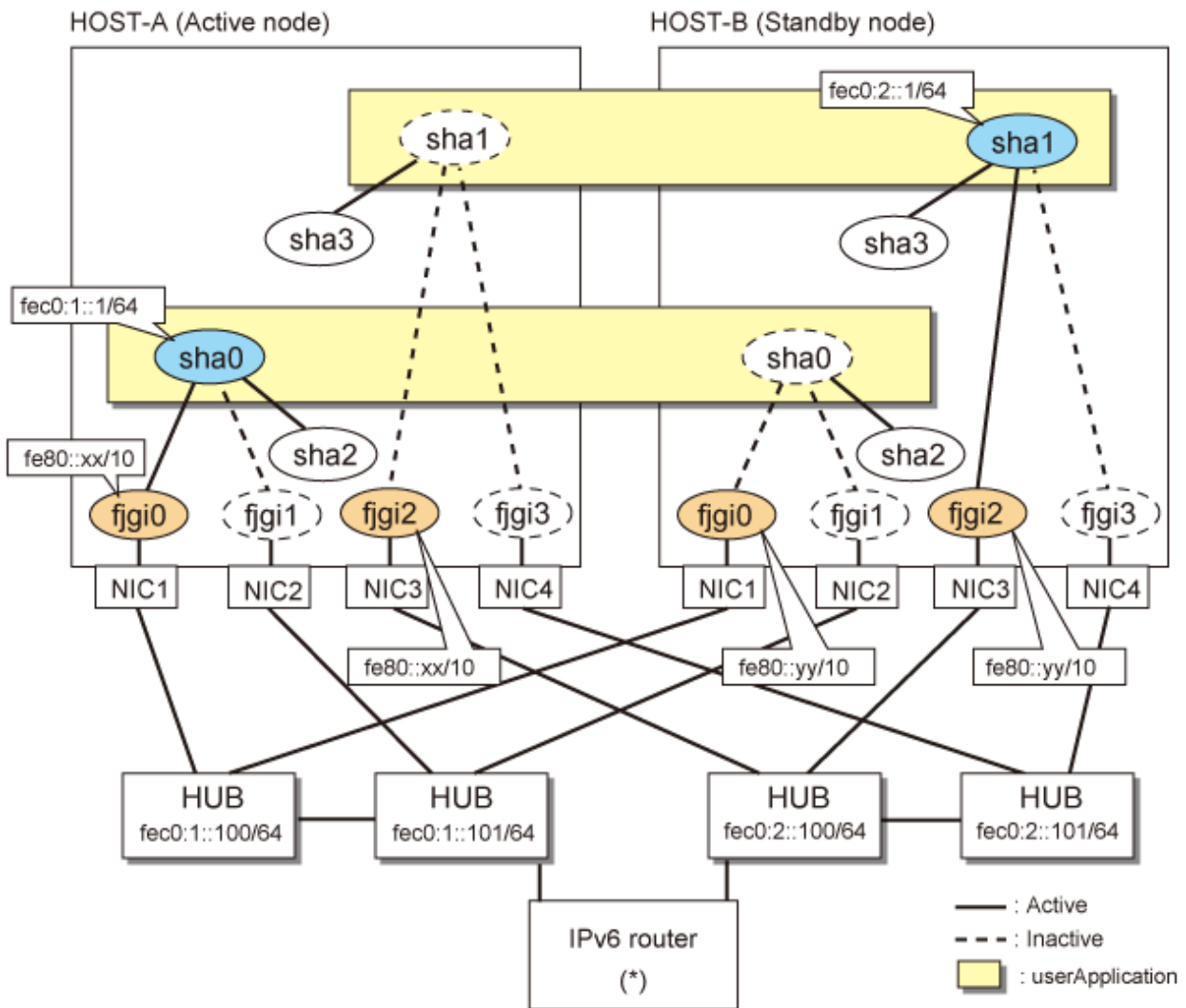
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.



Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX."
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
 For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2           # fjgi2 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0             # net0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net2             # net2 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi2 files as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2
# /usr/sbin/ipadm create-addr -T addrconf net2/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta      # HOST-A/B Takeover virtual IP (1)
fec0:1::100    swhub1       # Primary HUB IP (1)
fec0:1::101    swhub2       # Secondary HUB IP (1)
fec0:2::1      v6hostb      # HOST-A/B Takeover virtual IP (2)
fec0:2::100    swhub3       # Primary HUB IP (2)
fec0:2::101    swhub4       # Secondary HUB IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t net2,net3
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100,fec0:2::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi2 files as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2
# /usr/sbin/ipadm create-addr -T addrconf net2/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t net2,net3
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p fec0:2::100,fec0:2::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1" and "fec0:2::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.5.7 Example of the Cluster system (Mutual standby) with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

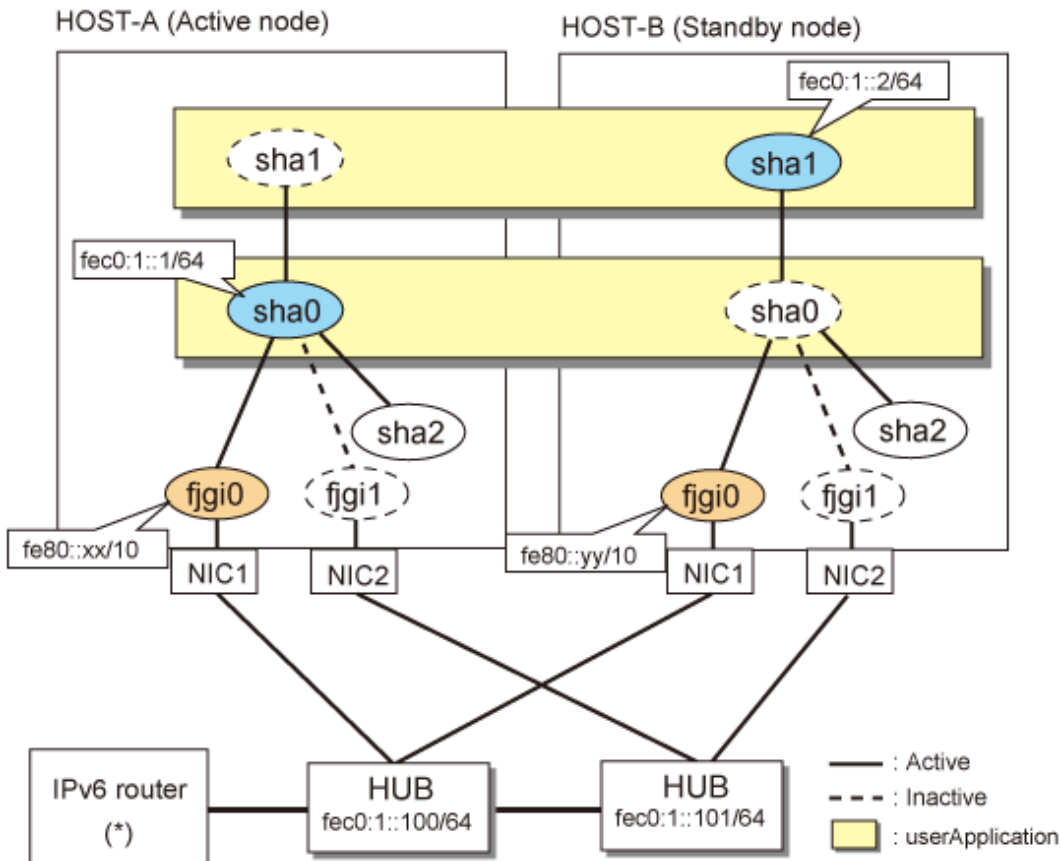
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX."
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
 For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta      # HOST-A/B Takeover virtual IP (1)
fec0:1::2      v6hostb      # HOST-A/B Takeover virtual IP (2)
fec0:1::100    swhub1       # Primary HUB IP
fec0:1::101    swhub2       # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,shal
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n shal
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,shal
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n shal
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GLs resources, select the SysNode compliant with HOST-A and HOST-B. Once GLs is created, register the two GLs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1" and "fec0:1::2".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.5.8 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

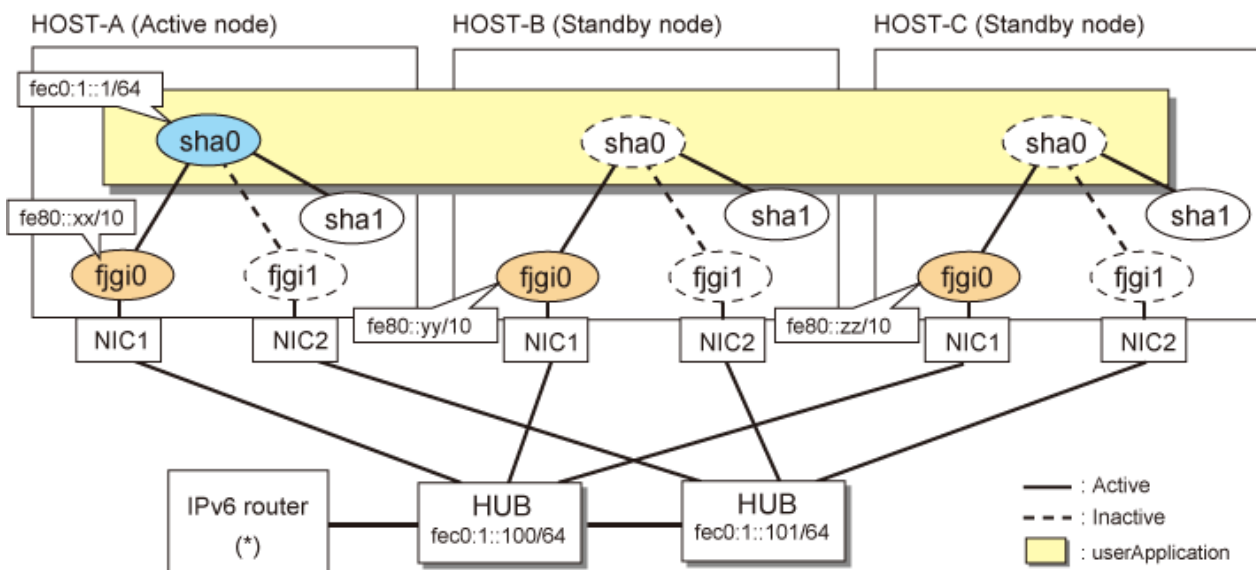
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 5) and 8) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta # HOST-A/B/C Takeover virtual IP  
fec0:1::100 swhub1 # Primary HUB IP  
fec0:1::101 swhub2 # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-C]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 8) of both HOST-B and HOST-C, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GLs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GLs is created, register the two GLs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "fec0:1::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6 Example of configuring NIC switching mode (IPv4/IPv6)

When using IPv6 address, it is required to set an IPv6 router on the same network. Also, specify the same prefix and prefix length of IPv6 address for redundant control line function configured in the IPv6 router.

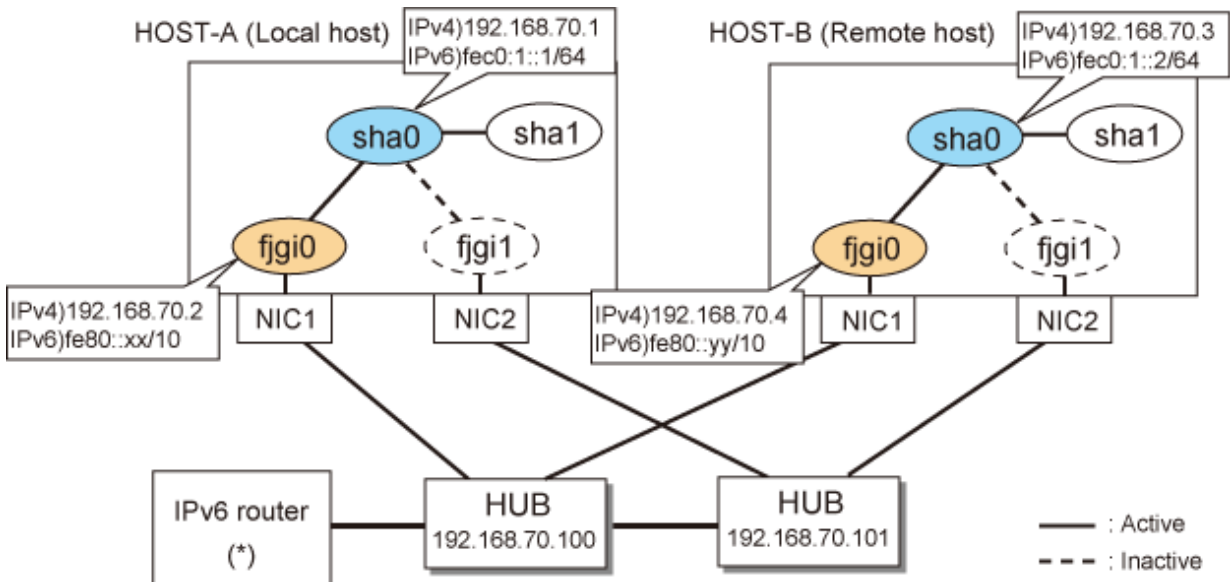
B.6.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX."
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:

For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    hostb    # HOST-B Virtual IP
192.168.70.4    host21   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta   # HOST-A Virtual IP
fec0:1::2      v6hostb   # HOST-B Virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10


```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t net0,net1
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

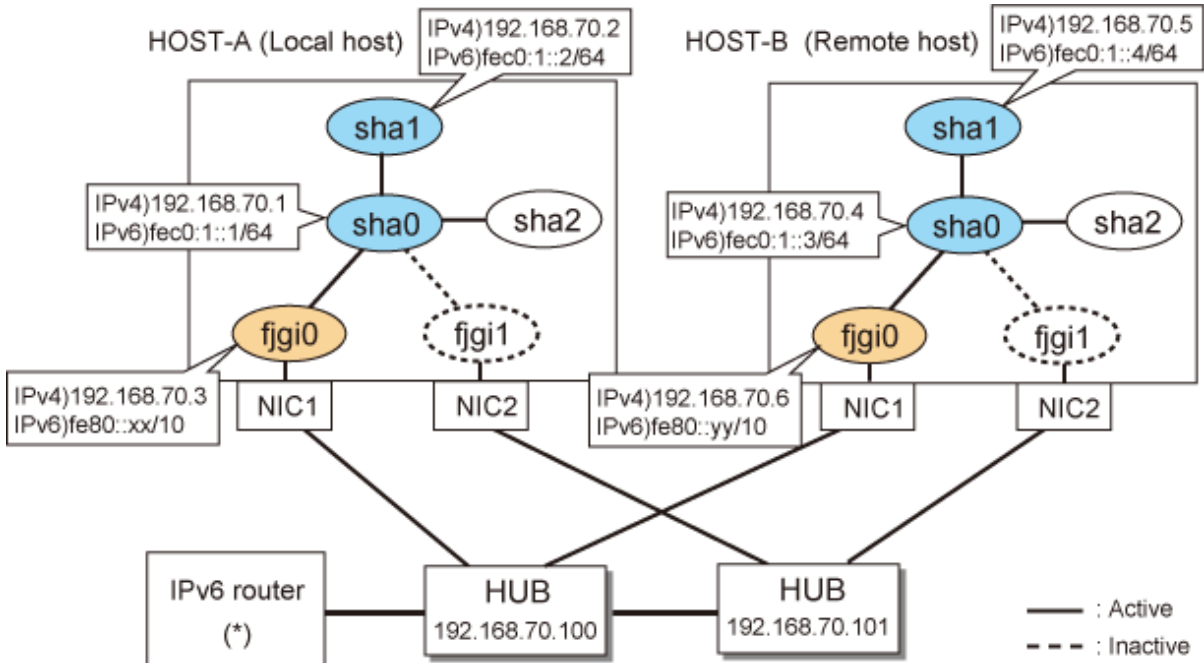
B.6.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0             # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta1 # HOST-A Virtual IP (1)
192.168.70.2    hosta2 # HOST-A Virtual IP (2)
```

```
192.168.70.3    host11 # HOST-A Physical IP
192.168.70.4    hostb1 # HOST-B Virtual IP (1)
192.168.70.5    hostb2 # HOST-B Virtual IP (2)
192.168.70.6    host21 # HOST-B Physical IP
192.168.70.100  swhub1 # Primary HUB IP
192.168.70.101  swhub2 # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1    # HOST-A Virtual IP (1)
fec0:1::2      v6hosta2    # HOST-A Virtual IP (2)
fec0:1::3      v6hostb1    # HOST-B Virtual IP (1)
fec0:1::4      v6hostb2    # HOST-B Virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t
fjgi0,fjgil
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.5
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t
net0,net1
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.5
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t fjgi0,fjgil
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

4-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t net0,net1
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

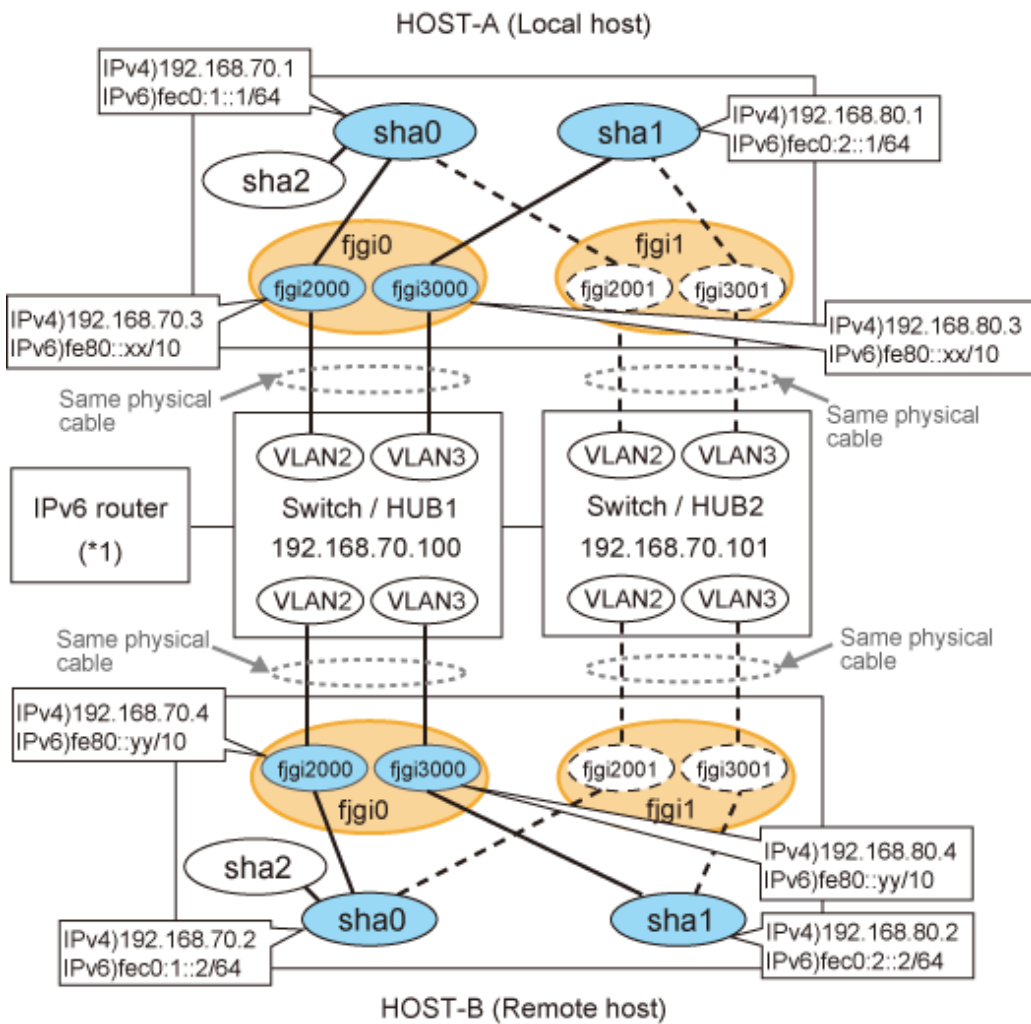
```
# /opt/FJShanet/usr/sbin/hanetpoll on
```

B.6.3 Configuring virtual interfaces with tagged VLAN (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

Note

An example of configuring `/etc/inet/ndpd.conf` to use Solaris server as an IPv6 router is described below:
For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi2000 # fjgi2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi3000 # fjgi3000 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net2000 # net2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net3000 # net3000 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/inet/hosts` file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.3    host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
192.168.70.4    host72   # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2    hostd    # HOST-B Virtual IP
192.168.80.4    host82   # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100  swhub1   # primary Switch/HUB IP
192.168.70.101  swhub2   # secondary Switch/HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in `/etc/hostname.fjgi2000` file and `/etc/hostname.fjgi3000` file. If a file does not exist, create a new file.

- Contents of `/etc/hostname.fjgi2000`

```
host71
```

- Contents of `/etc/hostname.fjgi3000`

```
host81
```

1-2) For Solaris 11 or later

Set the host by the interface used with the `dladm(1M)` command and the `ipadm(1M)` command and also by the host name defined above.

- Interface `net2000`

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host71/24 net2000/v4
```

- Interface `net2001`

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```


- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a host81/24 net3000/v4
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjg3000 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net3000

```
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1    # HOST-A Virtual IP(1)
fec0:2::1      v6hosta2    # HOST-A Virtual IP(2)
fec0:1::2      v6hostb1    # HOST-B Virtual IP(1)
fec0:2::2      v6hostB2    # HOST-B Virtual IP(2)
```

2) Creation of IPv4 virtual interface

2-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi2000,fjgi2001
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net2000,net2001
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t
net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3000, or with the ipadm(1M) command.

3) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::1/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

5) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3000 for Solaris 10, net2000 and net 3000 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3000 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host72
```

- Contents of /etc/hostname.fjgi3000

```
host82
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host72/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a host82/24 net3000/v4
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjgi3000 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net3000

```
# /usr/sbin/ipadm create-addr -T addrconf net3000/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Creation of IPv4 virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t
net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3000, or with the ipadm(1M) command.

3) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::2/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

5) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJsvhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJsvhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3000 for Solaris 10, net2000 and net 3000 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

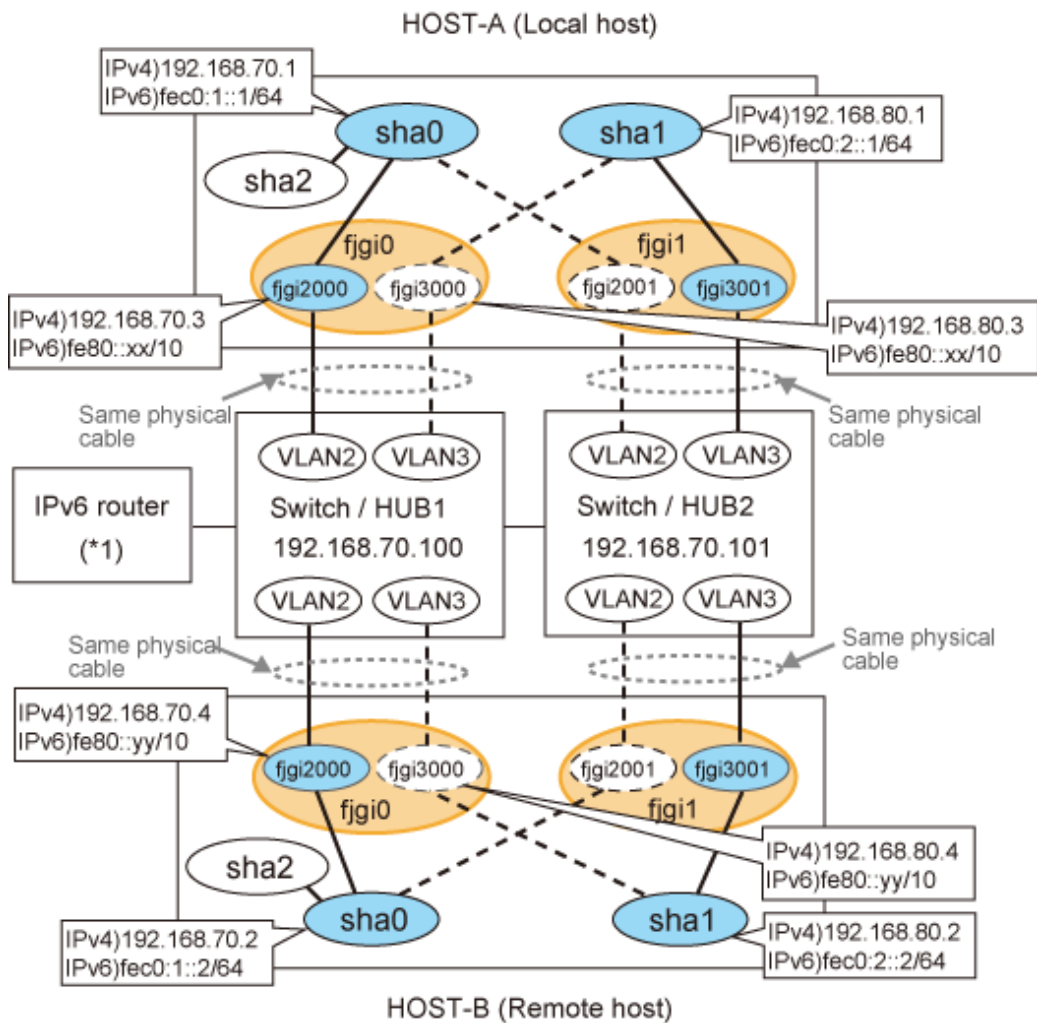
```
# /usr/sbin/shutdown -y -i6 -g0
```

B.6.4 Configuring virtual interfaces with tagged VLAN (asynchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
 For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi2000 # fjgi2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi3001 # fjgi3001 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net2000 # net2000 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net3001 # net3001 sends Prefix "fec0:2::0/64".
```

[HOST-A]

- 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    host71   # HOST-A Physical IP (Tagged VLAN interface)
192.168.80.1    hostb    # HOST-A Virtual IP
192.168.80.3    host81   # HOST-A Physical IP (Tagged VLAN interface)
192.168.70.2    hostc    # HOST-B Virtual IP
192.168.70.4    host72   # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2    hostd    # HOST-B Virtual IP
192.168.80.4    host82   # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100  swhub1   # Switch/HUB1 IP
192.168.80.100  swhub2   # Switch/HUB2 IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3001 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host71
```

- Contents of /etc/hostname.fjgi3001

```
host81
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host71/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T static -a host81/24 net3001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi12000 and /etc/hostname6.fjgi3001 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net3001

```
# /usr/sbin/ipadm create-addr -T addrconf net3001/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1 # HOST-A Virtual IP(1)
fec0:2::1      v6hosta2 # HOST-A Virtual IP(2)
fec0:1::2      v6hostb1 # HOST-B Virtual IP(1)
fec0:2::2      v6hostB2 # HOST-B Virtual IP(2)
```

2) Creation of IPv4 virtual interface

2-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi2000,fjgi2001
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net2000,net2001
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t
net3001,net3000
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3001, or with the ipadm(1M) command.

3) Creation of IPv6 virtual interface

```
# /opt/FJShanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
# /opt/FJShanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::1/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
# /opt/FJShanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3001 for Solaris 10, net2000 and net 3001 for Solaris 11 or later are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi2000 file and /etc/hostname.fjgi3001 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi2000

```
host72
```

- Contents of /etc/hostname.fjgi3001

```
host82
```

1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a host72/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
# /usr/sbin/ipadm create-ip net3001
# /usr/sbin/ipadm create-addr -T static -a host82/24 net3001/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi2000 and /etc/hostname6.fjgi3001 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net2000

```
# /usr/sbin/ipadm create-addr -T addrconf net2000/v6
```

- Interface net3001

```
# /usr/sbin/ipadm create-addr -T addrconf net3001/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Creation of IPv4 virtual interface

2-1) For Solaris 10


```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t
fjgi3001,fjgi3000
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t
net3001,net3000
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3001, or with the ipadm(1M) command.

3) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha1,sha1 -i fec0:2::2/64
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.80.100 -b off
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

6) Reboot

Run the following command to reboot the system. Using the ifconfig command, make sure that fjgi2000 and fjgi3001 for Solaris 10, net2000 and net 3001 for Solaris 11 or later are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

B.6.5 Example of the Cluster system (1:1 Standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

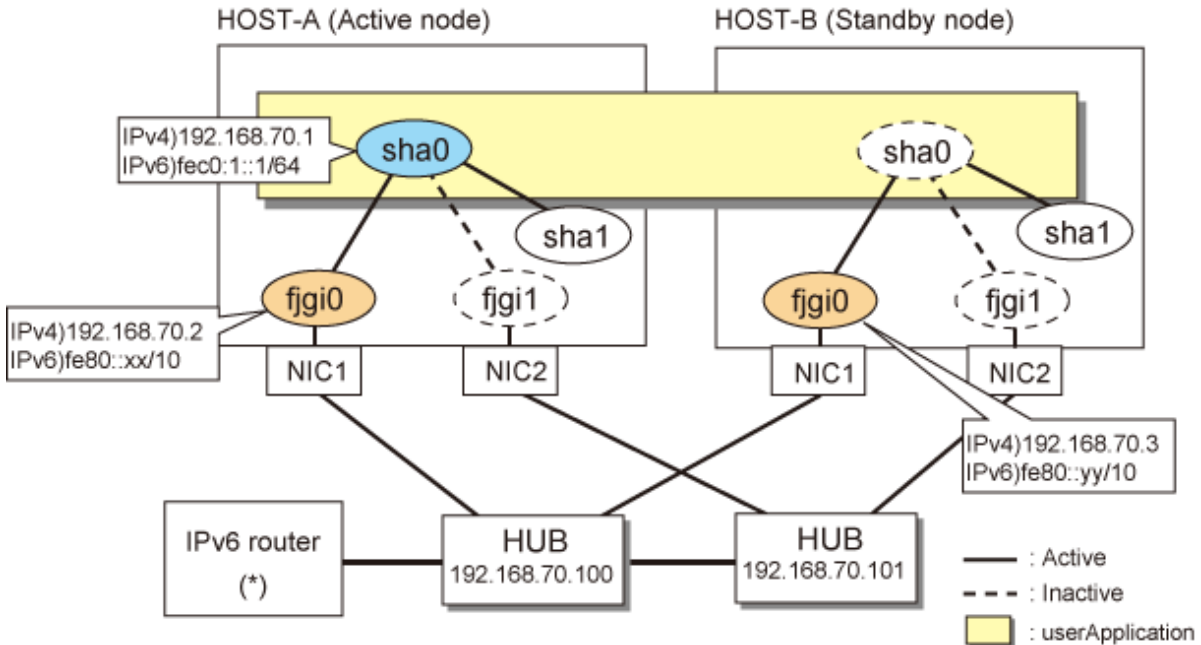
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "G.3 Troubleshooting".



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta  # HOST-A/B Takeover virtual IP
192.168.70.2    host11 # HOST-A Physical IP
192.168.70.3    host21 # HOST-B Physical IP
```

```
192.168.70.100 swhub1 # Primary HUB IP
192.168.70.101 swhub2 # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0 255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta1 # HOST-A/B Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
```

4-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

5) Setting up the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

8) Starting the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n shal
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resource, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1 - fec0:1::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.6 Example of the Cluster system (Mutual Standby) without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

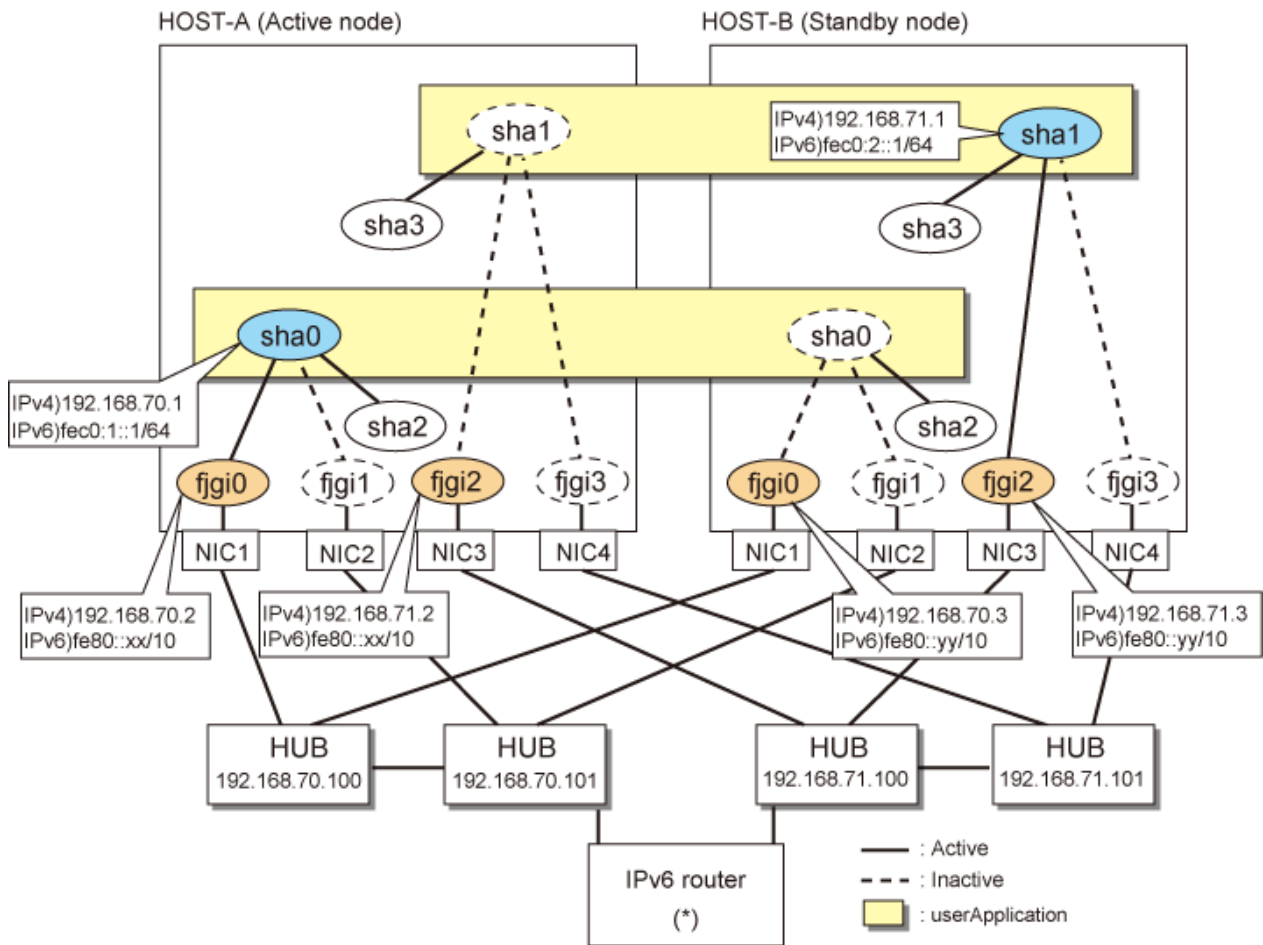
The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.



Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
 For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 fjgi2           # fjgi2 sends Prefix "fec0:2::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0             # net0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 net2             # net2 sends Prefix "fec0:2::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    hosta    # HOST-A/B Virtual IP (Take over IP address1)
192.168.70.2    host11   # HOST-A Physical IP (1)
192.168.70.3    host21   # HOST-B Physical IP (1)
192.168.71.1    hostb    # HOST-A/B Virtual IP (Take over IP address2)
192.168.71.2    host12   # HOST-A Physical IP (2)
192.168.71.3    host22   # HOST-B Physical IP (2)
192.168.70.100  swhub1   # Primary HUB IP (1)
192.168.70.101  swhub2   # Secondary HUB IP (1)
192.168.71.100  swhub3   # Primary HUB IP (2)
192.168.71.101  swhub4   # Secondary HUB IP (2)

```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi2 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi2

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2
# /usr/sbin/ipadm create-addr -T static -a host12/24 net2/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi2 files as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net2

```
# /usr/sbin/ipadm create-addr -T addrconf net2/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta    # HOST-A/B Takeover virtual IP (1)
fec0:2::1      v6hostb    # HOST-A/B Takeover virtual IP (2)
```


2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t net2,net3
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0, in /etc/hostname.fjgi2, or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2,fjgi3
```

4-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t net2,net3
```

5) Setting up the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

7) Creation of takeover virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha1
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2  
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi2 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi2

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net2

```
# /usr/sbin/ipadm create-ip net2  
# /usr/sbin/ipadm create-addr -T static -a host22/24 net2/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi2 files as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net2

```
# /usr/sbin/ipadm create-addr -T addrconf net2/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi2 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
fjgi0,fjgi1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t  
fjgi2,fjgi3
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
net0,net1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t  
net2,net3
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0, in /etc/hostname.fjgi2 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t fjgi2,fjgi3
```

4-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t net2,net3
```

5) Setting up the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off  
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0  
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha1
```

7) Creation of takeover virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha0  
# /opt/FJSSVhanet/usr/sbin/hanethvrsc create -n sha1
```

8) Starting the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
# /opt/FJSVhanet/usr/sbin/strptl -n sha3
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1 - fec0:1::1" and "192.168.71.1 - fec0:2::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.7 Example of the Cluster system (Mutual Standby) with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

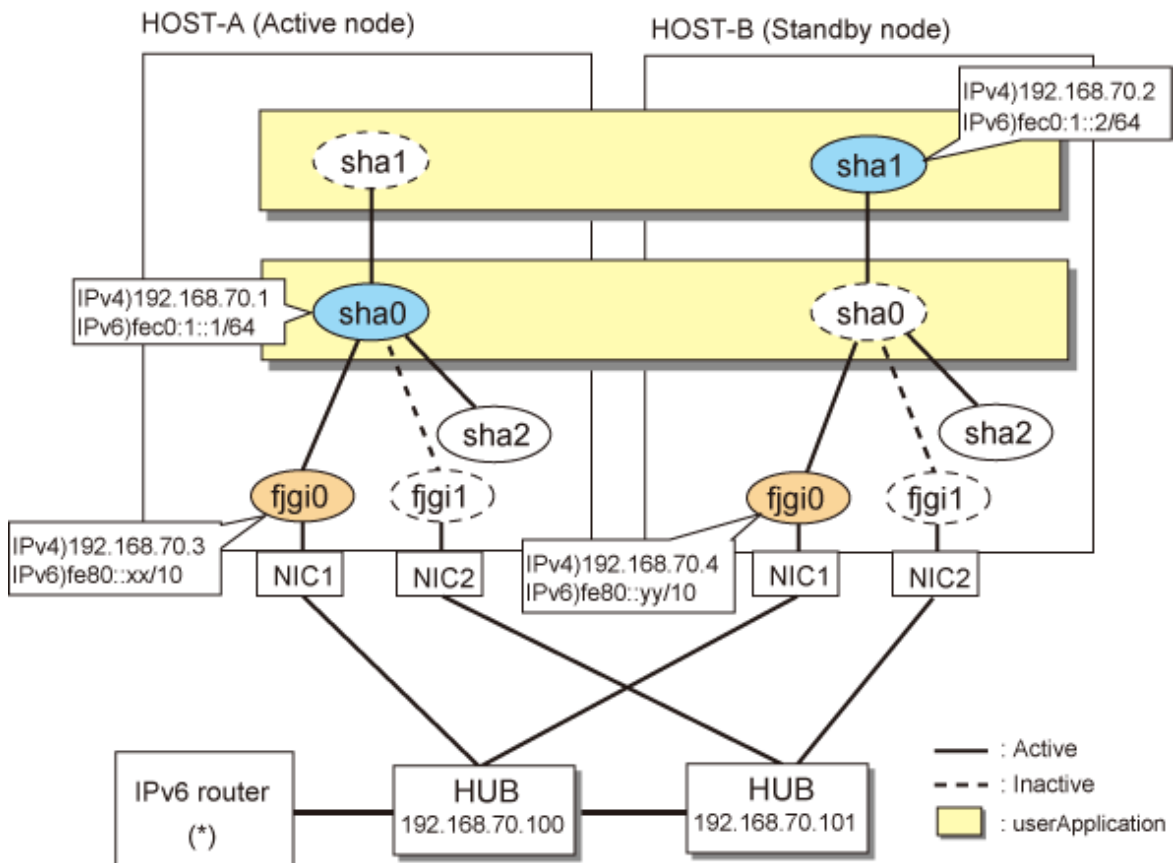
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.



When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fghiX" to "netX".
(X is a instance number.)

Note

An example of configuring `/etc/inet/ndpd.conf` to use Solaris server as an IPv6 router is described below:
For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fghi0           # fghi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0            # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/inet/hosts` file.

```
192.168.70.1  hosta  # HOST-A/B Virtual IP (Take over IP address1)
192.168.70.2  hostb  # HOST-A/B Virtual IP (Take over IP address2)
192.168.70.3  host11 # HOST-A Physical IP
192.168.70.4  host21 # HOST-B Physical IP
```

```
192.168.70.100  swhub1  # Primary HUB IP
192.168.70.101  swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta  # HOST-A/B Takeover virtual IP (1)
fec0:1::2      v6hostb  # HOST-A/B Takeover virtual IP (2)
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
fjgi0,fjgil
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t
net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,shal -i fec0:1::2/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,shal
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n shal
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
fjgi0,fjgil
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
net0,net1
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy -n sha0,sha1 -i 192.168.70.2
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

4-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
# /opt/FJJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
# /opt/FJJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```


6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0  
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha2
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A and HOST-B. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1 - fec0:1::1" and "192.168.70.2 - fec0:1::2".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.6.8 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy and zz in the figure below are assigned automatically by the automatic address configuration.

For configuring the cluster system, refer to the Cluster system manual.

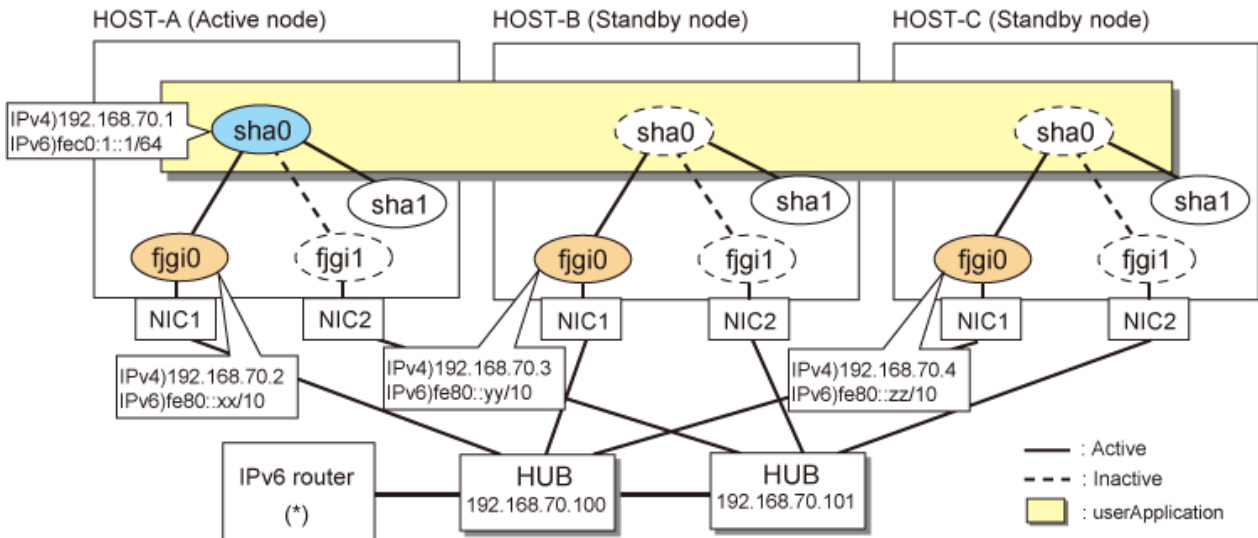
In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) and 9) in the procedure for setting up on each host.

Note

When using IPv6 address as a takeover virtual interface, it may take around 30 seconds to recover the communication after switching the node. In order to hold a communication instantly, start IPv6 routing daemon beforehand on both operating and standby nodes. For details on this issue, refer to "[G.3 Troubleshooting](#)".



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 fjgi0           # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 net0            # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A/B/C Takeover virtual IP
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.4    host31   # HOST-C Physical IP
192.168.70.100 swhub1  # Primary HUB IP
192.168.70.101 swhub2  # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1      v6hosta1      # HOST-A/B/C Takeover virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
net0,net1
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[HOST-C]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host31
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host31/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t
net0,net1
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

4-1) For Solaris 10

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgil
```

4-1) For Solaris 11 or later

```
# /opt/FJJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Starting the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/strptl -n sha1
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 9) of both HOST-B and HOST-C, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resources, select the SysNode compliant with HOST-A, HOST-B, and HOST-C. Once GIs is created, register the two GIs resources on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A, HOST-B, and HOST-C in the order of operation node followed by standby node. Then, register the takeover address "192.168.70.1 - fec0:1::1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

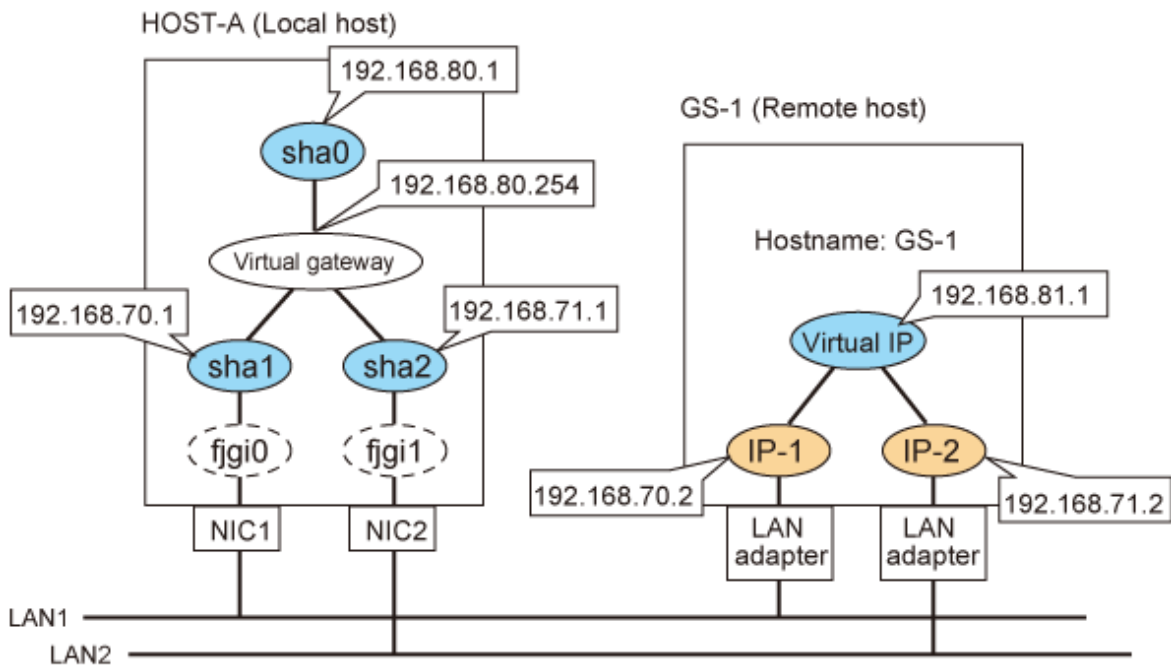
B.7 Example of configuring GS/SURE linkage mode

B.7.1 Example of the Single system in GS/SURE connection function (GS communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the GS, refer to the GS manual.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Virtual IP (mode:n)
192.168.71.1    host12 # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta  # HOST-A Virtual IP (mode:c)
192.168.80.254 virgw  # Virtual gateway
192.168.70.2    gs11  # GS-1 Physical IP (1)
192.168.71.2    gs12  # GS-1 Physical IP (2)
192.168.81.1    gsa   # GS-1 Virtual IP
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgi1
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```


3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.2,192.168.71.2 -m on
```

5) Activation of virtual interface

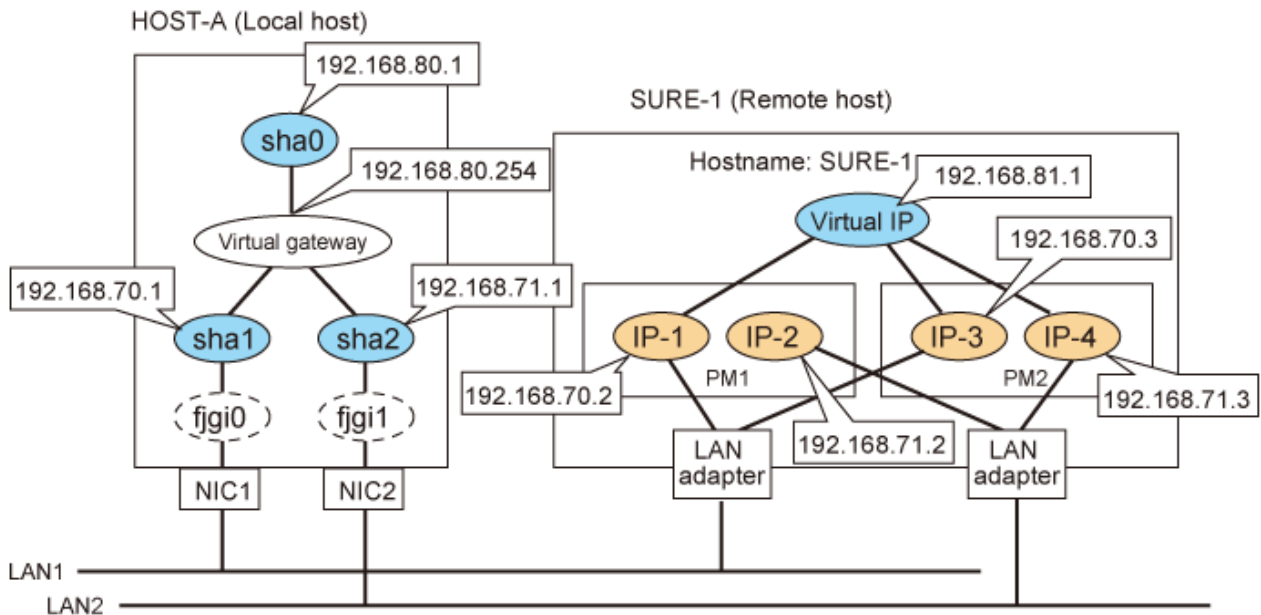
```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.7.2 Example of the Single system in GS/SURE connection function (SURE communication function)

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Virtual IP (mode:n)
192.168.71.1    host12 # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta  # HOST-A Virtual IP (mode:c)
192.168.80.254 virgw  # Virtual gateway
192.168.70.2    sure11 # SURE-1 Physical IP (1)
192.168.71.2    sure12 # SURE-1 Physical IP (2)
192.168.70.3    sure13 # SURE-1 Physical IP (3)
192.168.71.3    sure14 # SURE-1 Physical IP (4)
```

```
192.168.81.1    surea    # SURE-1 Virtual IP (1)
192.168.81.2    sureb    # SURE-1 Virtual IP (2)
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgil
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.2:1,192.168.71.2:1,192.168.70.3:2,192.168.71.3:2 -m on -r on
```

5) Activation of virtual interface

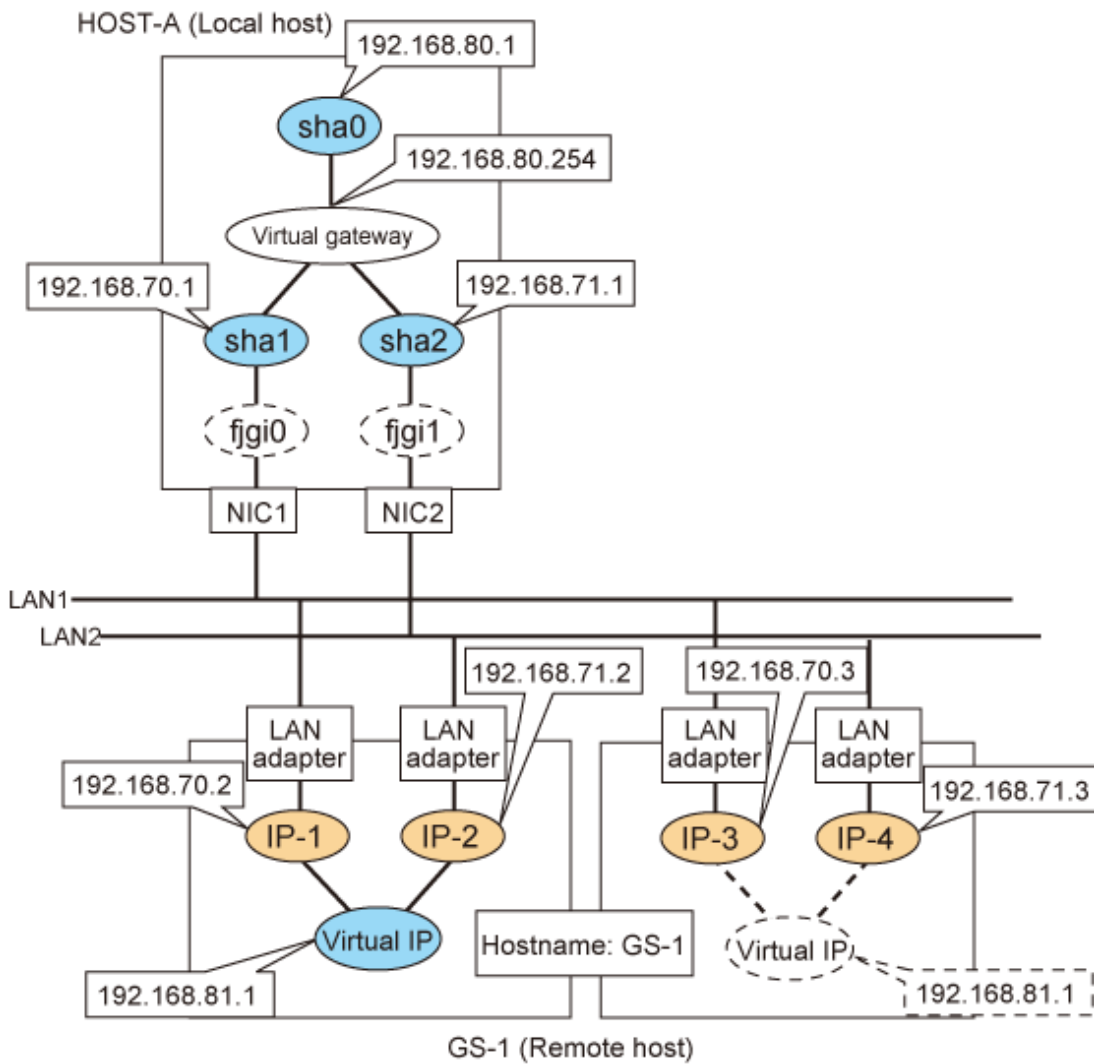
```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.7.3 Example of the Single system in GS/SURE connection function (GS Hot-standby)

This section describes an example of configuring an environment for GS Hot-standby.

For configuring the GS, refer to the GS manual.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11 # HOST-A Virtual IP (mode:n)
192.168.71.1    host12 # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta  # HOST-A Virtual IP (mode:c)
192.168.80.254 virgw  # Virtual gateway
192.168.70.2    gs11   # GS-1 Physical IP (1)
192.168.71.2    gs12   # GS-1 Physical IP (2)
192.168.70.3    gs13   # GS-1 Physical IP (3)
192.168.71.3    gs14   # GS-1 Physical IP (4)
192.168.81.1    gsa    # GS-1 Virtual IP
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
```

```
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgil
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.2,192.168.71.2 -m on
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.3,192.168.71.3
```

5) Activation of virtual interface

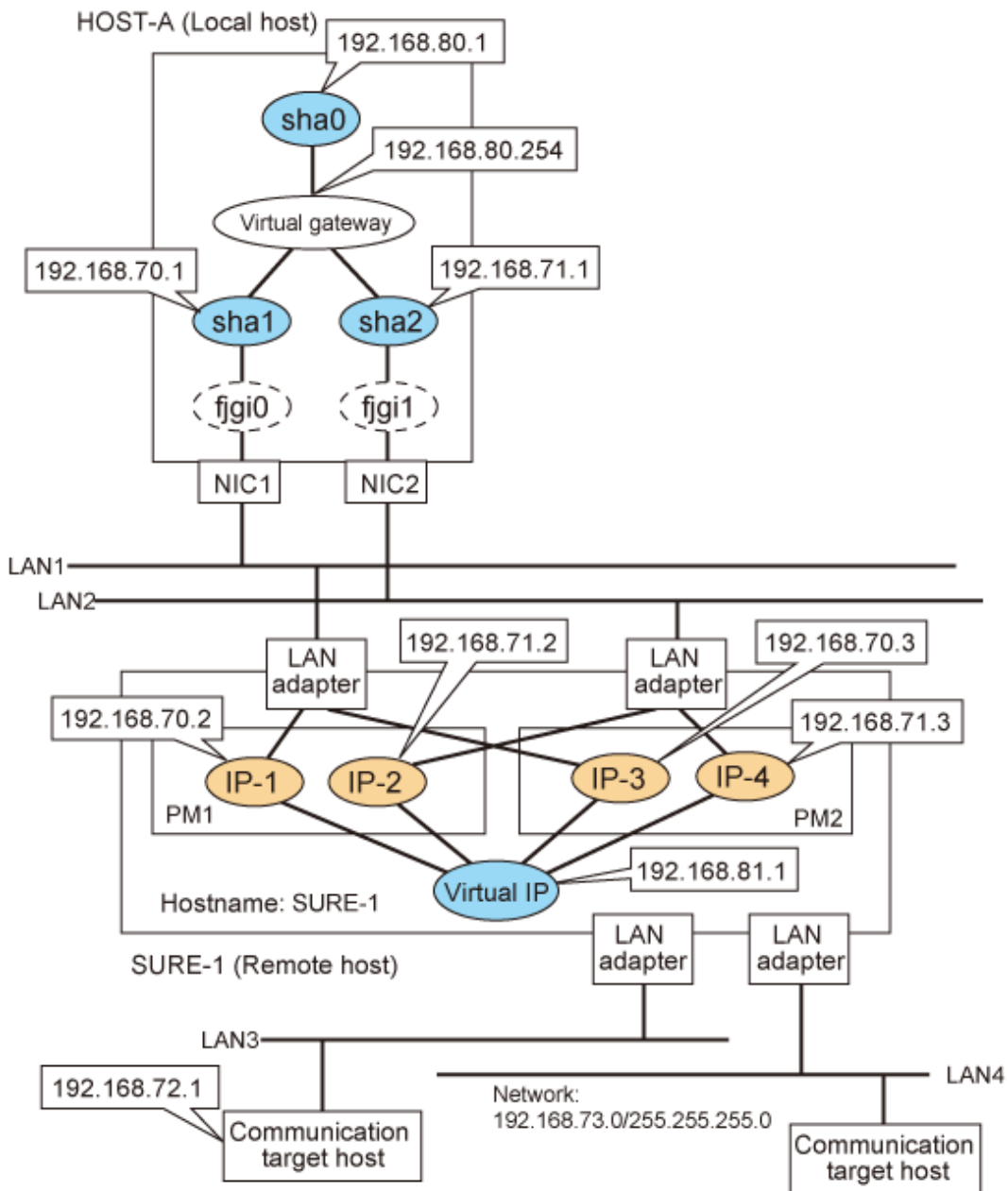
```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.7.4 Example of the Single system in TCP relay function

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Virtual IP (mode:n)
192.168.71.1    host12 # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta  # HOST-A Virtual IP (mode:c)
192.168.80.254 virgw  # Virtual gateway
192.168.70.2    sure11 # SURE-1 Physical IP (1)
192.168.71.2    sure12 # SURE-1 Physical IP (2)
192.168.70.3    sure13 # SURE-1 Physical IP (3)
192.168.71.3    sure14 # SURE-1 Physical IP (4)

```

```
192.168.81.1    surea  # SURE-1 Virtual IP (1)
192.168.81.2    sureb  # SURE-1 Virtual IP (2)
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgil
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.2:1,192.168.71.2:1,192.168.70.3:2,192.168.71.3:2 -m on -r on
```

5) Setting the TCP relay function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -i 192.168.81.1 -c
192.168.72.1,192.168.73.0:255.255.255.0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

B.7.5 Example of the Cluster system in GS/SURE connection function (GS communication function)

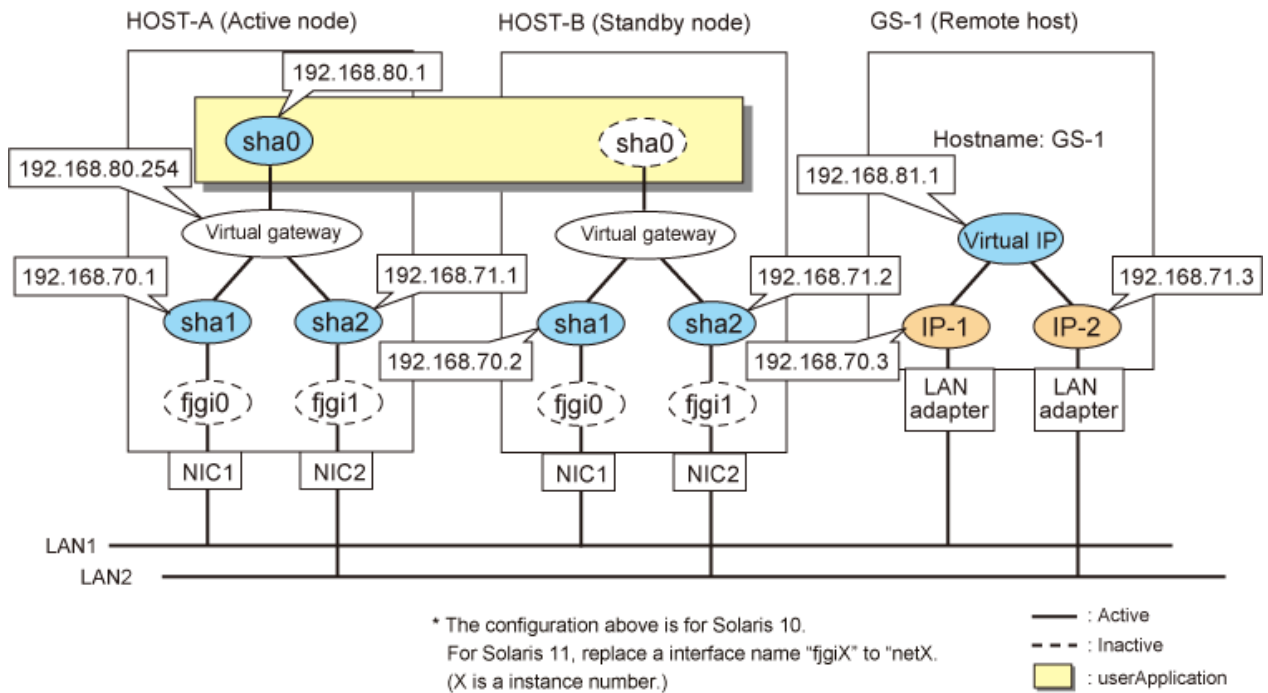
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the GS, refer to the GS manual.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Virtual IP (mode:n)
192.168.71.1    host12 # HOST-A Virtual IP (mode:n)
192.168.70.2    host21 # HOST-B Virtual IP (mode:n)
192.168.71.2    host22 # HOST-B Virtual IP (mode:n)
192.168.80.1    hosta  # HOST-A/B Virtual IP (mode:c, Takeover virtual IP)
192.168.80.254 virgw  # Virtual gateway
192.168.70.3    gs11  # GS-1 Physical IP (1)
192.168.71.3    gs12  # GS-1 Physical IP (2)
192.168.81.1    gsa   # GS-1 Virtual IP
  
```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```

192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
  
```

2) Creation of virtual interface

2-1) For Solaris 10

```

# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgi1
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
  
```

2-1) For Solaris 10

```

# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
  
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t  
192.168.70.3,192.168.71.3 -m on -r on
```

Setting the Standby node monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t  
192.168.70.2,192.168.71.2 -m on -r on
```



When configuring standby node monitoring information, it is necessary to specify the take over IP address for '-i' option.

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t fjgi0  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t fjgi1  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t net0  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t net1  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t  
192.168.70.3,192.168.71.3 -m on -r on
```

Setting the Active node monitoring information:


```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t
192.168.70.1,192.168.71.1 -m on -r on
```

Note

When configuring active node monitoring information, it is necessary to specify the take over IP address for '-i' option.

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 5) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

B.7.6 Example of the Cluster system in GS/SURE connection function (SURE communication function)

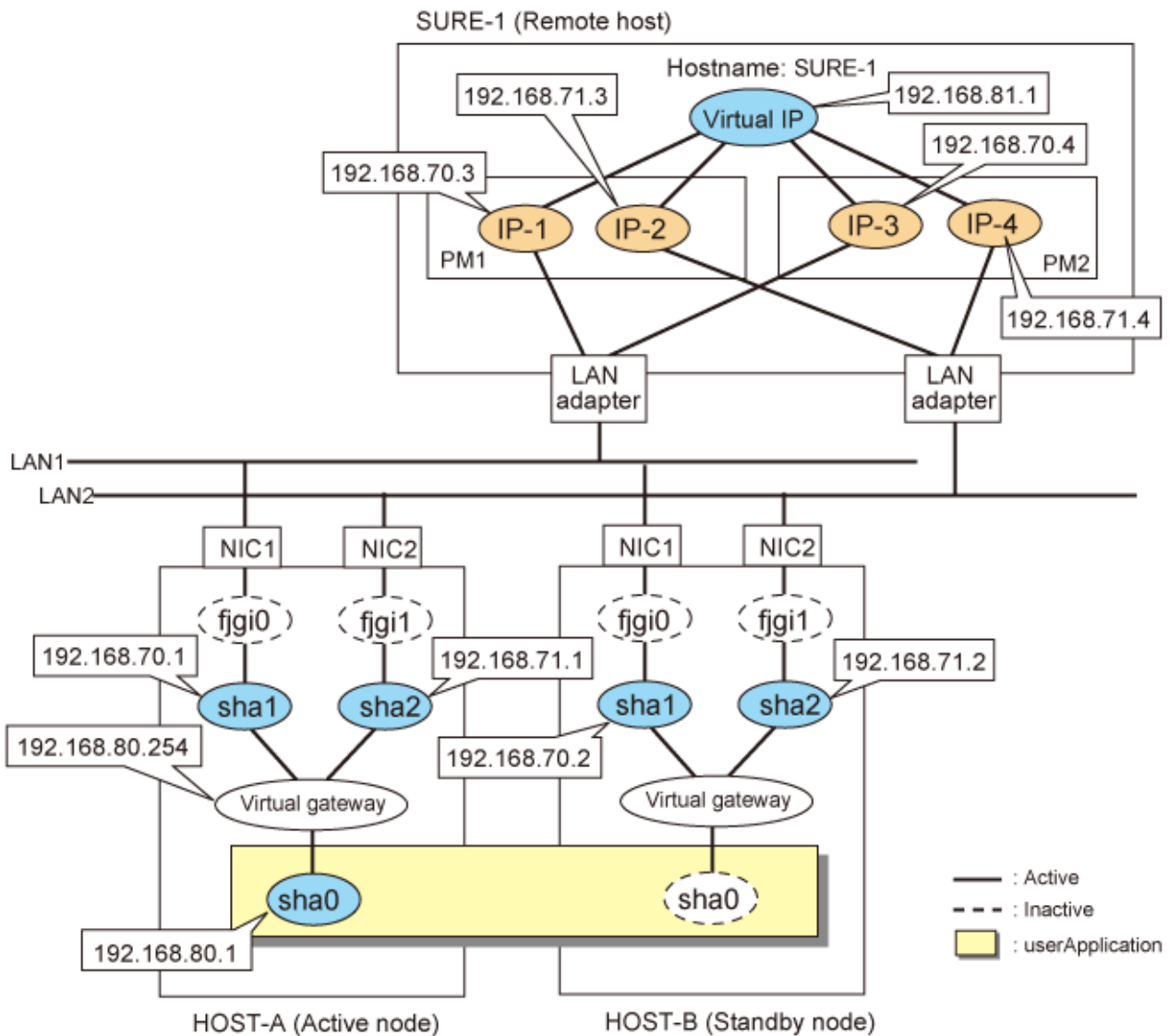
This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the SURE, refer to the SURE manual.

For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11 # HOST-A Virtual IP(mode:n)
192.168.71.1    host12 # HOST-A Virtual IP(mode:n)
192.168.70.2    host21 # HOST-B Virtual IP(mode:n)
192.168.71.2    host22 # HOST-B Virtual IP(mode:n)
192.168.80.1    hosta  # HOST-A/B Virtual IP(mode:c, Takeover virtual IP)
192.168.80.254 virgw  # Virtual gateway
192.168.70.3    sure11 # SURE-1 Physical IP(IP-1)
192.168.71.3    sure12 # SURE-1 Physical IP(IP-2)
192.168.70.4    sure13 # SURE-1 Physical IP(IP-3)
192.168.71.4    sure14 # SURE-1 Physical IP(IP-4)
192.168.81.1    surea  # SURE-1 Virtual IP

```

1-2) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
192.168.81.0    255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.3:1,192.168.71.3:1,192.168.70.4:2,192.168.71.4:2 -m on -r on
```

Setting the Standby node monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t
192.168.70.2,192.168.71.2 -m on -r on
```



Note

When configuring standby node monitoring information, it is necessary to specify the take over IP address for '-i' option.

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t fjgi1
# opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.2 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.2 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Setting the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

4) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n SURE-1 -i 192.168.81.1 -t
192.168.70.3:1,192.168.71.3:1,192.168.70.4:2,192.168.71.4:2 -m on -r on
```

Setting the Active node monitoring information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t
192.168.70.1,192.168.71.1 -m on -r on
```



Note

When configuring active node monitoring information, it is necessary to specify the take over IP address for '-i' option.

5) Creation of takeover virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

[Configuration by Cluster Admin View]

1) Configuration of userApplication

After completing step 4) of both HOST-A and HOST-B, connect to the administration server using Cluster Admin View, then setup the cluster environment.

To create GIs resource, select the SysNode for HOST-A and HOST-B. Once GIs is created, register it on the userApplication.

When registering on the userApplication, select the SysNode compliant with HOST-A and HOST-B in the order of operation node followed by standby node. Then, register the takeover address "192.168.80.1".

2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

Appendix C Operations in Solaris Zones Environment

This appendix describes the operation of GLS on Solaris Zones. For more information on Solaris Zones, see the documentation for Solaris Zones.

C.1 Overview of the Solaris Zones

A Solaris Zone is a technology that can logically separate one server into multiple independent partitions and that can build multiple virtual Solaris environments within a single server. It is possible to run various applications on each partition as a separate system. (software partitioning technology)

The software partitions where the virtual Solaris environments run are referred to as non-global zones, whereas the environment enabling these software partitions is referred to as the global zone. The redundant line control function ensures network high-reliability on non-global zones.

C.2 Network Configuration of Solaris Zones

Solaris Zones provide the following three types:

- Shared-IP zone

Physical interfaces configured on the global zone are shared with non-global zones in this network form. The zone defined as ip-type=shared in the zone configuration information is applied.

- Exclusive-IP zone

Physical interfaces, or virtual NICs that were created on the physical interfaces are occupied by specific non-global zones in this network form. The zone defined as ip-type=exclusive in the zone configuration information is applied.

- Kernel Zones

Physical interfaces, or virtual NICs that were created on the physical interfaces are occupied by specific non-global zones in this network form. The zone defined that brand is solaris-kz in the zone configuration information is applied.

Information

Either of the following resources can be set in the network interface settings of the exclusive-IP zone and Kernel Zones.

- anet resource

When booting a non-global zone, the anet resource automatically creates a temporary VNIC interface for the zone. When stopping the zone, the anet resource deletes the temporary VNIC interface created as described above.

- net resource

The net resource allocates a network interface existing in a global zone, to a non-global zone.

Note

The anet resource can not be used on guest domains of Oracle VM.

See

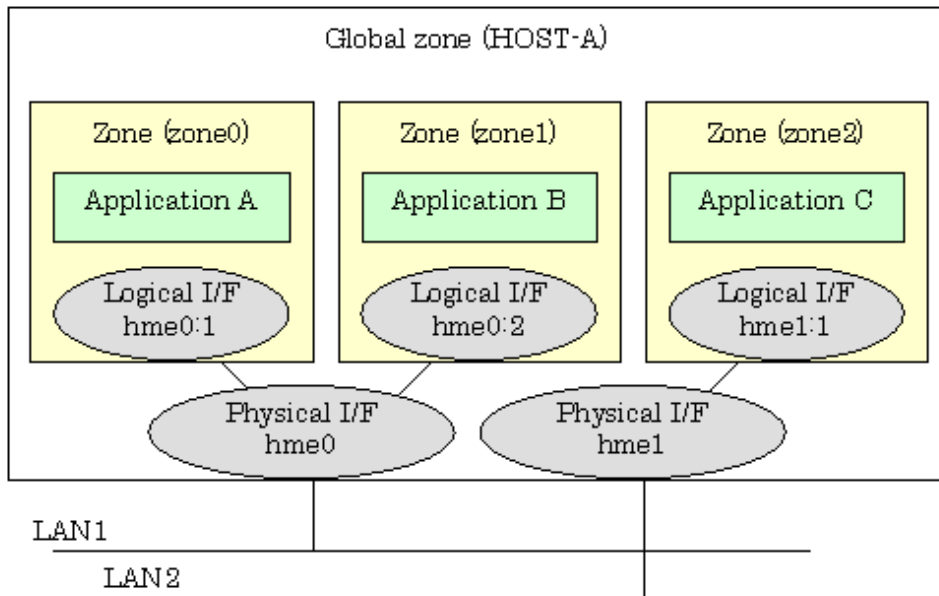
For more details, see the Solaris manual according to your OS version.

C.2.1 Network configuration of shared-IP zone

One or more IP address is allocated to each shared-IP zone. The IP addresses assigned to each non-global zone are added to the logical interface generated on the physical interface. The logical interface is hidden from the other non-global zones, so applications can only use the IP addresses (logical interface) allocated to the non-global zone.

The following figure shows the network interfaces configuration example of shared-IP zone.

Figure C.1 Network interface configuration example of shared-IP zone



Starting each non-global zone from the global zone will enable the global zones.

Note

IP addresses (logical interfaces) allocated to each global zone are created or deleted from Solaris along with startup or stop of non-global zones. If physical interfaces or virtual interfaces do not exist, the zone will not be communicated. If you make the network on global zones highly reliable through redundant line control, it is necessary to activate the virtual interface before startup of non-global zones. However, the redundant line control function will be first started during system startup, so users do not have to be aware of the startup order.

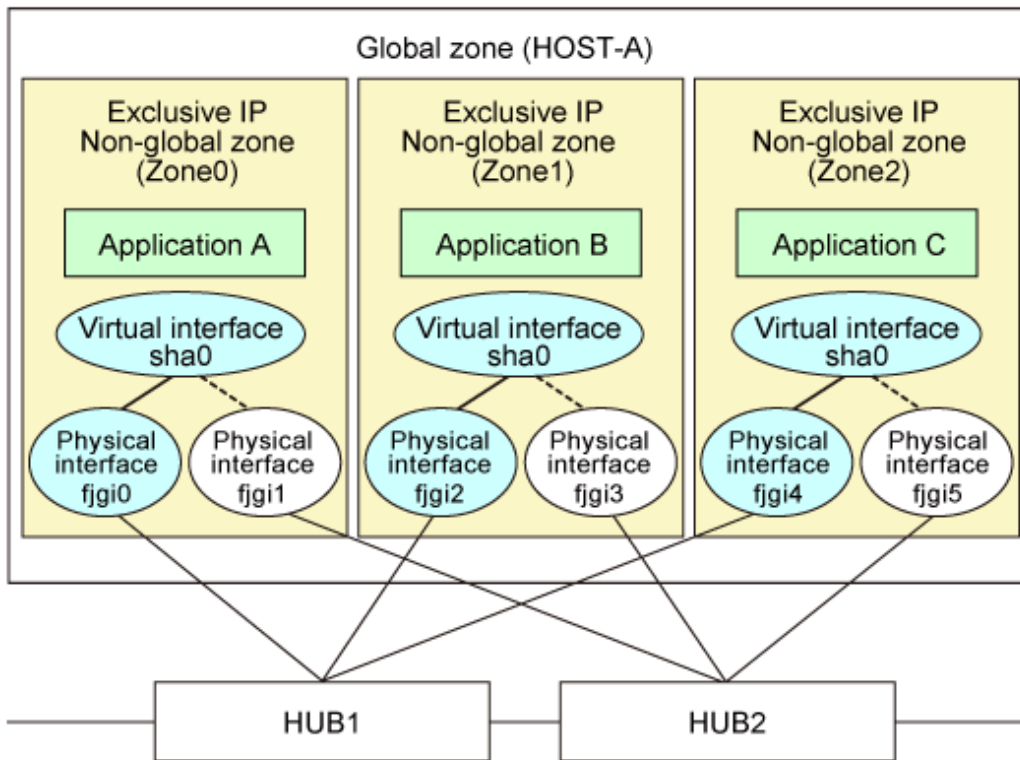
C.2.2 Network configuration of exclusive-IP zone

Physical interfaces are occupied, and functions of the IP level are available in the exclusive-IP zone. In addition, allocated physical interfaces are not available from other zones. To make the network with exclusive-IP zone highly reliable, install Redundant Line Control function in non-global zones and multiplex physical interfaces allocated in non-global zones. For the exclusive-IP zone, it is possible to perform operations such as interface activation and deactivation, just as with the global zone.

The following example shows a network interface configuration for exclusive-IP zone.

Figure C.2 Network interface configuration example of exclusive-IP zone

■ NIC Switching Mode



The non-global zone Zone0 is configured by specifying ip-type=exclusive, and physical interfaces fjgi0 and fjgi1 are allocated. Redundant Line Control function works on Zone0 and multiplexes fjgi0 and fjgi1 redundancy the same as the normal system. As for Zone1 and Zone2, Redundant Line Control function works on each zone in the same manner as Zone0 and multiplexes physical interfaces in the same manner as the normal system.

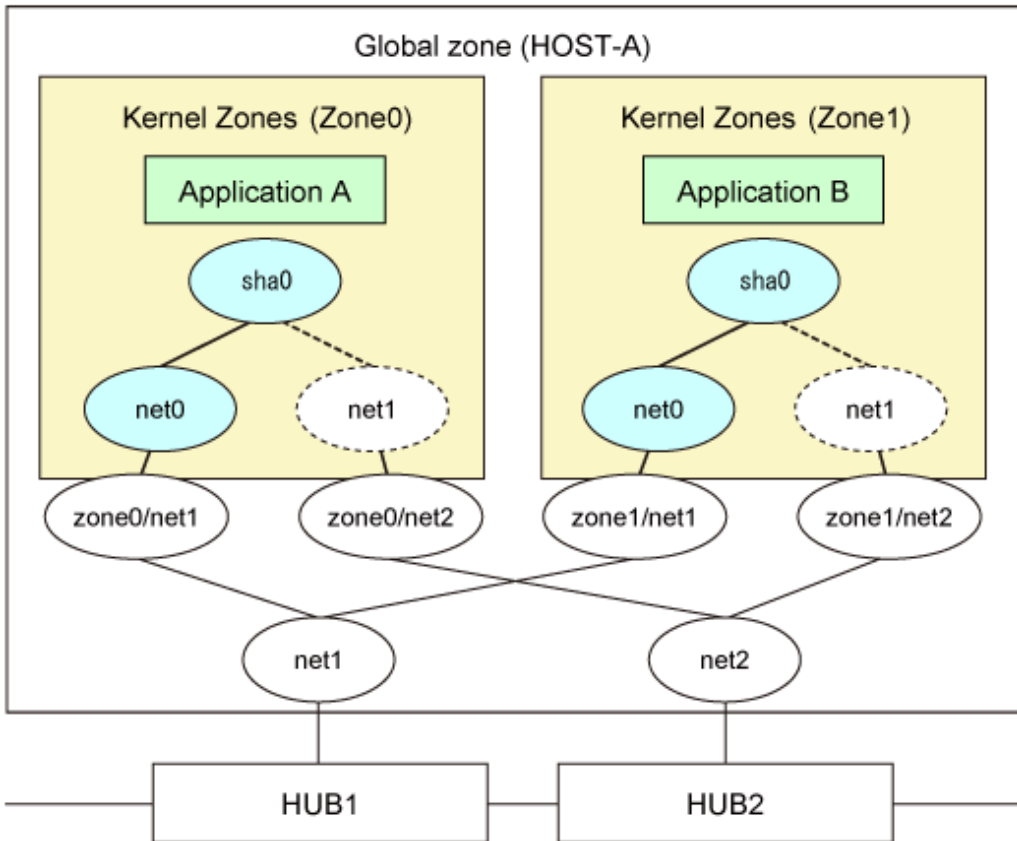
C.2.3 Network configuration of Kernel Zones

Physical interfaces are not occupied, and functions of the IP level are available in Kernel Zones by using the anet resource in the same manner as the global zone. To make the network with Kernel Zones highly reliable, install Redundant Line Control function in Kernel Zones and multiplex physical interfaces allocated in the zones. For Kernel Zones, it is possible to perform operations such as interface activation and deactivation, just as with the global zone.

The following example shows a network interface configuration for Kernel Zones.

Figure C.3 Network interface configuration example of Kernel Zones

■NIC Switching Mode



C.3 Support Set for Each Redundant Line Switching Mode

The following table describes how each redundant line control function supports Solaris Zones.

[Shared-IP Zones]

The following table shows the support for each redundant mode on the shared-IP zone.

Table C.1 Redundant mode supported on the shared-IP zone

| Redundant mode | Support |
|----------------------|-----------|
| Fast switching mode | Supported |
| NIC switching mode | Supported |
| Virtual NIC mode | Supported |
| GS/SURE linkage mode | Supported |

[Exclusive-IP Zones]

The following table shows two network configurations are available on the exclusive-IP zones.

- Redundant configuration on the exclusive-IP zones

Configure the virtual interface that configures the redundant NIC assigned on the exclusive-IP zones and use this virtual interface.

- Redundant configuration on the global zones

Configure the virtual interface that configures the redundant NIC on the global zones and use this virtual interface on the exclusive-IP zones.

The following table shows the support for each redundant mode on the exclusive-IP zones and the virtual network configurations supported in each mode.

Table C.2 Redundant mode supported on the exclusive-IP zones

| Redundant mode | Support | Corresponding virtual network configuration on the Global zone |
|----------------------|-------------|--|
| Fast switching mode | Unsupported | - |
| NIC switching mode | Supported | Redundant configuration on the exclusive-IP zones |
| Virtual NIC mode | Supported | Redundant configuration on the global zone |
| GS/SURE linkage mode | Unsupported | - |

[Kernel Zones]

The following table shows two network configurations are available on the kernel zones.

- Redundant configuration on the kernel zones

Configure the virtual interface that configures the redundant NIC assigned on the kernel zones and use this virtual interface.

- Redundant configuration on the global zones

Configure the virtual interface that configures the redundant NIC on the global zone and use this virtual interface on the kernel zones.

The following table shows the support for each redundant mode on the kernel zones and the virtual network configurations supported in each mode.

Table C.3 Redundant mode supported on the kernel zones

| Redundant mode | Support | Corresponding virtual network configuration |
|----------------------|-------------|---|
| Fast switching mode | Unsupported | - |
| NIC switching mode | Supported | Redundant configuration on the kernel zones |
| Virtual NIC mode | Supported | Redundant configuration on the global zone |
| GS/SURE linkage mode | Supported | Redundant configuration on the kernel zones |

 Information

- When you make the shared-IP zone network highly reliable through NIC switching, use physical IP takeover (operation mode "e"). If you use logical IP takeover (operation mode "d"), the redundant line control function will activate a logical IP address as a take over IP address as well as Solaris will activate another logical IP address during zone startup, which means the unnecessary IP address not used by the zone will be activated. If you add the zone settings after setting logical IP takeover (operation mode "d"), it is not necessary to change it to physical IP takeover (operation mode "e").
- The virtual IP address, logical IP address, and physical IP address allocated through redundant line control of the global zone can be used in the global zone only. The operating system will allocate IP addresses to the non-global zone during zone startup.
- In the environment of Solaris 11.1 or later, the following configuration enables to make a redundant using the same physical NIC on the exclusive-IP zones or the kernel zones and the global zone.
 - Create VNIC to each physical NIC on the global zone and make a VNIC redundant on the exclusive-IP zones or the kernel zones.
 - Directly make the physical NIC redundant on the global zone.
- To use the virtual NIC mode on the exclusive-IP zones and the kernel zones, see "Exclusive-IP zones" or "Kernel Zones" in "PRIMECLUSTER Global Link Services Configuration and Administration Guide 4.5: Redundant Line Control Function for Virtual NIC Mode."

C.4 Operation of Redundant Line Switching Mode on Solaris Zones

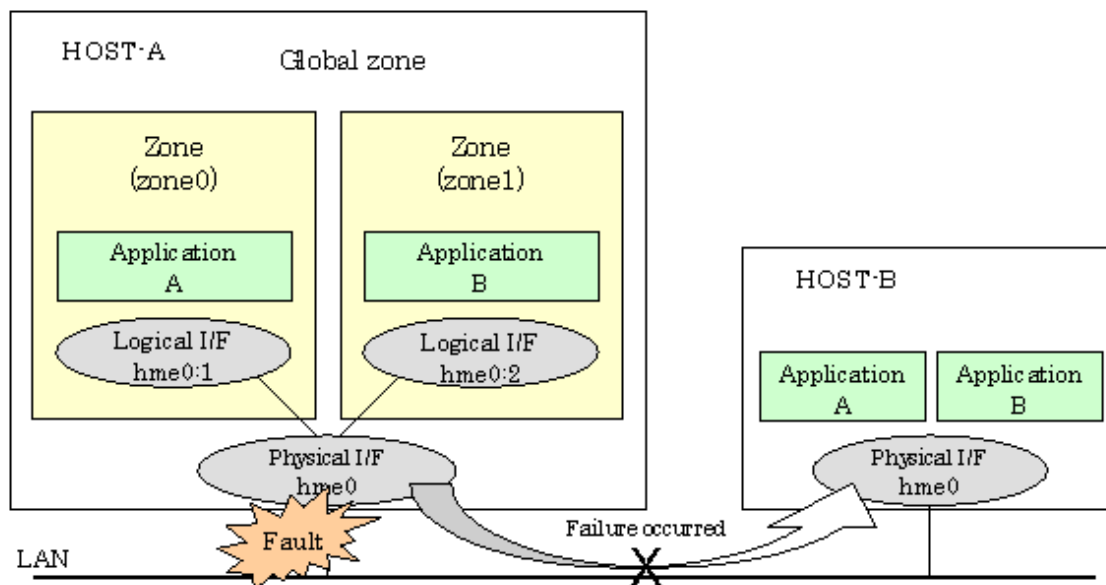
This section explains the monitoring method for the GLS network and the method for switching to a normally operating network on Solaris Zones when an error has occurred.

C.4.1 Configuration to ensure reliable networks of shared-IP zone

This section explains the operation of a configuration which increases reliability of networks with the shared-IP zone.

Normally, the shared-IP zone communicates with each other or the other systems by using a logical interface for a shared-IP zone allocated to the physical interface. If the physical interface fails, or part of the transmission route fails, communication will be disrupted.

Figure C.4 Interface structure without redundant line control



The above example shows that the Application A and B cannot communicate with each other when the transmission route fails.

The redundant line control function ensures operational continuity in the event of a transmission route failure.

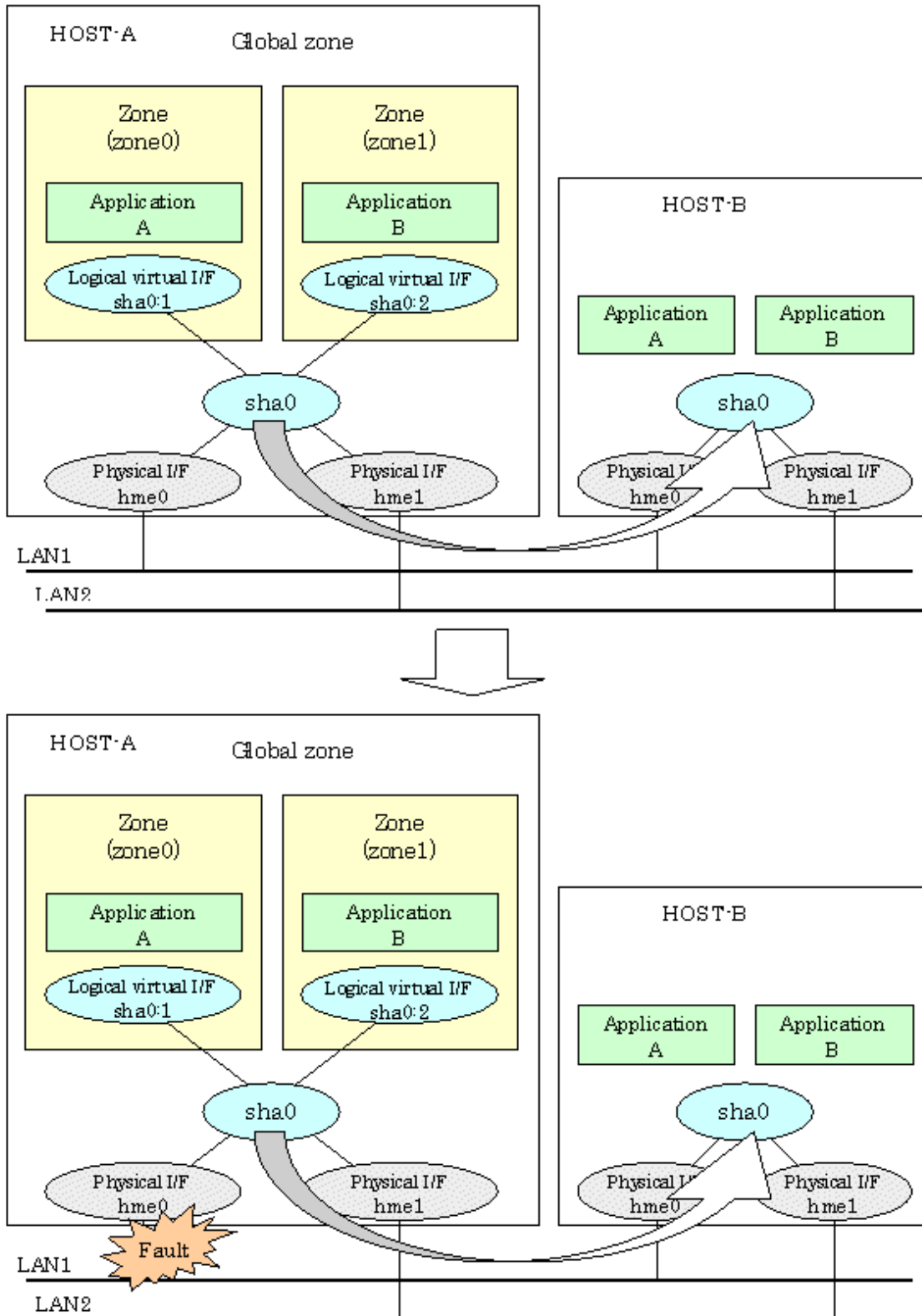
You can use the following modes to increase reliability for networks of the shared-IP zone:

- Fast switching mode
- NIC switching mode
- GS/SURE linkage mode

C.4.1.1 Network high-reliability of shared-IP zone (Fast switching mode, GS/SURE linkage mode)

The following example shows how interfaces can be structured in Fast switching mode or GS/SURE linkage mode.

Figure C.5 Network reliability in Fast switching mode or GS/SURE linkage mode

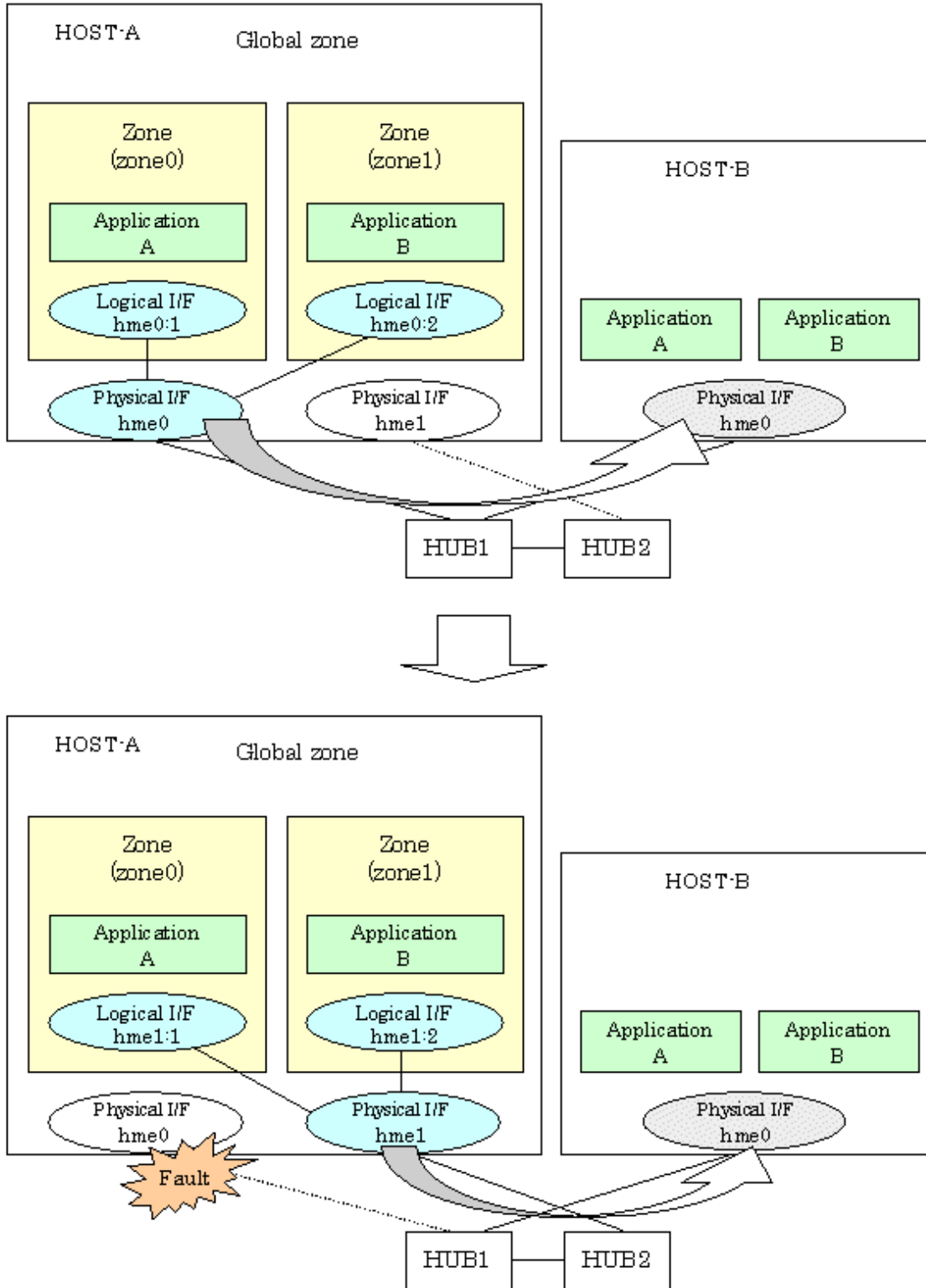


Even if a transmission route fails on either of the physical interfaces, the applications will be switched over to the logical virtual interface on the standby node through redundant line control, so operational continuity is never disrupted.

C.4.1.2 Network high-reliability of shared-IP zone (NIC switching mode)

The following example shows how interfaces can be structured in NIC switching mode.

Figure C.6 Network reliability in NIC switching mode



Even if a transmission route fails on the primary physical interface, the applications will be switched over to the secondary physical interface through redundant line control, so operational continuity is never disrupted.

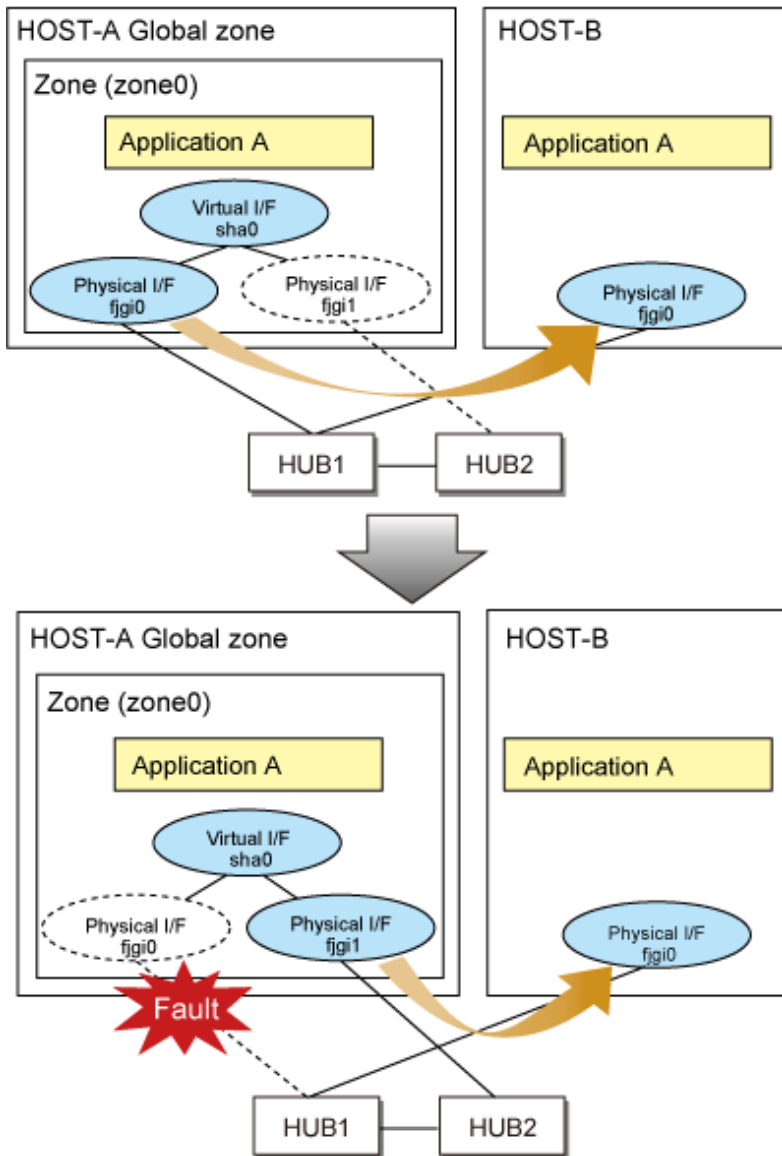
C.4.2 Configuration to ensure reliable networks of exclusive-IP zone

As to a method for increasing reliability of networks of the exclusive-IP zone, there is a method for achieving this through use of the NIC switching mode.

C.4.2.1 Network high-reliability of exclusive-IP zone (NIC switching mode)

The following example is for using NIC switching mode.

Figure C.7 For using NIC switching mode



Even if a transmission route fails on the primary physical interface, the applications will be switched over to the secondary physical interface through redundant line control, so operational continuity is never disrupted.

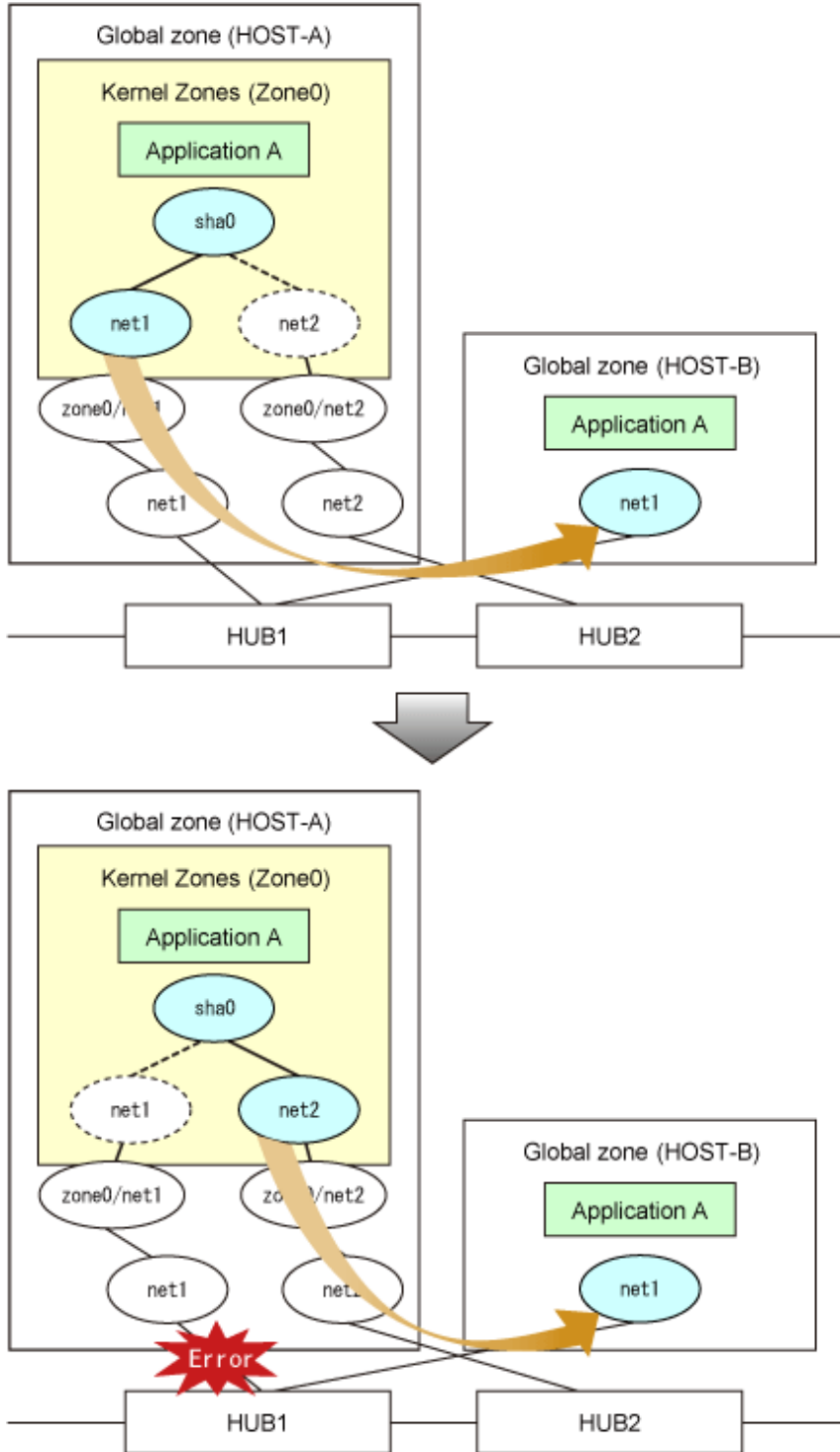
C.4.3 Configuration to ensure reliable networks of Kernel Zones

As to a method for increasing reliability of networks of Kernel Zones, there is a method for achieving this through use of the NIC switching mode or GS/SURE linkage mode.

C.4.3.1 Network high-reliability of Kernel Zones (NIC switching mode)

The following example is for using NIC switching mode.

Figure C.8 For using NIC switching mode

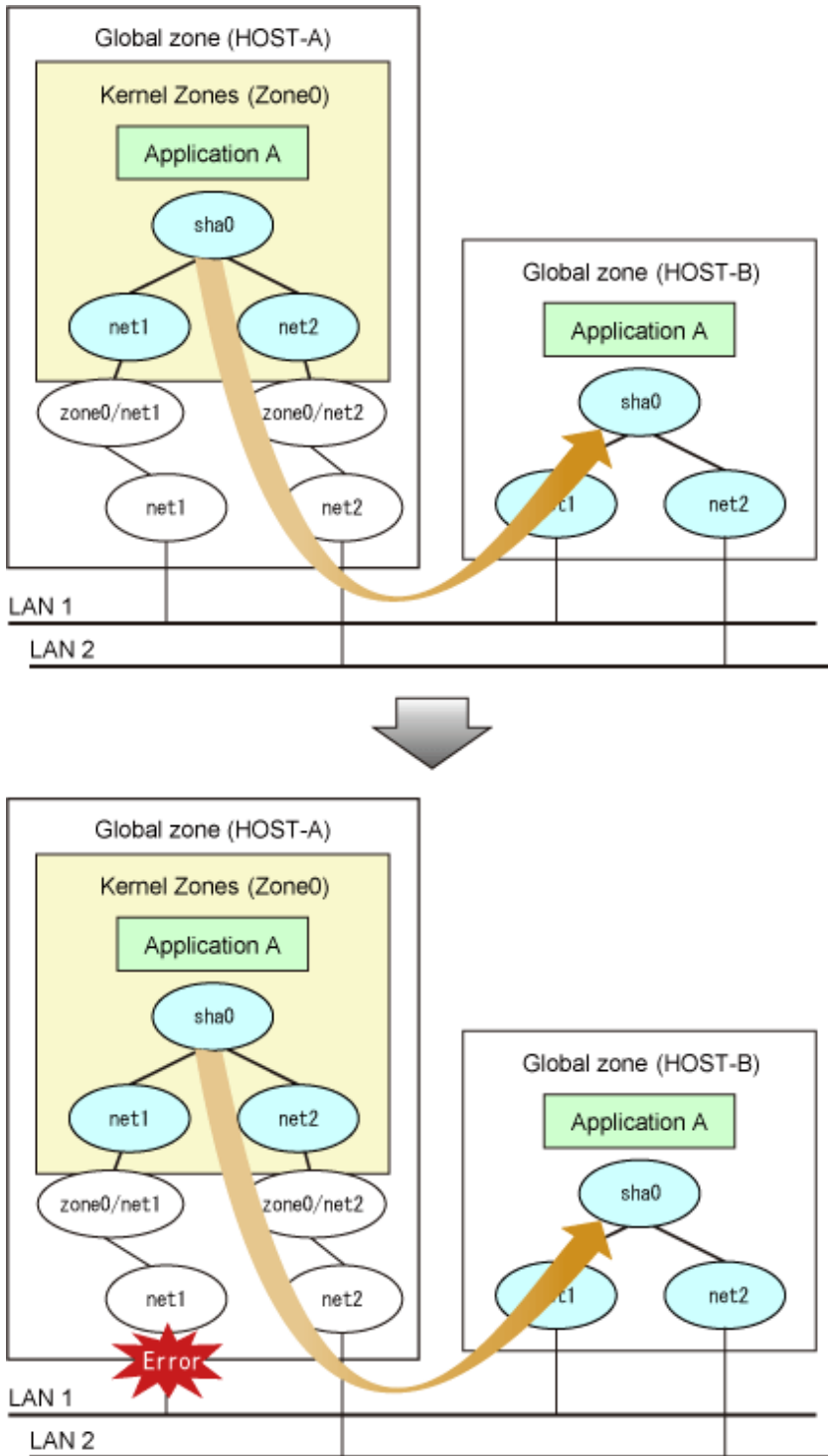


Even if a transmission route fails on the primary interface, the applications on Kernel Zones will be switched over to the secondary physical interface through redundant line control, so operational continuity is never disrupted.

C.4.3.2 Network high-reliability of Kernel Zones (GS/SURE linkage mode)

The following example is for using GS/SURE linkage mode.

Figure C.9 For using GS/SURE linkage mode



Even if a transmission route fails on one of the interfaces that are bundled by the virtual interface, the route will be switched to the other one through redundant line control so that the applications on Kernel Zone can be continued.

C.5 Configuration Procedure for Redundant Line Switching Mode on Solaris Zones

This section describes how to create a Solaris Zone.

C.5.1 Configuration Procedure for Non-Global Zones

The following is a configuration example where the OS version in the global zone is Solaris 11.3.

(1) Create a zone

The following example shows how to create NIC in the anet resource when the following non-global zone name is "zone0."

```
# zonecfg -z zone0
Use 'create' to begin configuring a new zone.
zonecfg:zone0> create
create: Using system default template 'SYSdefault'
zonecfg:zone0> add anet <- Create the anet interface.
zonecfg:zone0:anet> set linkname=net1 <- Specify a NIC name in the zone.
zonecfg:zone0:anet> set lower-link=net1 <- Specify a physical NIC to connect.
zonecfg:zone0:anet> end
zonecfg:zone0> add anet <- Create the anet interface.
zonecfg:zone0:anet> set linkname=net2 <- Specify a NIC name in the zone.
zonecfg:zone0:anet> set lower-link=net2 <- Specify a physical NIC to connect.
zonecfg:zone0:anet> end
zonecfg:zone0> export <- Check the setting.
create -b
set zonepath=/system/zones/%{zonename}
set autoboot=false
set autosutdown=shutdown
set ip-type=exclusive
add anet
set linkname=net0
set lower-link=auto
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
add anet
set linkname=net1
set lower-link=net1
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
add anet
set linkname=net2
set lower-link=net2
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
zonecfg:zone0> commit <- Register the zone.
zonecfg:zone0> exit <- Zone setting is completed.
# zoneadm list -vc <- Check if the zone is properly registered.
  ID NAME                STATUS      PATH                               BRAND  IP
  0  global                running    /                                 solaris shared
  -  zone0                 configured /system/zones/zone0             solaris excl
```

(2) Install the zone

You can install the zone using the following steps.

```
# zoneadm -z zone0 install
The following ZFS file system(s) have been created:
  rpool/VARSHARE/zones/zone0
Progress being logged to /var/log/zones/zoneadm.20180927T092443Z.zone0.install
```



```

Image: Preparing at /system/zones/zone0/root.

Install Log: /system/volatile/install.4117/install_log
AI Manifest: /tmp/manifest.xml.DX2y6a
SC Profile: /usr/share/auto_install/sc_profiles/enable_sci.xml
Zonename: zone0
Installation: Starting ...
<snip.>
Installation: Succeeded

Note: Man pages can be obtained by installing pkg:/system/manual
done.

Done: Installation completed in 627.854 seconds.

Next Steps: Boot the zone, then log into the zone console (zlogin -C)

to complete the configuration process.

Log saved in non-global zone as /system/zones/zone0/root/var/log/zones/zoneadm.
20180927T092443Z.zone0.install
# zoneadm list -vc <- Check if the zone is installed properly.
ID NAME          STATUS      PATH                                BRAND  IP
0 global         running    /                                    solaris shared
- zone0         installed  /system/zones/zone0                solaris excl

```

 **Note**

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

(3) Start the zone

Start the zone using the following steps.

```

# zoneadm -z zone0 boot <- Start the zone.
# zoneadm list -vc
ID NAME          STATUS      PATH                                BRAND  IP
0 global         running    /                                    solaris shared
1 zone0         running    /system/zones/zone0                solaris excl <- Check
if the zone is started properly.

```

(4) Log in to the zone

You can log in to the zone using the following steps:

```

# zlogin zone0
[Connected to zone 'zone0' pts/2]
Oracle Corporation      SunOS 5.11      11.3      September 2017
root@zone0:~#

```

(5) Check the interface state

If you check the interface state on the zone, it will be displayed as follows.

```

root@zone0:~# dladm show-link
LINK          CLASS    MTU    STATE  OVER
net2          vnic    1500  up     ?
net1          vnic    1500  up     ?
net0          vnic    1500  up     ?

```

(6) Log out of the zone

You can log out of the zone using the following steps:

```

root@zone0:~# exit
logout
[Connection to zone 'zone0' pts/2 closed]

```

(7) Change the network setting

You can change the network setting using the following steps.

In the network setting when the zone name is "zone0," the following example shows how to change the physical NIC in the global-zone to be connected to net1 in the non-global zone from net1 to net3.

```

# zonecfg -z zone0
zonecfg:zone0> export <- Check the setting.

create -b
set brand=solaris
set zonepath=/system/zones/{zonename}
set autoboot=false
set autoshutdown=shutdown
set ip-type=exclusive
add anet
set linkname=net2
set lower-link=net2
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
add anet
set linkname=net1
set lower-link=net1
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
add anet
set linkname=net0
set lower-link=auto
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
end
zonecfg:zone0> select anet linkname=net1 <- Select the resource.
zonecfg:zone0:anet> set lower-link=net3 <- Change the physical NIC to net3.
zonecfg:zone0:anet> end
zonecfg:zone0> commit <- Register the zone.
zonecfg:zone0> exit <- Zone setting is completed.

```



See

For more details, see the Solaris manual according to your OS version.

C.5.2 Configuration Procedure for Kernel Zones

The following is an example of configuring Kernel Zones.

(1) Create a zone

The following example shows how to create NIC in the anet resource when the following Kernel Zone name is "zone0".

```
# zonecfg -z zone0
Use 'create' to begin configuring a new zone.
zonecfg:zone0> create -t SYSsolaris-kz
zonecfg:zone0> add anet <- Create the anet interface.
zonecfg:zone0:anet> set lower-link=net1 <- Specify a physical NIC to connect.
zonecfg:zone0:anet> end
zonecfg:zone0> add anet <- Create the anet interface.
zonecfg:zone0:anet> set lower-link=net2 <- Specify a physical NIC to connect.
zonecfg:zone0:anet> end
zonecfg:zone0> export <- Check the setting.
create -b
set autoboot=false
set autosutdown=shutdown
set hostid=0x48bfa8db
add anet
set lower-link=auto
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=0
end
add anet
set lower-link=net1
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=1
end
add anet
set lower-link=net2
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=2
end
add device
set storage=dev:/dev/zvol/dsk/{global-rootzpool}/VARSHARE/zones/{zonename}/disk{id}
set bootpri=0
set id=0
end
add capped-memory
set physical=2G
end
zone0: keysource not exported: does not exist
zonecfg:zone0> commit <- Register a zone.
zonecfg:zone0> exit <- Zone setting is completed.
# zoneadm list -vc <- Check if the zone is properly registered.
ID NAME STATUS PATH BRAND IP
```

| | | | | |
|----------|------------|---|------------|--------|
| 0 global | running | / | solaris | shared |
| - zone0 | configured | - | solaris-kz | excl |

(2) Install the zone

You can install a zone using the following steps.

```
# zoneadm -z zone0 install
Progress being logged to /var/log/zones/zoneadm.20141014T053841Z.zone0.install
pkg cache: Using /var/pkg/publisher.
  Install Log: /system/volatile/install.4478/install_log
  AI Manifest: /tmp/zoneadm3888.5jaiki/devel-ai-manifest.xml
  SC Profile: /usr/share/auto_install/sc_profiles/enable_sci.xml
Installation: Starting ...
<snip.>
Installation: Succeeded
      Done: Installation completed in 237.304 seconds.
# zoneadm list -vc <- Check if the zone is installed properly.
ID NAME          STATUS      PATH          BRAND      IP
0 global         running    /             solaris    shared
- zone0         installed  -             solaris-kz excl
```



Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

(3) Start the zone

Start the zone using the following steps.

```
# zoneadm -z zone0 boot <- Start the zone.
# zoneadm list -vc
ID NAME          STATUS      PATH          BRAND      IP
0 global         running    /             solaris    shared
1 zone0         running    -             solaris-kz excl <- Check if the
zone is started properly.
```

(4) Log in to the zone

You can log in to the zone using the following steps.

```
# zlogin zone0
[Connected to zone 'zone0' pts/5]
Oracle Corporation      SunOS 5.11      11.2      June 2014
#
```

(5) Check the interface state

If you check the interface state on the zone, it will be displayed as follows.

```
# dladm show-link
LINK          CLASS      MTU      STATE      OVER
net0          phys      1500    up         --
net1          phys      1500    up         --
net2          phys      1500    up         --
```

(6) Log out of the zone

You can log out of the zone using the following steps.

```
# exit
logout

[Connection to zone 'zone0' pts/5 closed]
```

(7) Stop the zone

You can stop the zone using the following steps.

```
# zoneadm -z zone0 shutdown
# zoneadm list -vc
```

| ID | NAME | STATUS | PATH | BRAND | IP |
|----|--------|-----------|------|------------|--------|
| 0 | global | running | / | solaris | shared |
| - | zone0 | installed | - | solaris-kz | excl |

(8) Change the network setting

You can change the network setting using the following steps.

In the network setting when the zone name is "zone0", the following example shows how to change the physical NIC in the global-zone to be connected to net1 in the Kernel Zone from net1 to net3.

```
# zonecfg -z zone0
zonecfg:zone0> export <- Check the setting.
create -b
set brand=solaris-kz
set autoboot=false
set autosutdown=shutdown
set hostid=0x48bfa8db
add anet
set lower-link=auto
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=0
end
add anet
set lower-link=net1
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=1
end
add anet
set lower-link=net2
set configure-allowed-address=true
set link-protection=mac-nospoof
set mac-address=auto
set id=2
end
add device
set storage=dev:/dev/zvol/dsk/{global-rootzpool}/VARSHARE/zones/{zonename}/disk{id}
set bootpri=0
set id=0
end
add capped-memory
set physical=2G
```

```

end
add keysource
set raw="{base64}u7WpZB992vHOGnPgggu8q6w=="
end
zonecfg:zone0> select anet_id=1 <- Select the resource.
zonecfg:zone0:anet> set lower-link=net3 <-Change the physical NIC to net3.
zonecfg:zone0:anet> end
zonecfg:zone0> commit <- Register a zone.
zonecfg:zone0> exit <- Zone configuration is completed.

```



See

For further details, see the Solaris manual.

C.6 Examples of Configuring System Environments

This appendix explains how to configure the system environment with redundant network control.

IP addresses used in examples of configuring system environments are all local IP addresses. You can specify these IP addresses with host names.

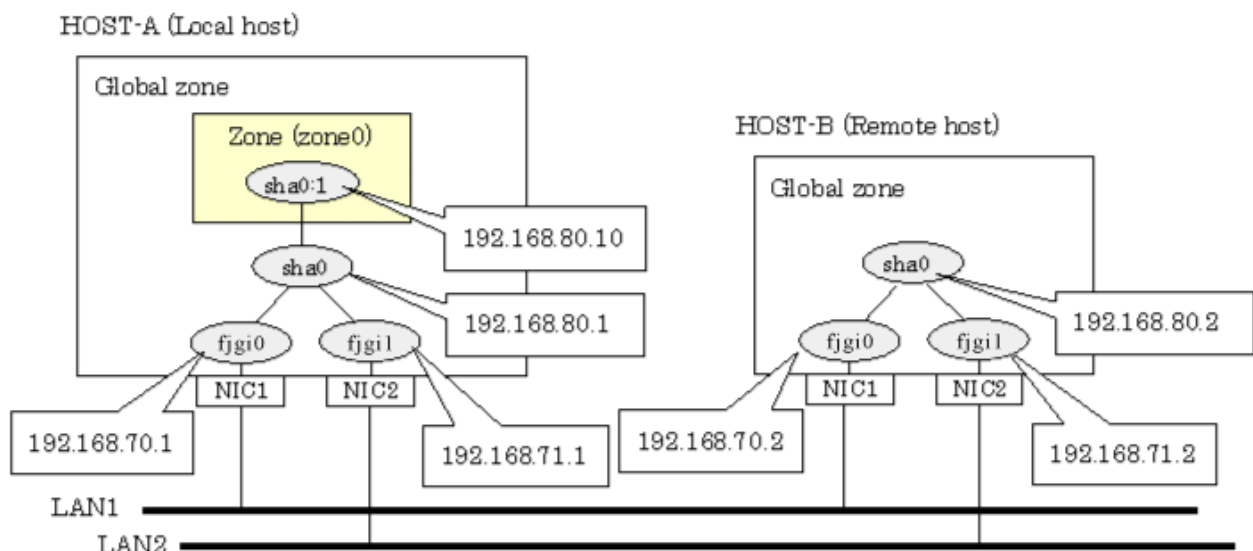
Moreover, interface names listed in examples of configuring system environments vary depending on the environment. Replace interface names according to the environment. For Solaris 11 or later, the default interface name is netX (X means the instance number).

C.6.1 Configuration Example to Ensure Network Reliability of Shared-IP Zone

This section explains how to configure highly reliable networks of the shared-IP zone.

C.6.1.1 Example of configuration with Fast switching mode (IPv4)

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    host11  # HOST-A Physical IP (1)
192.168.71.1    host12  # HOST-A Physical IP (2)
192.168.80.1    hosta   # HOST-A Virtual IP
192.168.70.2    host21  # HOST-B Physical IP (1)
192.168.71.2    host22  # HOST-B Physical IP (2)
192.168.80.2    hostb   # HOST-B Virtual IP
192.168.80.10   zone0   # zone0 Logical IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

5) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

5-1) Create a zone.

```
zonecfg:zone0> create  
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in Fast switching mode.

```
zonecfg:zone0> add net  
zonecfg:zone0:net> set address=192.168.80.10/24  
zonecfg:zone0:net> set physical=sha0  
zonecfg:zone0:net> end
```

Note

For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit  
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```

Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```


[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
```

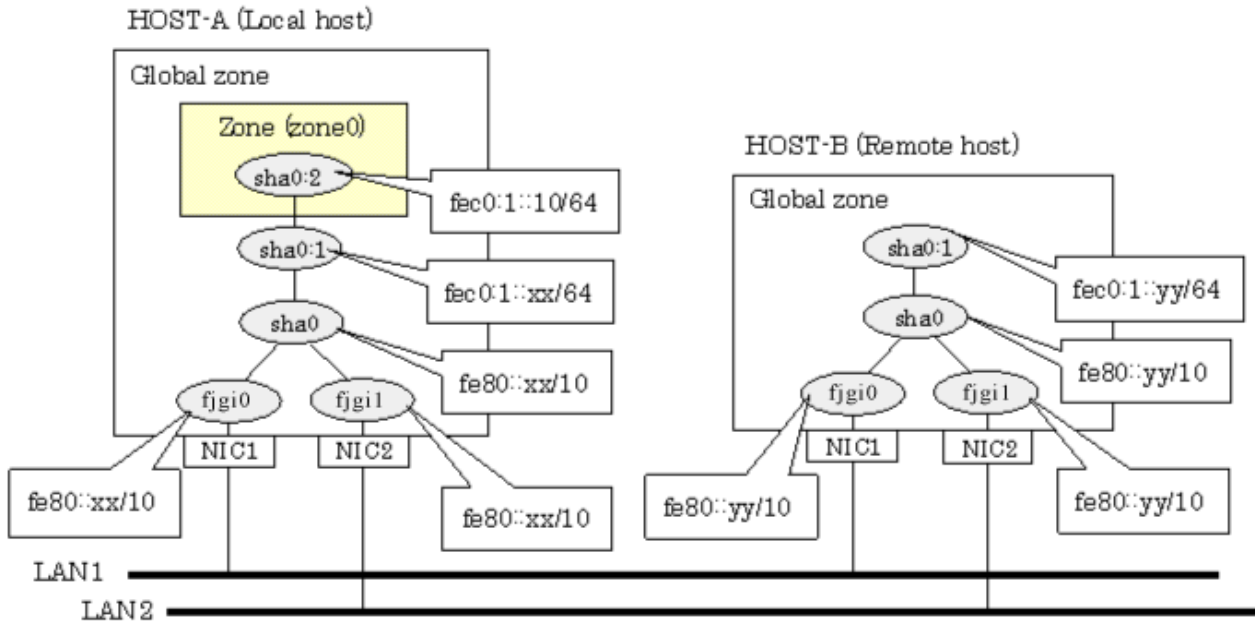
4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

C.6.1.2 Example of configuration with Fast switching mode (IPv6)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0 # sha0 sends Prefix "fec0:1::0/64".
```

Note

In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers.
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

5) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

5-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in Fast switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
```



Note

- For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.
- The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```

Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

[HOST-B]

1) Setting up the system

1-1) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-2) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

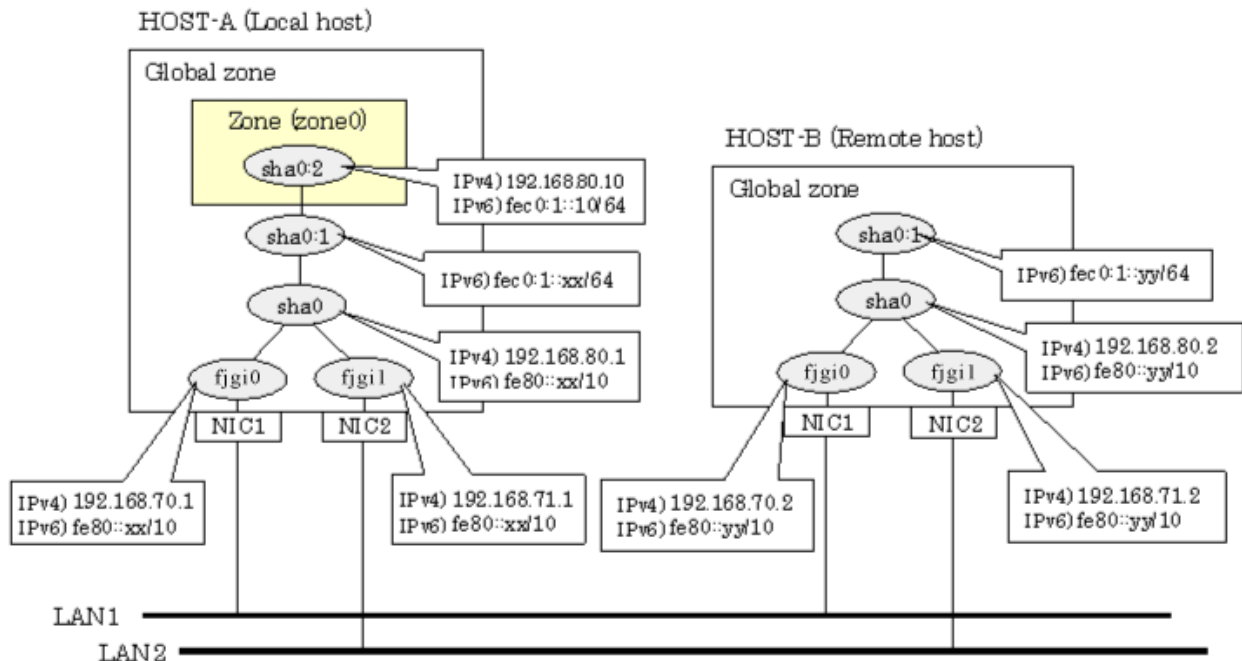
4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

C.6.1.3 Example of configuration with Fast switching mode (IPv4/IPv6)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```

192.168.70.1    host11  # HOST-A Physical IP (1)
192.168.71.1    host12  # HOST-A Physical IP (2)
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.70.2    host21  # HOST-B Physical IP (1)
192.168.71.2    host22  # HOST-B Physical IP (2)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.10   zone0    # zone0 Logical IP
    
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

- Contents of /etc/hostname.fjgi1

```
host12
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host12/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.71.0    255.255.255.0
192.168.80.0    255.255.255.0
```

1-4) Create /etc/inet/ndpd.conf file and set the followings:

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.
prefix fec0:1::0/64 sha0             # sha0 sends Prefix "fec0:1::0/64".
```



In the Solaris server that runs Fast switching mode, configure two or more router as IPv6 router. If the IPv6 router breaks down, it cannot use site-local address to communicate. To prevent this, it is recommended to setup at least two IPv6 routers. For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t fjgi0,fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t net0,net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

4) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

5) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

5-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

5-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in Fast switching mode.

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.80.10/24
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=sha0
zonecfg:zone0:net> end
```

Note

- For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.
- The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.

5-3) Check the above setting.

```
zonecfg:zone0> export
```

5-4) Check setup consistency.

```
zonecfg:zone0> verify
```

5-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

6) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```



Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

7) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file and /etc/hostname.fjgi1 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

- Contents of /etc/hostname.fjgi1

```
host22
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a host22/24 net1/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) Create /etc/inet/ndpd.conf file. Defined information is the same as for HOST-A.

1-5) For Solaris 10

Create /etc/hostname6.fjgi0 and /etc/hostname6.fjgi1 files as an empty file.

1-5) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- Interface net1

```
# /usr/sbin/ipadm create-addr -T addrconf net1/v6
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 and fjgi1 are enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t fjgi0,fjgi1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t net0,net1
# /opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t net0,net1
```

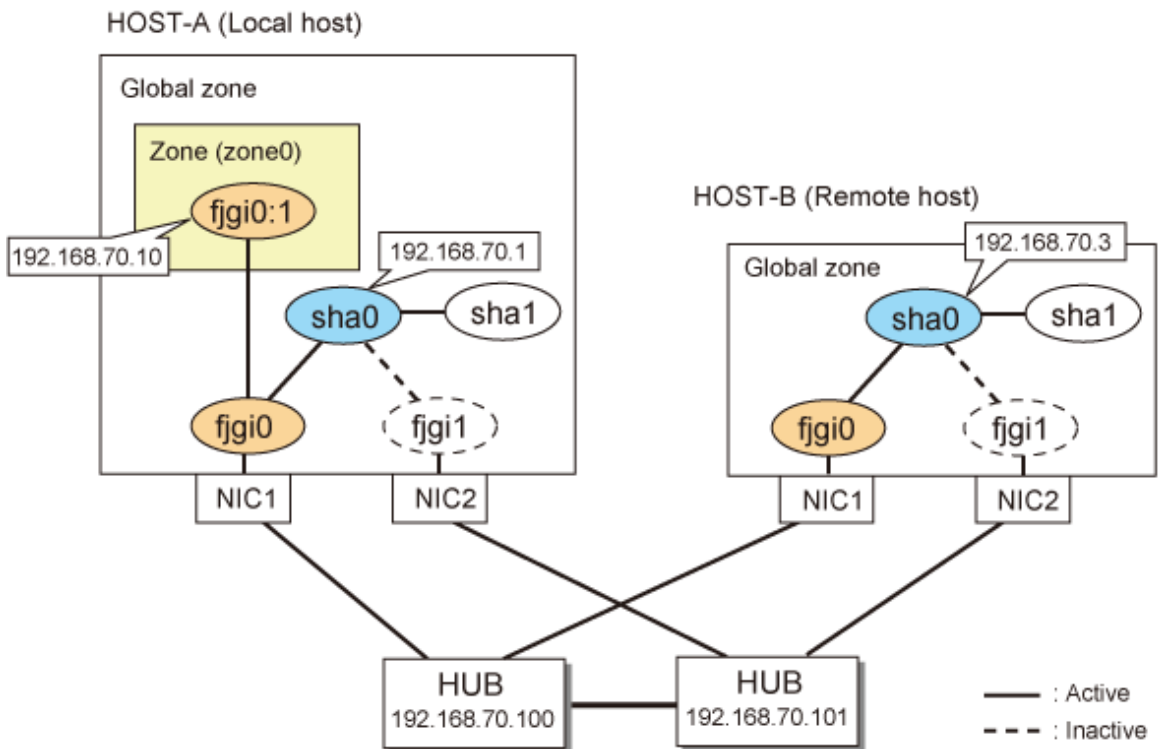
4) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

C.6.1.4 Example of configuration with NIC switching mode (IPv4 logical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.3    hostb    # HOST-B Virtual IP
192.168.70.10   zone0    # zone0 Logical IP
192.168.70.100 swhub1   # Primary HUB IP
192.168.70.101 swhub2   # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file.

- Contents of /etc/hostname.fjgi0

```
hosta
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hosta/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net0,net1
```



Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured by /etc/hostname.fjgi0 file or the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Change the method of deactivating the standby interface

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

9-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

9-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

9-2-1) For Solaris 10

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10/24
zonecfg:zone0:net> set physical=fjgi0
zonecfg:zone0:net> end
```

9-2-1) For Solaris 11 or later

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10/24
zonecfg:zone0:net> set physical=net0
zonecfg:zone0:net> end
```

Note

- For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.
- If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.

9-3) Check the above setting.

```
zonecfg:zone0> export
```

9-4) Check setup consistency.

```
zonecfg:zone0> verify
```

9-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

10) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```



When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

11) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file.

- Contents of /etc/hostname.fjgi0

```
hostb
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostb/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t net0,net1
```

Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured by /etc/hostname.fjgi0 file or the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

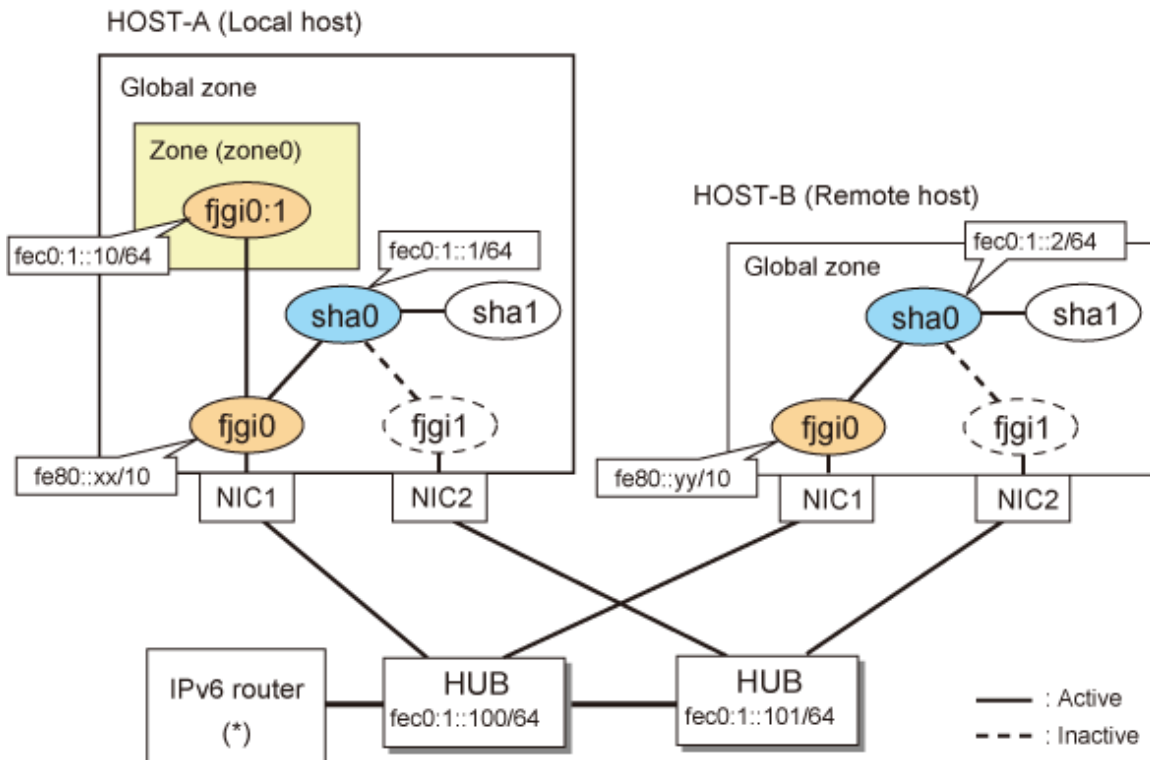
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

C.6.1.5 Example of configuration with NIC switching mode (IPv6 logical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)



Note

An example of configuring `/etc/inet/ndpd.conf` to use Solaris server as an IPv6 router is described below:
For details on `/etc/inet/ndpd.conf`, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 net0 # nt0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

- 1-1) For Solaris10

Create `/etc/hostname6.fjgi0` file as an empty file.

- 1-1) For Solaris11 or later

Set the interface to be used by using the `ipadm(1M)` command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

- 1-2) Define IP addresses and hostnames in `/etc/inet/ipnodes` file.

```
fec0:1::1 v6hosta # HOST-A Virtual IP  
fec0:1::2 v6hostb # HOST-B Virtual IP  
fec0:1::100 swhub1 # Primary HUB IP  
fec0:1::101 swhub2 # Secondary HUB IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure `fjgi0` is enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

- 3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t fjgi0,fjgi1
```

- 3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t net0,net1
```

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

6) Change the method of deactivating the standby interface

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

9) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

9-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

9-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

9-2-1) For Solaris 10

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=fjgi0
zonecfg:zone0:net> end
```

9-2-1) For Solaris 11 or later

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=net0
zonecfg:zone0:net> end
```

Note

- The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.
If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.
- For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.

9-3) Check the above setting.

```
zonecfg:zone0> export
```

9-4) Check setup consistency.

```
zonecfg:zone0> verify
```

9-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

10) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```



When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

11) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

[HOST-B]

1) Setting up the system

1-1) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-1) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-2) Define takeover virtual IP addresses and hostnames in /etc/inet/ipnodes file. Defined information is the same as for HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t net0,net1
```


4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p fec0:1::100,fec0:1::101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

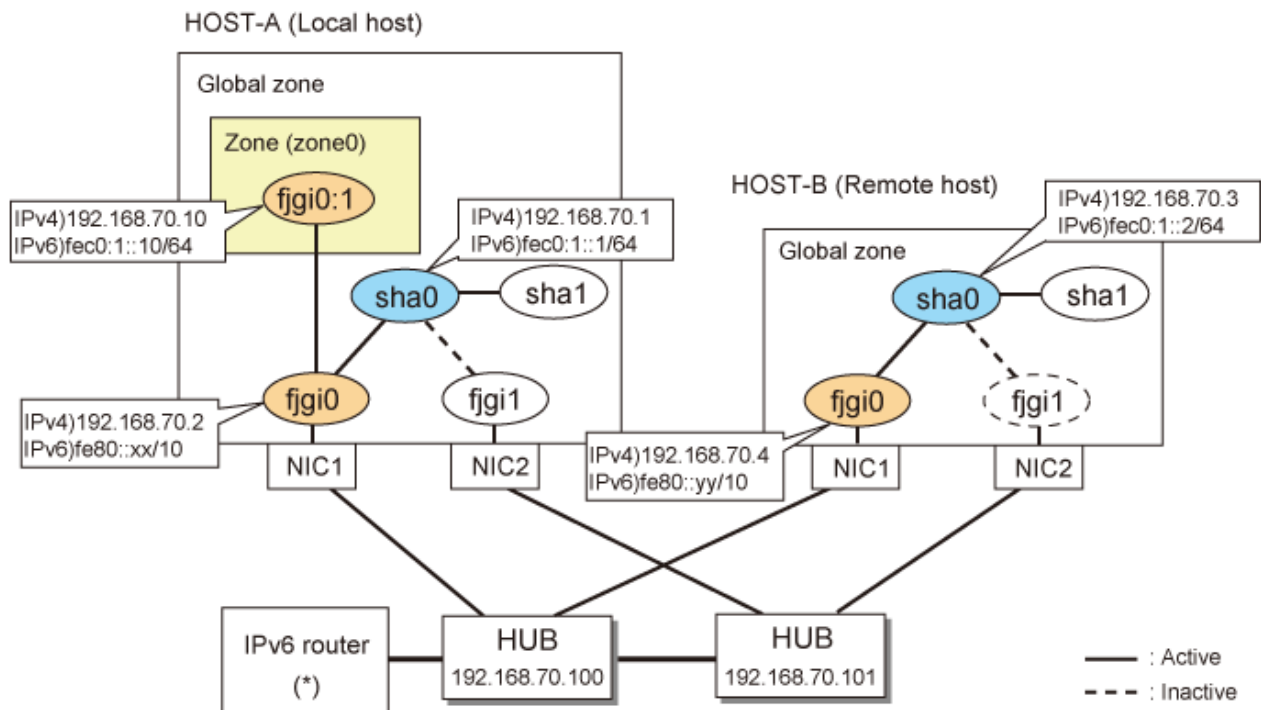
C.6.1.6 Example of configuration with NIC switching mode (IPv4/IPv6)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx, yy in the figure below are assigned automatically by the automatic address configuration.

The dotted line indicates that the interface is inactive.

If the Standby patrol monitoring function is not used, omit 6) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX."
(X is a instance number.)

Note

An example of configuring /etc/inet/ndpd.conf to use Solaris server as an IPv6 router is described below:
For details on /etc/inet/ndpd.conf, refer to the Solaris manual.

- For Solaris 10

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 fjgi0 # fjgi0 sends Prefix "fec0:1::0/64".
```

- For Solaris 11 or later

```
ifdefault AdvSendAdvertisements true # Every interface sends a router advertisement.  
prefix fec0:1::0/64 net0 # net0 sends Prefix "fec0:1::0/64".
```

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1 hosta # HOST-A Virtual IP  
192.168.70.2 host11 # HOST-A Physical IP  
192.168.70.3 hostb # HOST-B Virtual IP  
192.168.70.4 host21 # HOST-B Physical IP  
192.168.70.10 zone0 # zone0 Logical IP  
192.168.70.100 swHub1 # Primary HUB IP  
192.168.70.101 swHub2 # Secondary HUB IP
```

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host11
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0  
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0 255.255.255.0
```

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file.

```
fec0:1::1 v6hosta # HOST-A Virtual IP  
fec0:1::2 v6hostb # HOST-B Virtual IP
```

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t fjgi0,fjgi1
```

3-1) For Solaris 11 or later

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t net0,net1
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

7) Change the method of deactivating the standby interface

```
# /opt/FJSSVhanet/usr/sbin/hanetparam -d plumb
```

8) Activation of virtual interface

```
# /opt/FJSSVhanet/usr/sbin/strhanet
```

9) Starting the HUB monitoring function

```
# /opt/FJSSVhanet/usr/sbin/hanetpoll on
```

10) Set up a zone

Set up a zone by executing the following command:

```
# /usr/sbin/zonecfg -z zone0
```

10-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

10-2) Specify an IP address that is allocated to the zone and the virtual interface name that is defined in NIC switching mode.

10-2-1) For Solaris 10

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10
zonecfg:zone0:net> set physical=fjgi0
zonecfg:zone0:net> end
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=fjgi0
zonecfg:zone0:net> end
```

10-2-1) For Solaris 11 or later

```
zonecfg:zone0> add net
zonecfg:zone0:net> set address=192.168.70.10
zonecfg:zone0:net> set physical=net0
zonecfg:zone0:net> end
zonecfg:zone0> add net
zonecfg:zone0:net> set address=fec0:1::10/64
zonecfg:zone0:net> set physical=net0
zonecfg:zone0:net> end
```

Note

- For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.
- The host name of the IPv6 address cannot be specified for the zone network setting. If you use the IPv6 address, specify an IP address instead of the host name.
If you specify the redundant physical interface in NIC switching mode, specify the primary physical interface.

10-3) Check the above setting.

```
zonecfg:zone0> export
```

10-4) Check setup consistency.

```
zonecfg:zone0> verify
```

10-5) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```

11) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```



Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

12) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) For Solaris 10

Write the hostnames defined above in /etc/hostname.fjgi0 file. If a file does not exist, create a new file.

- Contents of /etc/hostname.fjgi0

```
host21
```

1-2) For Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host21/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

1-4) For Solaris 10

Create /etc/hostname6.fjgi0 file as an empty file.

1-4) For Solaris 11 or later

Set the interface to be used by using the ipadm(1M) command.

- Interface net0

```
# /usr/sbin/ipadm create-addr -T addrconf net0/v6
```

1-5) Define IP addresses and hostnames in /etc/inet/ipnodes file. Defined content is same as HOST-A.

2) Reboot (For Solaris 10)

Run the following command to reboot the system. Make sure fjgi0 is enabled as IPv4/IPv6 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of IPv4 virtual interface

3-1) For Solaris 10

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t
fjgi0,fjgil
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t net0,net1
```

Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi0 or with the ipadm(1M) command.

4) Creation of IPv6 virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
```

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

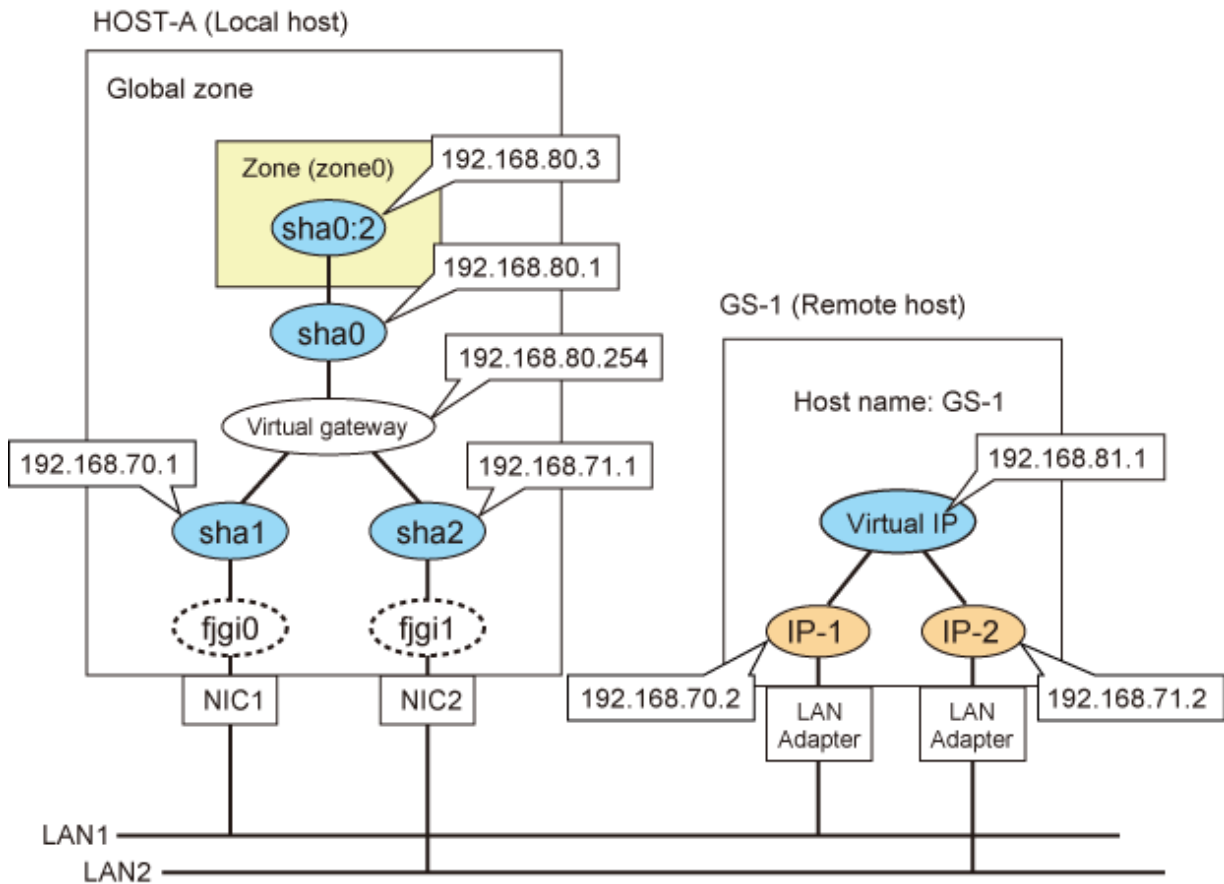
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

C.6.1.7 Example of configuration with GS/SURE linkage mode

This section describes an example configuration procedure of the network shown in the diagram below.

For configuring the GS, refer to the GS manual.

The dotted line indicates that the interface is inactive.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file.

```
192.168.70.1    host11    # HOST-A Virtual IP (mode:n)
192.168.71.1    host12    # HOST-A Virtual IP (mode:n)
192.168.80.1    hosta     # HOST-A Virtual IP (mode:c)
192.168.80.254 virgw     # Virtual gateway
192.168.70.2    gs11     # GS-1 Physical IP IP(IP-1)
192.168.71.2    gs12     # GS-1 Physical IP IP(IP-2)
192.168.81.1    gsa      # GS-1 Virtual IP
```

1-2) Define the subnet mask in the /etc/inet/netmasks file.

```
192.168.70.0 255.255.255.0
192.168.71.0 255.255.255.0
192.168.80.0 255.255.255.0
```

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t fjgi0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t fjgi1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m n -i 192.168.70.1 -t net0
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m n -i 192.168.71.1 -t net1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t sha1,sha2
```

3) Creation of logical virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
```

4) Setting up the virtual gateway

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

5) Setting the Communication target monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.1 -t
192.168.70.2,192.168.71.2 -m on -r on
```

6) Set up a zone

Set up a zone by executing the following command:

```
/usr/sbin/zonecfg -z zone0
```

6-1) Create a zone.

```
zonecfg:zone0> create
zonecfg:zone0> set zonepath=/zones/zone0
```

Note

For Solaris 11 or later, the default network is the exclusive-IP zone (ip-type=exclusive). Change the default network to the shared-IP zone (ip-type=shared) before setting above values. For details, refer to the Solaris manual.

6-2) Check the above setting.

```
zonecfg:zone0> export
```

6-3) Check setup consistency.

```
zonecfg:zone0> verify
```

6-4) Register the setting.

```
zonecfg:zone0> commit
zonecfg:zone0> exit
```


Note

In GS/SURE linkage mode, communication is not supported with the IP address specified by the zonecfg command.

After activating a logical virtual interface and starting up a zone, you need to assign an IP address to a zone by using the ifconfig(1M) command.

7) Install the zone

Install the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 install
```

Note

When a zone is booted for the first time after installation, the zone is in an unconfigured state. Therefore, it is necessary to define an internal zone configuration. Please refer to the manual of Solaris for the definition methods.

8) Start up the zone

Start up the zone by executing the following command:

```
# /usr/sbin/zoneadm -z zone0 boot
```

9) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

10) Assigning the logical interface to the zone

```
# /usr/sbin/ifconfig sha0:2 zone zone0
```

Note

When rebooting a zone for maintenance work, remove the assignment of the logical virtual interfaces to the zone by using the ifconfig command, and then stop the zone.

```
# /usr/sbin/ifconfig sha0:2 -zone
```

If you stop the zone while the logical virtual interfaces are assigned to the zone, logical virtual interfaces are removed by the operating system.

Point

When the zone is automatically started on startup of the system, execute the script in the background that configures the IP address and wait for the startup of a zone from the script "/etc/opt/FJSVhanet/script/service.sh" of the service for Redundant Line Control function of user command execution function. The following is an example of the script.

```
'fjsvhanet-poll')  
#  
# add procedure for fjsvhanet-poll service  
#  
# logger -p daemon.notice "execute script for fjsvhanet-poll service"
```

```
#
/etc/opt/FJSVhanet/script/user_zone.sh &
#
;;
```

[/etc/opt/FJSVhanet/script/user_zone.sh]

```
#!/bin/sh
# target zone name
ZONENAME="zone01"

# get the state of target zone
STATE=`zoneadm -z $ZONENAME list -p | awk -F: '{print $3}'`

# wait for the running state
while [ "$STATE" != "running" ]
do
    sleep 1
    STATE=`zoneadm -z $ZONENAME list -p | awk -F: '{print $3}'`
done

# assign the logical interface (sha0:2) to the zone
/usr/sbin/ifconfig sha0:2 zone $ZONENAME
```

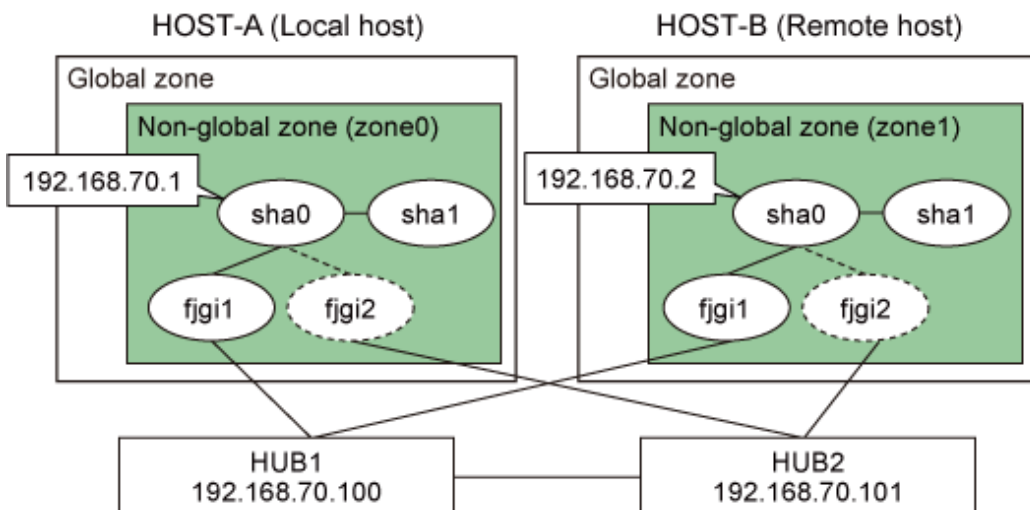
When manually starting the zone, you must assign logical virtual interfaces to the zone by using the ifconfig command every time after starting the zone.

C.6.2 Configuration Example to Ensure Network Reliability of Exclusive-IP Zone

This section explains how to configure highly reliable networks of the exclusive-IP zone.

C.6.2.1 Example of configuration in the exclusive-IP zone (Physical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name "fjgiX" to "netX".
(X is a instance number.)

[HOST-A zone0]

1) Login to the non-global zone

1-1) Login to the non-global zone by executing the following command:

```
# /usr/sbin/zlogin zone0
```

2) Setting up the system

2-1) Define IP addresses and hostnames in the /etc/inet/hosts file.

```
192.168.70.1    zone0    # HOST-A zone0 Virtual IP
192.168.70.2    zone1    # HOST-B zone1 Virtual IP
192.168.70.100  swhub1   # primary HUB IP
192.168.70.101  swhub2   # secondary HUB IP
```

2-2) When the OS type in a non-global zone is Solaris 10

Write the hostnames defined above in the /etc/hostname.fjgi1 file.

- Contents of /etc/hostname.fjgi1

```
zone0
```

2-2) When the OS type in a non-global zone is Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a zone0/24 net1/v4
```

2-3) Define the subnet mask in the /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

3) Reboot (For Solaris 10)

Run the following command to reboot the non-global zone. Run this command from the non-global zone. Make sure fjgi1 is enabled by running the ifconfig command after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

4) Creation of virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t fjgi1,fjgi2
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net1,net2
```



Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.fjgi1 or with the ipadm(1M) command.

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B zone1]

1) Login to the non-global zone

1-1) Login to the non-global zone by executing the following command:

```
# /usr/sbin/zlogin zone1
```

2) Setting up the system

2-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for HOST-A zone0.

2-2) When the OS type in a non-global zone is Solaris 10

Write the hostnames defined above in the /etc/hostname.fjgi1 file.

- Contents of /etc/hostname.fjgi1

```
zone1
```

2-2) When the OS type in a non-global zone is Solaris 11 or later

Set the host by the interface used with the ipadm(1M) command and also by the host name defined above.

- Interface net1

```
# /usr/sbin/ipadm create-ip net1
# /usr/sbin/ipadm create-addr -T static -a zone1/24 net1/v4
```

2-3) Define the subnet mask in the /etc/inet/netmasks file. Defined content is same as for HOST-A zone0.

3) Reboot (For Solaris 10)

Run the following command to reboot the non-global zone. Run this command from the non-global zone. Make sure fjgi1 is enabled by running the ifconfig command after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

4) Creation of virtual interface

4-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t fjgi1,fjgi2
```

4-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t net1,net2
```

Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/hostname.fgi1 or with the ipadm(1M) command.

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

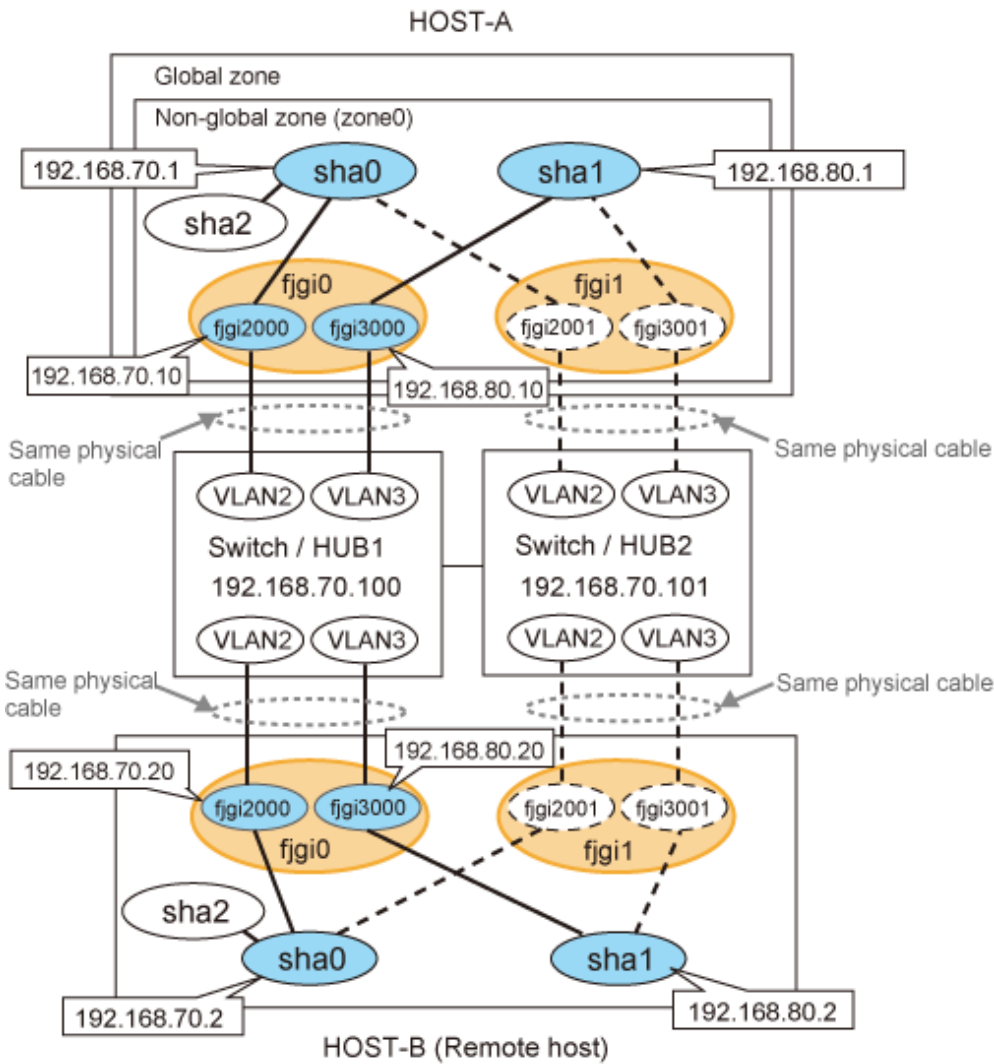
```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

C.6.2.2 Example of configuration with tagged VLAN interfaces (synchronized switching)

This section describes an example configuration procedure of the network shown in the diagram below.



* The configuration above is for Solaris 10.
 For Solaris 11, replace a interface name "fjgiX" to "netX".
 (X is a instance number.)

[HOST-A Global zone]

1) Setting up the system

1-1) For Solaris 11 or later, set the interface to be used by using the dladm(1M) command.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-2) Set non-global zones so that the following interfaces can be used in non-global zones with the exclusive-IP configuration: fjgi2000, fjgi2001, fjgi3000, and fjgi3001 for Solaris 10; net2000, net2001, net3000, and net3001 for Solaris 11 or later. For more information about setting non-global zones, see the manual of Solaris.

[HOST-A zone0]

1) Login to the non-global zone

1-1) Login to the non-global zone by executing the following command:

```
# /usr/sbin/zlogin zone0
```

2) Setting up the system

2-1) Define IP addresses and hostnames in /etc/inet/hosts file.

```
192.168.70.1    zone0a    # zone-0 Virtual IP
192.168.70.10  zone071   # zone-0 Physical IP (Tagged VLAN interface)
192.168.80.1    zone0b    # zone-0 Virtual IP
192.168.80.10  zone081   # zone-0 Physical IP (Tagged VLAN interface)
192.168.70.2    hostc     # HOST-B Virtual IP
192.168.70.20  host72    # HOST-B Physical IP (Tagged VLAN interface)
192.168.80.2    hostd     # HOST-B Virtual IP
192.168.80.20  host82    # HOST-B Physical IP (Tagged VLAN interface)
192.168.70.100 swhub1    # primary Switch/HUB IP
192.168.70.101 swhub2    # secondary Switch/HUB IP
```

2-2) For Solaris 10

Write the hostnames defined above in the /etc/hostname.fjgi2000 file and the /etc/hostname.fjgi3000 file.

- Contents of /etc/hostname.fjgi2000

```
host71
```

- Contents of /etc/hostname.fjgi3000

```
host81
```

2-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a hosta71/24 net2000/v4
```

- Interface net3000

```
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a hosta81/24 net3000/v4
```

2-3) Define the subnet mask in the /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
192.168.80.0    255.255.255.0
```

3) Creation of virtual interface

3-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t fjgi3000,fjgi3001
```

3-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3000, or with the ipadm(1M) command.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

5) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

6) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

7) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the ifconfig command after rebooting the system: fjgi2000 and fjgi3000 for Solaris 10; net2000 and net3000 for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/inet/hosts file. Defined information is the same as for HOST-A zone0.

1-2) For Solaris 10

Write the hostnames defined above in the /etc/hostname /etc/hostname.fjgi2000 file and the /etc/hostname.fjgi3000 file.

- Contents of /etc/hostname.fjgi2000

```
host72
```

- Contents of /etc/hostname.fjgi3000

```
host82
```


1-2) For Solaris 11 or later

Set the host by the interface used with the dladm(1M) command and the ipadm(1M) command and also by the host name defined above.

- Interface net2000

```
# /usr/sbin/dladm create-vlan -l net0 -v 2
# /usr/sbin/ipadm create-ip net2000
# /usr/sbin/ipadm create-addr -T static -a hosta72/24 net2000/v4
```

- Interface net2001

```
# /usr/sbin/dladm create-vlan -l net1 -v 2
```

- Interface net3000

```
# /usr/sbin/dladm create-vlan -l net0 -v 3
# /usr/sbin/ipadm create-ip net3000
# /usr/sbin/ipadm create-addr -T static -a hosta82/24 net3000/v4
```

- Interface net3001

```
# /usr/sbin/dladm create-vlan -l net1 -v 3
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A zone0.

2) Creation of virtual interface

2-1) For Solaris 10

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
fjgi2000,fjgi2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
fjgi3000,fjgi3001
```

2-1) For Solaris 11 or later

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
net2000,net2001
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
net3000,net3001
```



Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/hostname.fjgi2000, in /etc/hostname.fjgi3000, or with the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b on
```

4) Setting up the HUB monitoring function (Synchronized switching)

```
# /opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

5) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
# /opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

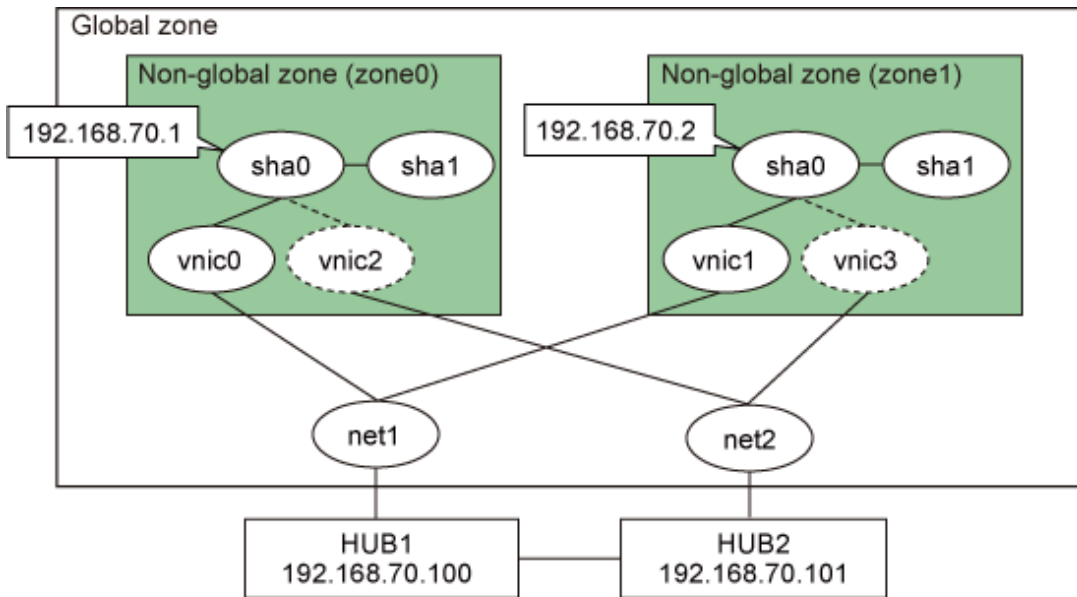
6) Reboot

Run the following command to reboot the system. Make sure the following interfaces are enabled by using the `ifconfig` command after rebooting the system: `fjgi2000` and `fjgi3000` for Solaris 10; `net2000` and `net3000` for Solaris 11 or later.

```
# /usr/sbin/shutdown -y -i6 -g0
```

C.6.2.3 Example of configuration with VNIC (Physical IP takeover)

This section describes an example configuration procedure of the network shown in the diagram below. However, VNIC (interface created by the `dladm(1M)` command) used in this example of configuration is available with Solaris 11 or later. Therefore, this function is not available in Solaris 10.



※The above diagram shows a configuration using the `net` resource.
For a configuration using the `anet` resource, replace `vnicX` with `netX` (X means the instance number).

[Global zone]

1) Setting up the system

- To use the `net` resource when setting non-global zones with the exclusive-IP configuration

1-1) Set the interface to be used by using the `dladm(1M)`.

- Interface `vnic0`

```
# /usr/sbin/dladm create-vnic -l net1 vnic0
```

- Interface `vnic1`

```
# /usr/sbin/dladm create-vnic -l net1 vnic1
```

- Interface `vnic2`

```
# /usr/sbin/dladm create-vnic -l net2 vnic2
```

- Interface `vnic3`

```
# /usr/sbin/dladm create-vnic -l net2 vnic3
```

1-2) Set non-global zones so that the interfaces of vnic0, vnic1, vnic2, and vnic3 can be used.

- To use the anet resource when setting non-global zones with the exclusive-IP configuration

It is not necessary to set the interface to be used by using the dladm(1M).



See

For details on setting non-global zones, see the manual of Solaris 11 or later according to your OS version.

[zone0]

1) Login to the non-global zone

1-1) Login to the non-global zone by executing the following command:

```
# /usr/sbin/zlogin zone0
```

2) Setting up the system

2-1) Define IP addresses and hostnames in the /etc/inet/hosts file.

```
192.168.70.1    zone0    # HOST-A zone0 Virtual IP
192.168.70.2    zone1    # HOST-B zone1 Virtual IP
192.168.70.100  swhub1   # primary HUB IP
192.168.70.101  swhub2   # secondary HUB IP
```

2-2) Set the interface with host names defined above by using the ipadm(1M) command.

- Interface vnic0

```
# /usr/sbin/ipadm create-ip vnic0
# /usr/sbin/ipadm create-addr -T static -a zone0/24 vnic0/v4
```

2-3) Define the subnet mask in the /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

3) Reboot

Run the following command to reboot the non-global zone. Run this command from the non-global zone. Make sure vnic0 is enabled by running the ifconfig command after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

4) Creation of virtual interface

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t vnic0,vnic2
```



Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured by the ipadm command.

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[zone1]

1) Login to the non-global zone

1-1) Login to the non-global zone by executing the following command:

```
# /usr/sbin/zlogin zone1
```

2) Setting up the system

2-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for zone0.

2-2) Set the interface with host names defined above by using the ipadm(1M) command.

- Interface vnic1

```
# /usr/sbin/ipadm create-ip vnic1  
# /usr/sbin/ipadm create-addr -T static -a zone1/24 vnic1/v4
```

2-3) Define the subnet mask in the /etc/inet/netmasks file. Defined content is same as for zone0.

3) Reboot

Run the following command to reboot the non-global zone. Run this command from the global zone. Make sure vnic1 is enabled by running the ifconfig command after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

4) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t vnic1,vnic3
```



Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured by the ipadm command.

5) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

6) Setting up the Standby patrol monitoring function

```
# /opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

7) Activation of virtual interface

```
# /opt/FJShanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJShanet/usr/sbin/hanetpoll on
```

C.6.3 Configuration Example to Ensure Network Reliability of Kernel Zones

For the configuration procedure to ensure network reliability of Kernel Zones, perform the same procedure as for a physical environment on Kernel Zones. For the examples of configuring each system environment, see "[Appendix B Examples of configuring system environments](#)."



Information

For the line switching mode supported in Kernel Zones, see "[C.3 Support Set for Each Redundant Line Switching Mode](#)." Moreover, for the procedure for configuration zones in Kernel Zones, see "[C.5.2 Configuration Procedure for Kernel Zones](#)" or the manual of Solaris.

Appendix D Operation in Oracle VM Environments

This appendix describes the operation of GLS in Oracle VM environments. For details on Oracle VM, see "Oracle VM Server for SPARC Guide."

D.1 Overview of Oracle VM

Oracle VM is a virtual hardware environment which runs using the hypervisor. By dividing one platform into several virtual server environments, operating systems can be run separately.

Redundant Line Control function also ensures network high-reliability on a virtual server (guest domain).

D.2 Network Configuration of Oracle VM

In the Oracle VM environment, the virtual network (vnet) can be defined on a virtual server. The virtual network communicates with other domains or physical networks via the virtual switch (vsw).

Redundant Line Control function makes the network in the Oracle VM environment highly reliable by multiplexing the virtual network (vnet) connected to two virtual switches for each domain.

In the Oracle VM environment, Redundant Line Control function supports the NIC switching mode, the virtual NIC mode, and the GS/SURE linkage mode.



Redundant Line Control function multiplexes networks for each domain. In the Oracle VM environment, install Redundant Line Control function for each domain.

D.3 Support Set for Each Redundant Line Switching Mode

The following table describes how each redundant line control function is supported in Oracle VM environments.

Table D.1 Redundant line control in Oracle VM environments

| | | Domain | |
|-----------------------------|----------------------|----------------|--------------|
| | | Control domain | Guest domain |
| Destination to install GLS | | Control domain | Guest domain |
| Redundant line control mode | Fast switching mode | Not possible | Not possible |
| | NIC switching mode | Possible | Possible |
| | Virtual NIC mode | Possible | Not possible |
| | GS/SURE linkage mode | Not possible | Possible |

GLS: Global Link Services



When making the interface that was created by SR-IOV redundant, use the NIC switching mode.

D.4 Operation of Redundant Line Switching Mode in Oracle VM Environments

This section describes how to monitor the GLS network in Oracle VM environments and how to switch to a normal network when a network failure occurs.

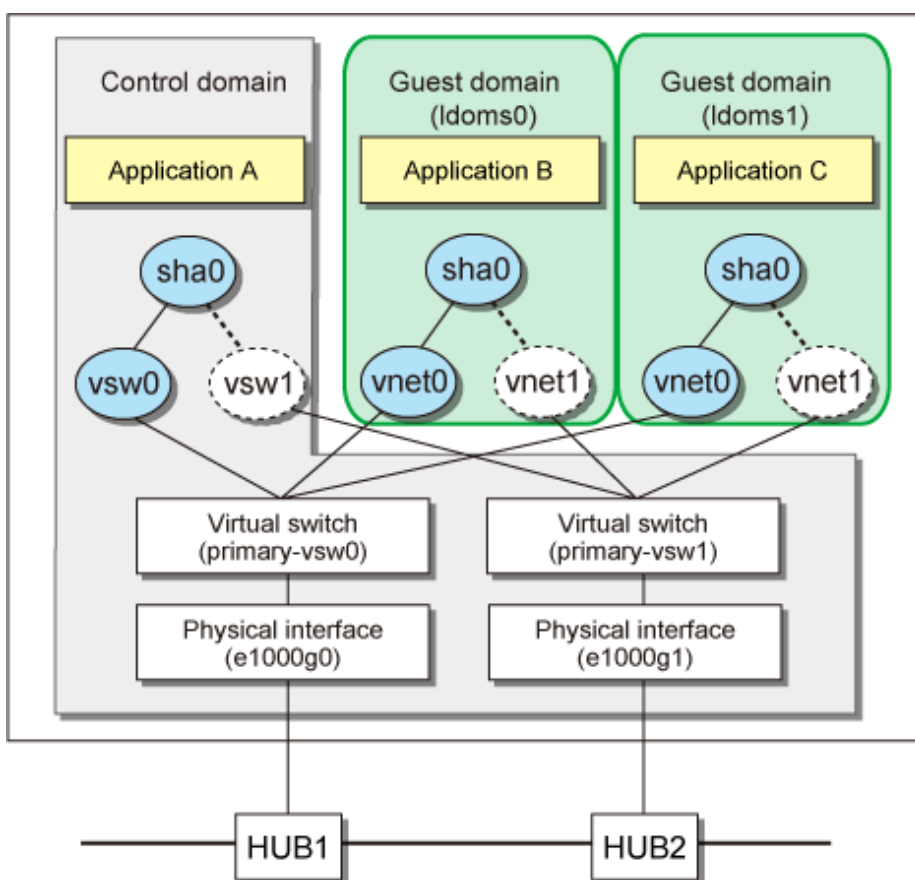
D.4.1 Configuration to ensure reliable networks in Oracle VM environment (Solaris 10)

The following is an example of a configuration for an Oracle VM environment in the case of using the NIC switching mode in Solaris 10 environment.

In the system below, virtual switches "primary-vsw0" and "primary-vsw1" are configured by using physical NICs "e1000g0" and "e1000g1" on the control domain. The virtual network devices "vnet0" and "vnet1" generated on the virtual switches are used on guest domains.

On each domain, GLS multiplexes the virtual devices to configure the virtual interface sha0. For the virtual NIC to be multiplexed, "vsw0" and "vsw1" are specified on the control domain, and "vnet0" and "vnet1" are specified on guest domains.

For configurations using the NIC switching mode, the applications for each domain will perform data transmission using the virtual device ("vsw0" or "vnet0") multiplexed with the NIC switching mode. If an error occurs in the transfer path for the virtual device multiplexed with the NIC switching mode, since the IP address being used with each domain will be taken over from the active interface (vsw0, vnet0) to the standby interface (vsw1, vnet1), the applications on each domain will be able to continue transmission.



Information

- When multiplexing the virtual networks (vsw and vnet) with the NIC switching mode in Oracle VM environments, specify 0:0:0:0:0:0 to the MAC address of the standby patrol. Therefore, the virtual MAC address generated by Oracle VM with the standby patrol function will be used.
- To configure the cluster system environment of Redundant Line Control function in Oracle VM environments, see "Using PRIMECLUSTER in Oracle VM Server for SPARC Environments" in "PRIMECLUSTER Installation and Administration Guide."
- For the HUB monitoring destination, set up items such as the switches outside of the domain. If one has set those within the domain for monitoring, even if there is a malfunction with the physical interface comprising the virtual switches, the malfunction may not be detectable.

D.4.2 Configuration to ensure reliable networks in Oracle VM environment (Solaris 11 or later)

The following is an example of a configuration for an Oracle VM environment in the case of using the NIC switching mode in Solaris 11 or later environment.

In the system below, virtual switches "primary-vsw0" and "primary-vsw1" are configured by using physical NICs "net0" and "net1" on the control domain. Virtual network devices "vnet0" and "vnet1" generated on the virtual switches are used on the guest domains.

The configuration of the control domain is any one of (1) or (2) below.

- (1) GLS multiplexes the physical NICs (net0 and net1) to configure the virtual interface sha0
- (2) GLS multiplexes the virtual network devices (vnet0 and vnet1) to configure the virtual interface sha0

- Solaris 11.2 or later

The configuration (1) is recommended. However, both configurations (1) and (2) are available.

- Solaris 11.1 or earlier

Only the configuration (2) is available.

On the guest domains, GLS multiplexes the virtual network devices (vnet0 and vnet1) to configure the virtual interface sha0.

In this configuration, the applications for each domain will perform data transmission using NIC multiplexed with the NIC switching mode. If an error occurs in the transfer path for NIC multiplexed with the NIC switching mode, since the IP address being used with each domain will be taken over from the active interface (net0, vnet0) to the standby interface (net1, vnet1), the applications on each domain will be able to continue transmission.

Figure D.1 Example when GLS multiplexes the physical NICs (net0 and net1) to configure the virtual interface sha0

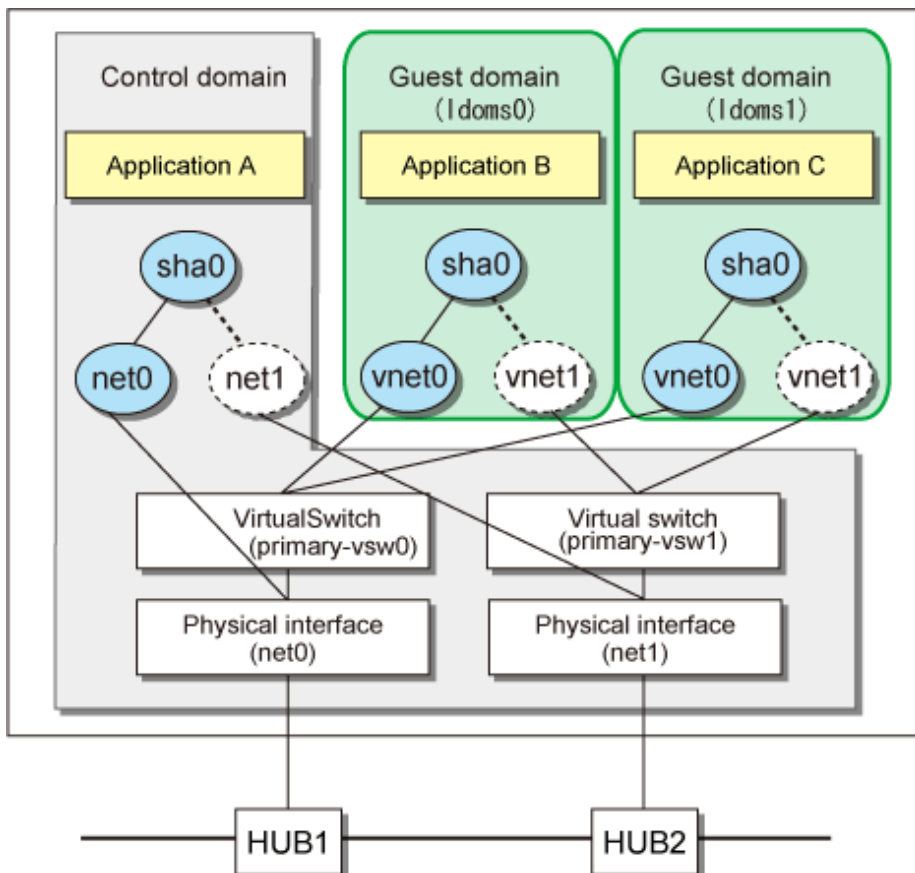
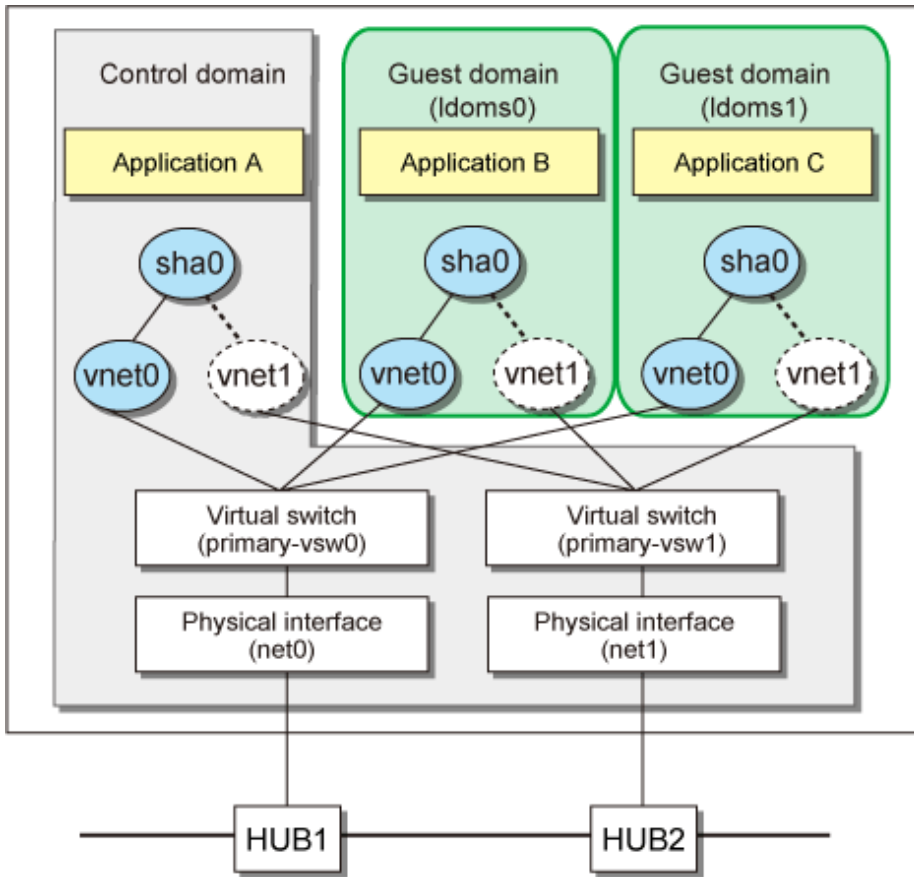


Figure D.2 Example when GLS multiplexes the virtual network devices (vnet0 and vnet1) to configure the virtual interface sha0



Note

In Solaris 11.2 SRU15031 or later (Oracle VM 3.2 or later) environment, the configuration to set the virtual switches as the network devices is no longer supported. As a result, the configuration to multiplex the virtual switches cannot be used in GLS. To multiplex the virtual switches, configure the virtual network devices on the virtual switches to multiplex the virtual network devices as shown in "Figure D.2 Example when GLS multiplexes the virtual network devices (vnet0 and vnet1) to configure the virtual interface sha0."

Information

- When multiplexing the virtual networks (vnet) with the NIC switching mode in Oracle VM environments, specify 0:0:0:0:0:0 to the MAC address of the standby patrol. Therefore, the virtual MAC address generated by Oracle VM with the standby patrol function will be used.
- To configure the cluster system environment of Redundant Line Control function in Oracle VM environments, see "Using PRIMECLUSTER in Oracle VM Server for SPARC Environments" in "PRIMECLUSTER Installation and Administration Guide."
- For the HUB monitoring destination, set up items such as the switches outside of the domain. If one has set those within the domain for monitoring, even if there is a malfunction with the physical interface comprising the virtual switches, the malfunction may not be detectable.

D.5 Procedure for Configuring Redundant Line Control in Oracle VM Environments

According to "Oracle VM Server for SPARC Guide" create the virtual switch service (vsw) on the control domain and add the virtual network device (vnet) to the guest domain. After installing GLS to the control domain and guest domain, perform the configuration operation by using the same procedure as for a physical server.

D.6 Examples of Configuring System Environments

This appendix explains how to configure the system environment with redundant network control.

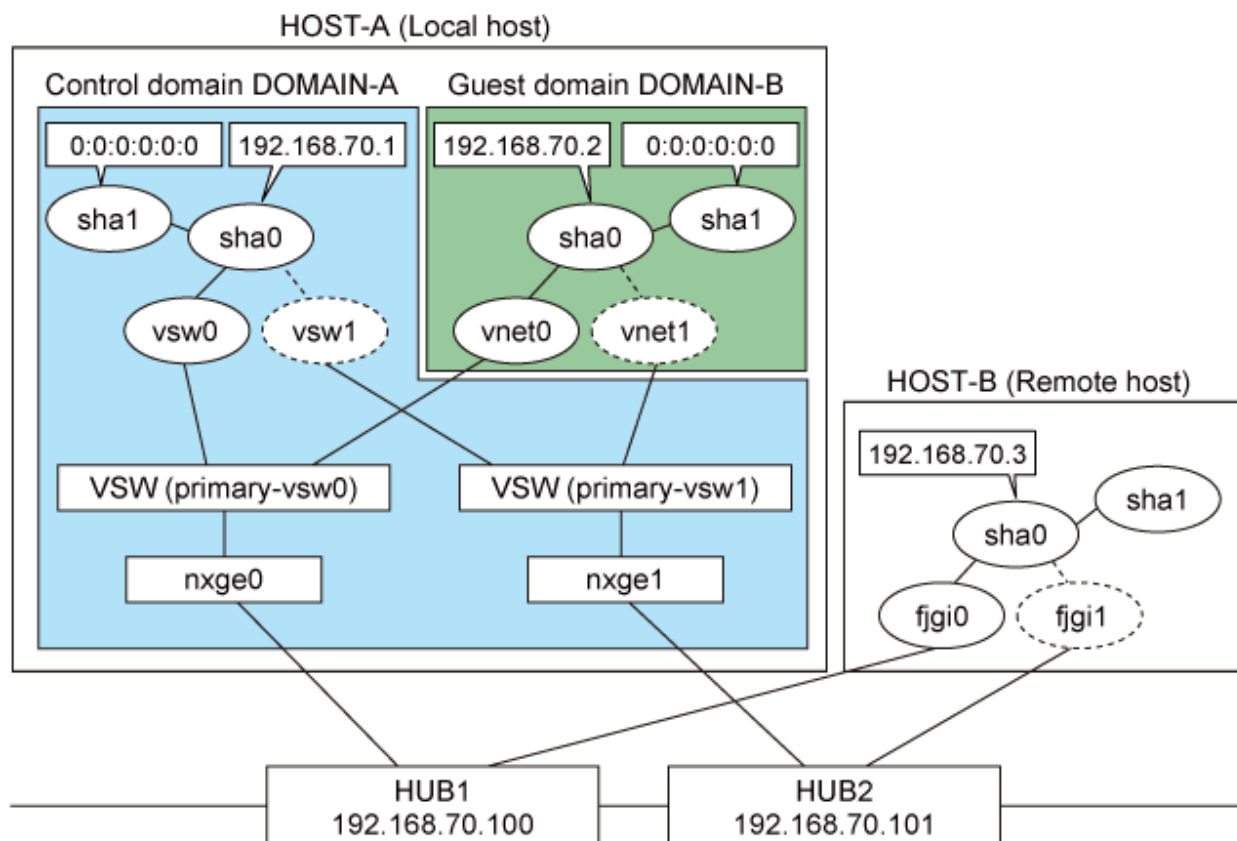
IP addresses used in examples of configuring system environments are all local IP addresses. You can specify these IP addresses with host names.

Moreover, interface names listed in examples of configuring system environments vary depending on the environment. Replace interface names according to the environment.

D.6.1 Example of configuration to ensure reliable networks in Oracle VM environment (Solaris 10)

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 5) in the procedure for setting up on each host.



* The configuration above is for Solaris 10.
For Solaris 11, replace a interface name as followings:

- vsw0 -> net3 - vnet1 -> net1
- vsw1 -> net4 - fjgi0 -> net0
- vnet0 -> net0 - fjgi1 -> net1

[HOST-A: DOMAIN-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file.

```
192.168.70.1    domaina # HOST-A Virtual IP of DOMAIN-A
192.168.70.2    domainb # HOST-A Virtual IP of DOMAIN-B
192.168.70.3    hostb   # Virtual IP of HOST-B
192.168.70.100  swhub1  # primary HUB IP
192.168.70.101  swhub2  # secondary HUB IP
```

1-2) Write the hostnames defined above in the /etc/hostname."interface-name" files.

- Contents of /etc/hostname.vsw0

```
domaina
```

1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Reboot

Run the following command to reboot the system. Make sure vsw0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t vsw0,vsw1
```

Note

Ensure that the physical IP address that is specified to the option '-i' must be the same IP address that is set in /etc/hostname.vsw0.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

Information

When multiplexing the virtual devices (vsw and vnet) in the Oracle VM environment, specify 0:0:0:0:0 to the MAC address of the standby patrol. Therefore, the virtual MAC address assigned to the virtual devices by the standby patrol will be used.

6) Change the method of deactivating the standby interface

```
# /opt/FJSVhanet/usr/sbin/hanetparam -d plumb
```

7) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

8) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-A DOMAIN-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for HOST-A.

1-2) Write the hostnames defined above in the /etc/hostname.vnet0 file.

- Contents of /etc/hostname.vnet0

```
domainb
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure vnet0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t vnet0,vnet1
```



Ensure that the physical IP address that is specified to the option '-i' must be the same IP address that is set in /etc/hostname.vnet0.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```



When multiplexing the virtual devices (vsw and vnet) in the Oracle VM environment, specify 0:0:0:0:0 to the MAC address of the standby patrol. Therefore, the virtual MAC address assigned to the virtual devices by the standby patrol will be used.

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for HOST-A DOMAIN-A.

1-2) Write the hostnames defined above in the /etc/hostname.fjgi0 file.

- Contents of /etc/hostname.fjgi0

```
hostb
```

1-3) Define the subnet mask in the /etc/inet/netmasks file. Defined content is same as HOST-A.

2) Reboot

Run the following command to reboot the system. Make sure fjgi0 are enabled as IPv4 interfaces after rebooting the system.

```
# /usr/sbin/shutdown -y -i6 -g0
```

3) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t fjgi0,fjgil
```



Ensure that the physical IP address that is specified to the option '-e' must be the same IP address that is set in /etc/hostname.fjgi0.

4) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

5) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shal -m p -t sha0
```

6) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

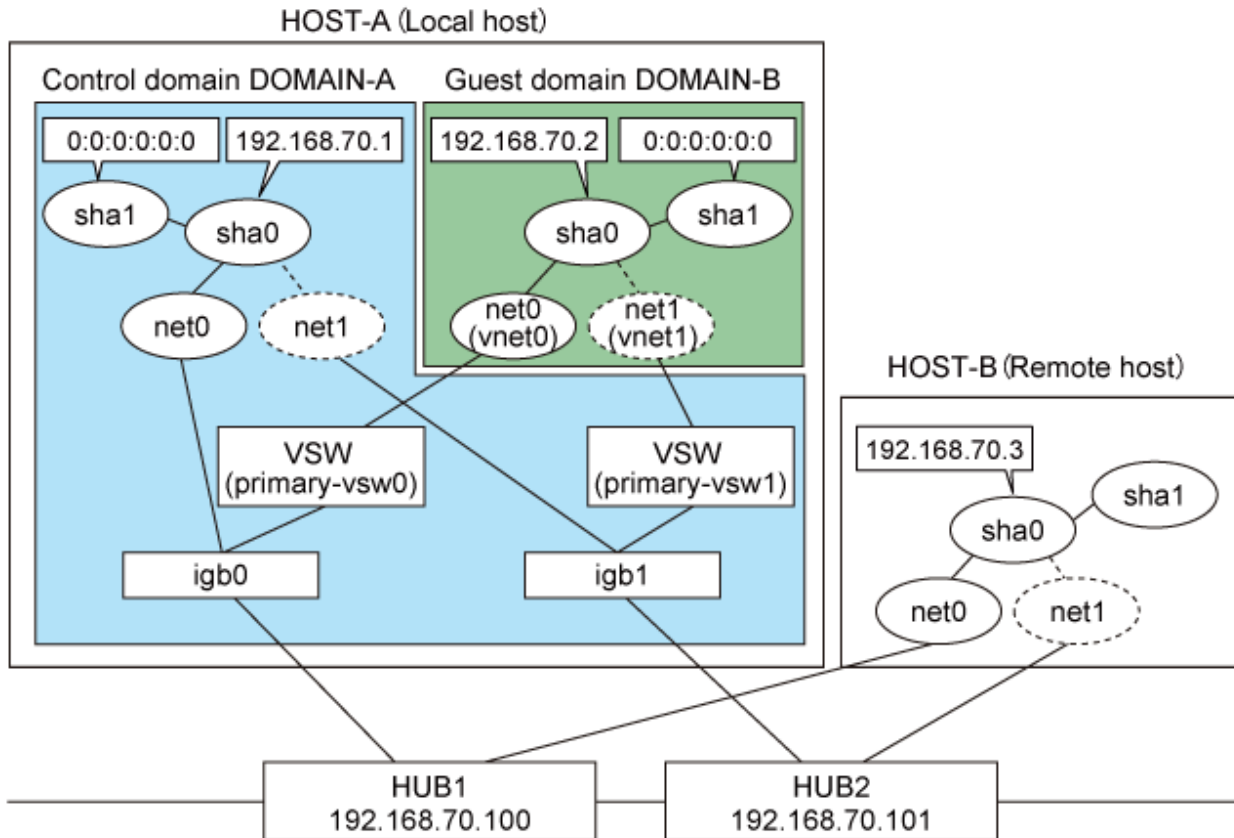
7) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

D.6.2 Example of configuration to ensure reliable networks in Oracle VM environment (Solaris 11 or later)

This section describes an example configuration procedure of the network shown in the diagram below.

If the Standby patrol monitoring function is not used, omit 4) in the procedure for setting up on each host.



[HOST-A: DOMAIN-A]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file.

```
192.168.70.1    domaina # HOST-A Virtual IP of DOMAIN-A
192.168.70.2    domainb # HOST-A Virtual IP of DOMAIN-B
192.168.70.3    hostb   # Virtual IP of HOST-B
192.168.70.100 swhub1  # primary HUB IP
192.168.70.101 swhub2  # secondary HUB IP
```

1-2) By using the ipadm(1M) command, configure the settings with the interface to be used and the host names defined in step 1-1).

- Interface to be used: net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a domaina/24 net0/v4
```

- 1-3) Define the subnet mask in /etc/inet/netmasks file.

```
192.168.70.0    255.255.255.0
```

2) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t net0,net1
```

Note

Ensure that the physical IP address that is specified to the option '-i' must be the same IP address that is set by the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

4) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

5) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-A DOMAIN-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for HOST-A DOMAIN-A.

1-2) By using the ipadm(1M) command, configure the settings with the interface to be used and the host names defined in step 1-1).

- Interface to be used: net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a domainb/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t net0,net1
```

Note

Ensure that the physical IP address that is specified to the option '-i' must be the same IP address that is set by the ipadm(1M) command.

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

4) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

Information

When multiplexing the virtual NIC (vnet) in the Oracle VM environment, specify 0:0:0:0:0 to the MAC address of the standby patrol. Therefore, the virtual MAC address assigned to the virtual NIC by the standby patrol will be used.

5) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

[HOST-B]

1) Setting up the system

1-1) Define IP addresses and hostnames in the /etc/inet/hosts file. Defined information is the same as for HOST-A DOMAIN-A.

1-2) By using the ipadm(1M) command, configure the settings with the interface to be used and the host names defined in step 1-1).

- Interface to be used: net0

```
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a hostb/24 net0/v4
```

1-3) Define the subnet mask in /etc/inet/netmasks file. Defined information is the same as for HOST-A.

2) Creation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t net0,net1
```

Note

Ensure that the physical IP address that is specified to the option '-e' must be the same IP address that is set by the ipadm(1M) command

3) Setting up the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

4) Setting up the Standby patrol monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

5) Activation of virtual interface

```
# /opt/FJSVhanet/usr/sbin/strhanet
```

6) Starting the HUB monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```


Appendix E Cloning Environments

In GLS, the already configured cluster system can be cloned to configure the new cluster system by changing the IP address.

This chapter explains the procedure of cloning through the examples of the single system for each communication mode and the 1:1 active standby cluster system.

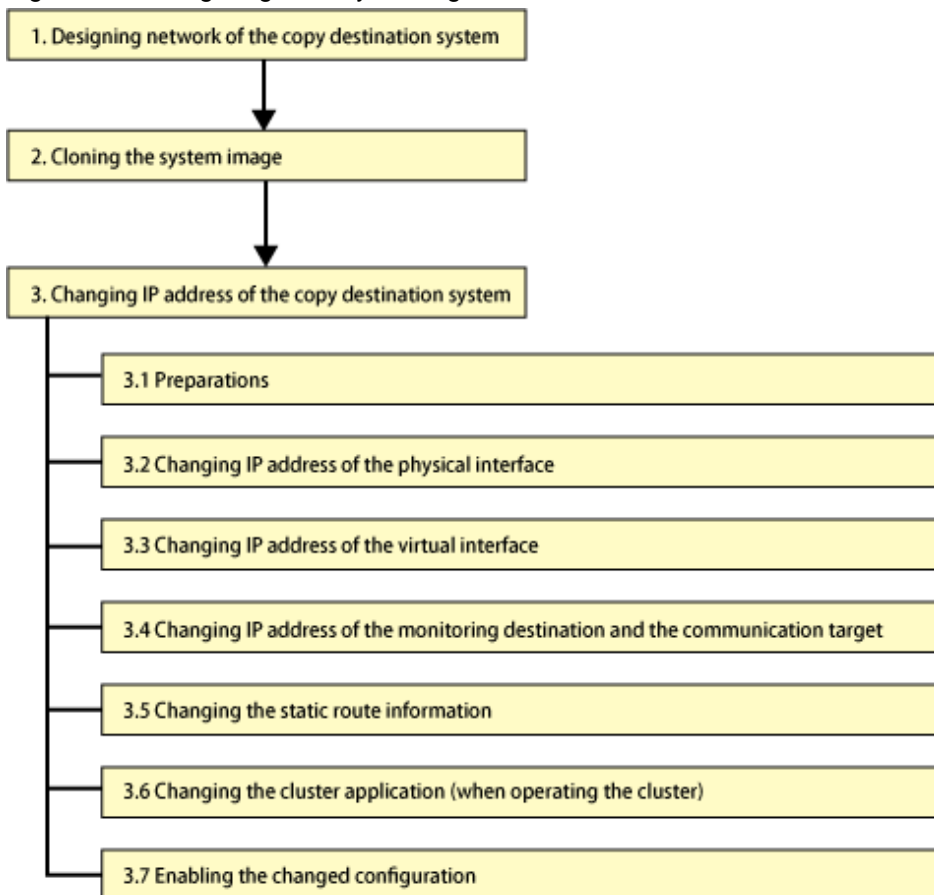
Note

- Cloning follows the condition of the cloning software to be used and the cloning function.
- Before cloning the cluster system, see the manual "PRIMECLUSTER Installation and Administration Guide" to understand the procedure to change the whole cluster system.

Configuring by cloning

The procedure to configure GLS by cloning is as follows.

Figure E.1 Configuring GLS by cloning



E.1 Designing network of the copy destination system

On the TCP/IP network, the unique IP address is assigned to each node to identify the communication target node. If the same IP address is assigned to multiple nodes, normal communication is disabled.

When cloning the system, the setting of the IP address of the copy source system is transferred to the copy destination system without change. Therefore, the IP address must be changed to avoid the duplication of the IP address between the copy destination system and the copy source system. The IP address of the monitoring destination or the IP address of the communication target also must be changed when the copy destination system is connected to the network different from the network on the copy source system. In this case, before cloning

the system, list all the IP addresses that should be changed on the copy destination system, and design how the value of these IP addresses should be changed.

Later sections describe the example of how to design the network for each communication mode.

In the copy destination system, it is assumed that you use the same interface name as the one in the copy source system.

E.1.1 Designing the network of Fast switching mode

When cloning the system of Fast switching mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Physical interface
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system.

[Design example 1: Fast switching mode - Single system]

Below is the design example of how to clone HOST-A of "[B.1.1 Example of the Single system.](#)"

| IP address to be changed | | | Value in copy source | Value in copy destination |
|--------------------------|--------------------|------|----------------------|---------------------------|
| HOST-A | Virtual interface | sha0 | 192.168.80.1 | 192.168.180.1 |
| | Physical interface | net0 | 192.168.70.1 | 192.168.170.1 |
| | | net1 | 192.168.71.1 | 192.168.171.1 |

[Design example 2: Fast switching mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "[B.1.4 Example of the Cluster system \(1:1 Standby\).](#)"

| IP address to be changed | | | Value in copy source | Value in copy destination |
|----------------------------|--------------------|---------|----------------------|---------------------------|
| HOST-A | Virtual interface | sha0 | 192.168.80.1 | 192.168.180.1 |
| | Physical interface | net0 | 192.168.70.1 | 192.168.170.1 |
| | | net1 | 192.168.71.1 | 192.168.171.1 |
| HOST-B | Virtual interface | sha0 | 192.168.80.2 | 192.168.180.2 |
| | Physical interface | net0 | 192.168.70.2 | 192.168.170.2 |
| | | net1 | 192.168.71.2 | 192.168.171.2 |
| Takeover virtual interface | | sha0:65 | 192.168.80.3 | 192.168.180.3 |

E.1.2 Designing the network of NIC switching mode

When cloning the system of NIC switching mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Physical interface
- Monitoring destination IP of the HUB monitoring function (when the destination HUB is different)
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system. Check the IP address of the router on the destination network in advance as well when the copy destination system is connected to the network different from the network on the copy source system.

[Design example 3: NIC switching mode - Single system]

Below is the design example of how to clone HOST-A of "[B.4.1 Example of the Single system without NIC sharing.](#)"

| IP address to be changed | | | Value in copy source | Value in copy destination |
|--------------------------|---------------------|-------|----------------------------------|------------------------------------|
| HOST-A | Logical IP address | sha0/ | 192.168.70.1 | 192.168.170.1 |
| | Physical IP address | net0 | 192.168.70.2 | 192.168.170.2 |
| | HUB | | 192.168.70.100 192.168.70.101 | 192.168.170.100 192.168.170.101 |

[Design example 4: NIC switching mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "B.4.6 Example of the Cluster system (1:1 Standby)."

| IP address to be changed | | | Value in copy source | Value in copy destination |
|----------------------------|---------------------|---------|----------------------------------|------------------------------------|
| HOST-A | Logical IP address | sha0/ | 192.168.70.1 | 192.168.170.1 |
| | Physical IP address | net0 | 192.168.70.2 | 192.168.170.2 |
| | HUB | | 192.168.70.100 192.168.70.101 | 192.168.170.100 192.168.170.101 |
| HOST-B | Logical IP address | sha0/ | 192.168.70.1 | 192.168.170.1 |
| | Physical IP address | net0 | 192.168.70.3 | 192.168.170.3 |
| | HUB | | 192.168.70.100 192.168.70.101 | 192.168.170.100 192.168.170.101 |
| Takeover virtual interface | | sha0:65 | 192.168.70.1 | 192.168.170.1 |

E.1.3 Designing the network of GS/SURE linkage mode

When cloning the system of GS/SURE linkage mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Virtual gateway
- Remote host (when the destination host is different)
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system.

[Design example 5: GS/SURE linkage mode - Single system]

Below is the design example of how to clone HOST-A of "B.7.1 Example of the Single system in GS/SURE connection function (GS communication function)."

| IP address to be changed | | | Value in copy source | Value in copy destination |
|--------------------------|--------------------|------------|----------------------|---------------------------|
| HOST-A | Virtual interface | sha0 | 192.168.80.1 | 192.168.180.1 |
| | Virtual gateway | | 192.168.80.254 | 192.168.180.254 |
| | Virtual interface | sha1 | 192.168.70.1 | 192.168.170.1 |
| | | sha2 | 192.168.71.1 | 192.168.171.1 |
| GS-1 | Virtual IP address | Virtual IP | 192.168.81.2 | 192.168.181.1 |
| | Real IP address | IP-1 | 192.168.70.2 | 192.168.170.2 |
| | | IP-2 | 192.168.71.2 | 192.168.171.2 |

[Design example 6: GS/SURE linkage mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "B.7.5 Example of the Cluster system in GS/SURE connection function (GS communication function)."

| IP address to be changed | | | Value in copy source | Value in copy destination |
|----------------------------|--------------------|------------|----------------------|---------------------------|
| HOST-A | Virtual interface | sha0 | 192.168.80.1 | 192.168.180.1 |
| | Virtual gateway | | 192.168.80.254 | 192.168.180.254 |
| | Virtual interface | sha1 | 192.168.70.1 | 192.168.170.1 |
| | | sha2 | 192.168.71.1 | 192.168.171.1 |
| HOST-B | Virtual interface | sha0 | 192.168.80.1 | 192.168.180.1 |
| | Virtual gateway | | 192.168.80.254 | 192.168.180.254 |
| | Virtual interface | sha1 | 192.168.70.2 | 192.168.170.2 |
| | | sha2 | 192.168.71.2 | 192.168.171.2 |
| Takeover virtual interface | | sha0:65 | 192.168.80.1 | 192.168.180.1 |
| GS-1 | Virtual IP address | Virtual IP | 192.168.81.3 | 192.168.181.3 |
| | Real IP address | IP-1 | 192.168.70.3 | 192.168.170.3 |
| | | IP-2 | 192.168.71.3 | 192.168.171.3 |

E.2 Copying the system image

Copy the system image to the copy destination system.

For the setting values of the OS and other middleware, see the manuals for each product and change them.



- Before starting the copy destination system, unplug the NIC cable, stop the copy source system, or connect the copy destination system with the network separated from the copy source system to prevent the duplicated IP address between the copy destination system and the copy source system.
- After cloning the cluster system, start the copy destination system in single user mode to configure the setting to stop the automatic start of RMS. After this setting, change the configuration of the copy destination system. For details, see "E.3.1 Preparations."

E.3 Changing the setting of the copy destination system

This section explains how to change the setting of GLS in the copy destination system.



- The procedure explained below is available when all the GLS setting is specified by the IP address (decimal dotted notation). When cloning the environment where the virtual interface or the monitoring destination is set by specifying the host name, the GLS setting can be changed by setting the /etc/inet/hosts file in accordance with the copy destination environment with the same host name as in the copy source system, and then, by restarting OS.
- If the IP address is described in the script that is executed by the user command execution function, modify the script file according to the copy destination environment.

E.3.1 Preparations

Before changing the setting of GLS in the copy destination system, configure the following setting.

1. Modifying the /etc/inet/hosts file

Before changing the setting of GLS, start OS in single user mode, and then set the IP address that is previously specified in "[E.1 Designing network of the copy destination system](#)" to the /etc/inet/hosts file. Change the host name if necessary.

Below is the example when changing the IP address of HOST-A in [Design example 1: Fast switching mode - Single system].

[Copy source]

```
192.168.70.1    host11    # HOST-A Physical IP(1)
192.168.71.1    host12    # HOST-A Physical IP(2)
192.168.80.1    hosta     # HOST-A Virtual IP
```

[After change]

```
192.168.170.1  host11    # HOST-A Physical IP(1)
192.168.171.1  host12    # HOST-A Physical IP(2)
192.168.180.1  hosta     # HOST-A Virtual IP
```

2. Stopping automatic start of RMS

When cloning the system where GLS is operated by the cluster, configure the setting to stop the automatic start of RMS. By this setting, when starting OS in multi user mode in the copy destination system, the take over IP address in the copy source system will not be redundantly activated in the copy destination system.

```
# /opt/SMAW/SMAWRrms/bin/hvsetenv HV_RCSTART 0
```

3. Starting OS in multi user mode

Start OS in multi user mode to change the setting of GLS. Before starting OS, unplug the NIC cable, stop the copy source system, or connect the copy destination system with the network separated from the copy source system to prevent the duplicated IP address between the copy destination system and the copy source system.

4. Deleting the setting of takeover virtual interface in GLS

When cloning the system where GLS is operated by the cluster, check that RMS is stopped. After that, delete all the setting of takeover virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n all
```

5. Stopping the virtual interface of GLS

Stop the active virtual interface to change the setting of GLS.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
# /opt/FJSVhanet/usr/sbin/stphanet
```

E.3.2 Changing the IP address of the physical interface

Change the IP address of the physical interface of Fast switching mode and change the IP address of the primary physical interface of NIC switching mode to the IP address that is preliminary specified in "[E.1 Designing network of the copy destination system](#)."

Modify the IP address, and netmask according to the copy destination environment.

Below is the example when changing the setting of net0 in [Design example 1: Fast switching mode - Single system].

- Perform the setting with the interface used with the ipadm(1M) command and the host name defined above.

```
# /usr/sbin/ipadm delete-ip net0
# /usr/sbin/ipadm create-ip net0
# /usr/sbin/ipadm create-addr -T static -a host11/24 net0/v4
```

- Change the subnet mask definition in the `/etc/inet/netmasks` file. Since the subnet mask is defined using a file, the subnet mask of the virtual interface is defined at the same time.

[Before change]

```
192.168.70.0 255.255.255.0
192.168.71.0 255.255.255.0
192.168.80.0 255.255.255.0
```

[After change]

```
192.168.170.0 255.255.255.0
192.168.171.0 255.255.255.0
192.168.180.0 255.255.255.0
```

E.3.3 Changing the IP address of the virtual interface

Change the IP address of the virtual interface according to "E.1 Designing network of the copy destination system." Below is the example for each communication mode.

Fast switching mode

Take the following steps to change the IP address that is described in the design example in "E.1.1 Designing the network of Fast switching mode."

[How to change in design example 1: Fast switching mode - Single system]

1. Changing IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

[How to change in design example 2: Fast switching mode - Cluster system (1:1 Active standby)]

1. Changing IP address of the virtual interface (HOST-A)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

2. Changing IP address of the virtual interface (HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.2
```

3. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.180.3
```

NIC switching mode

Take the following steps to change the IP address that is described in the design example in "E.1.2 Designing the network of NIC switching mode"

[How to change in design example 3: NIC switching mode - Single system]

1. Changing IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e
192.168.170.2
```

[How to change in design example 4: NIC switching mode - Cluster system (1:1 Active standby)]

1. Changing IP address of the virtual interface (HOST-A)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e 192.168.170.2
```

2. Changing IP address of the virtual interface (HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e 192.168.170.3
```

3. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

GS/SURE linkage mode

Take the following steps to change the IP address that is described in the design example in "[E.1.3 Designing the network of GS/SURE linkage mode.](#)"

[How to change in design example 5: GS/SURE linkage mode - Single system]

1. Changing IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha1 -i 192.168.170.1  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha2 -i 192.168.171.1
```

2. Changing IP address of the virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0  
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.180.254
```

[How to change in design example 6: GS/SURE linkage mode - Cluster system (1:1 Active standby)]

1. Changing IP address of the virtual interface (HOST-A)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha1 -i 192.168.170.1  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha2 -i 192.168.171.1
```

2. Changing IP address of the virtual interface (HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha1 -i 192.168.170.2  
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha2 -i 192.168.171.2
```

3. Changing IP address of the virtual gateway (Both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0  
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.180.254
```

4. Reconfiguring the takeover virtual interface (both HOST- and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

E.3.4 Changing the IP address of the monitoring destination and the remote host

Change the IP address in the destination of the HUB monitoring and the IP address of the remote host according to "[E.1 Designing network of the copy destination system.](#)" If the IP address is not necessary to be changed, move to the next step.

Below is the example for each communication mode.

Fast switching mode

The IP address in the monitoring destination is not set. In this case, no IP address is necessary to be changed.

NIC switching mode

Take the following procedure to change the IP address that is described in "[E.1.2 Designing the network of NIC switching mode.](#)"

Execute the hanetpoll modify command to change the IP address in the monitoring destination in each copy destination system.

[Setting of design example 3 and design example 4 common for each HOST]

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha0 -p 192.168.170.100,192.168.170.101
```

GS/SURE linkage mode

Take the following procedure to change the IP address that is described in "[E.1.3 Designing the network of GS/SURE linkage mode.](#)"

Execute the hanetobserv command to change the IP address of remote host in each copy destination system.

[Setting in design example 5]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n GS-1
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.181.1 -t
192.168.170.2,192.168.171.2 -m on -r on
```

[Setting of design example 6 common for each HOST]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n GS-1
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.181.3 -t
192.168.170.3,192.168.171.3 -m on -r on
```

Also change the monitoring setting between the active node and the standby node.

[HOST-A setting of design example 6]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n HOST-B
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.180.1 -t
192.168.170.2,192.168.171.2 -m on -r on
```

[HOST-B setting of design example 6]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n HOST-A
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.180.1 -t
192.168.170.1,192.168.171.1 -m on -r on
```

E.3.5 Changing the setting of cluster application (in cluster operation)

If the take over IP address of the cluster is changed in "[E.3.3 Changing the IP address of the virtual interface](#)", delete the GLs resource before cloning once, and then configure it again.

For details, see "PRIMECLUSTER Installation and Administration Guide".

E.3.6 Enabling the changed setting

After the IP address is changed in the copy destination system, restart OS to check if the IP address is changed properly. Take the following steps:

1. Cancelling the automatic start suspension of RMS

When cloning the system where GLS is operated by the cluster, cancel the setting that suspends the automatic start of RMS.


```
# /opt/SMAW/SMAWRrms/bin/hvsetenv HV_RCSTART 1
```

2. Starting OS in multi user mode

Connect the NIC cable and restart OS in multi user mode.

3. Checking the IP address

After OS is restarted, check if the changed IP address is enabled. Check if the following procedure is complete.

- The changed IP address is set for each physical interface and for each virtual interface.
- The changed IP address is set for the monitoring target IP address and the monitoring works properly (in NIC switching mode).
- The IP address of the communication target The changed IP address is set for the IP address of the communication target, and the monitoring works properly (in GS/SURE linkage mode).
- After RMS is started, the changed take over IP address is set for the active node of the cluster. After that, when the node is switched, the changed take over IP address is set for the standby node (in cluster system).

Appendix F Changes from previous versions

This appendix discusses changes to the GLS specification. It also suggests some operational guidelines.

F.1 Changes from Redundant Line Control function 4.0 to version 4.1A10

The following table shows a list of changes.

Table F.1 List of changes from Redundant Line Control function 4.0 to 4.1A10

| Category | Item | Version |
|-----------------------|----------------------|----------------------------------|
| Incompatible commands | hanetbackup command | PRIMECLUSTER GLS 4.1A10 or later |
| | hanetrestore command | PRIMECLUSTER GLS 4.1A10 or later |

F.1.1 New command

There is no new command for Redundant Line Control function 4.1A10.

F.1.2 Incompatible commands

The following are the incompatible commands of Redundant Line Control function from the previous version. In addition, please refer to "[Chapter 7 Command reference](#)" about the details of each command.

F.1.2.1 hanetbackup command

[Contents]

Now, it is possible to backup the configuration file without taking package version into account.

[Changes]

Before modification

When restoring backup configuration files, the user must keep in track on which version of the backup configuration files belong to.

After modification

When restoring backup configuration files, the user is not required to know the version of the backup configuration files.

F.1.2.2 hanetrestore command

[Contents]

Now, it is possible to restore the configuration file without taking package version into account.

[Changes]

Before modification

When restoring backup configuration files, the user must keep in track on which version of the backup configuration files belong to.

After modification

When restoring backup configuration files, the user is not required to know the version of the backup configuration files.

[Notes]

For the configuration files on Redundant Line Control function 4.1A10, the user is still not required to know the version of the backup configuration files when restoring the backup configuration files.

F.2 Changes from Redundant Line Control function 4.1A10 to version 4.1A20

The following table shows a list of changes.

Table F.2 List of changes from Redundant Line Control function 4.1A10 to 4.1A20

| Category | Item | Version |
|------------------------|---|----------------------------------|
| Incompatible commands | hanetconfig command | PRIMECLUSTER GLS 4.1A20 or later |
| | hanetpoll command | PRIMECLUSTER GLS 4.1A20 or later |
| | hanetobserv command | PRIMECLUSTER GLS 4.1A20 or later |
| Incompatible functions | Resource state monitoring function for standby node | PRIMECLUSTER GLS 4.1A20 or later |
| | Interface state monitoring feature | PRIMECLUSTER GLS 4.1A20 or later |

F.2.1 New command

There are no new commands for Redundant Line Control function 4.1A20.

F.2.2 Incompatible commands

In Redundant Line Control function 4.1A20, the following commands are incompatible commands from the previous versions. In addition, please refer to "[Chapter 7 Command reference](#)" about the details of each command.

F.2.2.1 hanetconfig command

[Contents]

If a host name you specify via hanetconfig command includes invalid characters (except for alphanumeric characters, period, and hyphen) mentioned in RFC952 and RFC1123, it is treated as an error.

[Changes]

Before modification

Invalid characters were not treated as an error.

After modification

Invalid characters were treated as an error.

[Notes]

When migrating the backup configuration setting file to 4.1A20, if the backup configuration settings file (created via hanetbackup command) prior to 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

F.2.2.2 hanetpoll command

[Contents]

If a host name you specify via hanetpoll command includes invalid characters (except for alphanumeric characters, period, and hyphen) mentioned in RFC952 and RFC1123, it is treated as an error.

[Changes]

Before modification

Invalid characters were not treated as an error.

After modification

Invalid characters were treated as an error.

[Notes]

When migrating the backup configuration setting file to 4.1A20, if the backup configuration settings file (created via hanetbackup command) prior to 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

F.2.2.3 hanetobserv command

[Contents]

If a host name you specify via hanetobserv command includes invalid characters (except for alphanumeric characters, period, and hyphen) mentioned in RFC952 and RFC1123, it is treated as an error. For details on this issue, refer to "[7.5 hanetobserv Command](#)".

[Changes]

Before modification

Invalid characters were not treated as an error.

After modification

Invalid characters were treated as an error.

[Notes]

When migrating the backup configuration setting file to 4.1A20, if the backup configuration settings file (created via hanetbackup command) prior to 4.1A10 contains host name written in characters other than alphanumeric, period or hyphen, delete these characters. The virtual interface cannot be activated if the host name contains characters other than alphanumeric, period or hyphen.

F.2.3 Other incompatibles

F.2.3.1 Resource state monitoring function for standby node

[Contents]

When creating cluster application, it is possible to convert standby node of GLS resource into "Standby" state by setting a value of "StandbyTransition" attribute. If neglecting this configuration, it will not monitor the status of standby node of GLS resource. For reference, see "[5.1.4 Monitoring resource status of standby node](#)".

[Changes]

Before modification

GLS resource is set to "Offline" and it does not monitor the standby node of GLS resource state.

After modification

GLS resource is converted as "Standby" status and it monitors the standby node of GLS resource status.

[Notes]

- For GS/SURE linkage mode, the virtual interface on standby node side is inactive and its monitoring function stops. Therefore, it cannot monitor the GLS resource on the standby node. Unlike other modes, GS/SURE linkage mode does not require to specify "StandbyTransition" attribute because it does not run the resource monitoring.
- When attempting to restore the configuration file for 4.1A10 to the cluster system of version 4.1A20 or later using the backup function of a cluster system, the value "StandbyTransition" attribute will not be set as the default value. If this configuration is used without any modification, it does not monitor the GLS resource status in standby node. In such case, temporary stop the cluster application and use RMS Wizard to apply the "StandbyTransition" attribute in the configuration file.

F.2.3.2 Interface state monitoring feature

[Contents]

If a user abruptly uses `ifconfig(1M)` command to change the status of configured physical interface up or down, interface state monitoring function recovers this change to the state where it was initially running. For details on interface state monitoring function, refer to "[2.3.4 Interface status monitoring feature](#)".

[Changes]

Before modification

It does not recover to the original state.

After modification

Recovers to the original state.

[Notes]

In order to terminate the usage of NIC switching mode or to apply changes to physical interfaces, restart interface status monitoring function of the bundled physical interface using `resethanet -s` command after deleting or changing the configuration settings. For details on `resethanet` command, refer to "[7.15 resethanet Command](#)".

F.3 Changes from Redundant Line Control function 4.1A20 to version 4.1A30

The following table shows a list of changes.

Table F.3 List of changes from Redundant Line Control function 4.1A20 to 4.1A30

| Category | Item | Version |
|------------------------|---|----------------------------------|
| Incompatible commands | hanetconfig command | PRIMECLUSTER GLS 4.1A30 or later |
| | hanetpoll command | PRIMECLUSTER GLS 4.1A30 or later |
| | strhanet command | PRIMECLUSTER GLS 4.1A30 or later |
| | stphanet command | PRIMECLUSTER GLS 4.1A30 or later |
| | dsppoll command | PRIMECLUSTER GLS 4.1A30 or later |
| Incompatible functions | Activation timing of GS/SURE linkage mode on the cluster system | PRIMECLUSTER GLS 4.1A30 or later |
| | Verifying the network address | PRIMECLUSTER GLS 4.1A30 or later |
| | Logical number of NIC switching mode | PRIMECLUSTER GLS 4.1A30 or later |

F.3.1 New command

There are no new commands for Redundant Line Control function 4.1A30.

F.3.2 Incompatible commands

In Redundant Line Control function 4.1A30, the following commands are incompatible commands from the previous versions. In addition, please refer to "[Chapter 7 Command reference](#)" about the details of each command.

F.3.2.1 hanetconfig command

[Contents]

Dynamic expansion/modification/deletion is allowed by the command while operating Redundant Line Control function.

[Changes]

Before modification

System reboot reflects configured values, which were added, modified, or deleted during the operation.

After modification

The configured value will be effective immediately after the configuration values were added, modified, or deleted during the operation.

F.3.2.2 hanetpoll command

[Contents]

Starting or stopping the polling process of each virtual interface as well as configuration or display of polling is allowed for the HUB monitoring function on NIC Switching mode.

[Changes]

Before modification

If there were multiple virtual interfaces, starting or stopping polling and configuring/displaying configuration values could not be achieved individually.

Configuration parameters of multiple virtual interfaces would look like the following.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = OFF
  interval(idle)    = 5( 60) sec
  time              = 5 times
  max_retry         = 5 retry
  repair_time       = 5 sec
FAILOVER Status     = YES
Name   HUB Poll Hostname
+-----+-----+-----+-----+-----+
sha0   OFF   swhub1,swhub2
sha1   ON    swhub3,swhub4
```

After modification

Now it is possible to start or stop polling and configure or display the configuration values of each virtual interface in the case where multiple virtual interfaces are present.

Configuration parameters of multiple virtual interfaces would look like the following.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
[ Standard Polling Parameter ]
  interval(idle)    = 5( 60) sec
  times             = 5 times
  max_retry         = 5 retry
  repair_time       = 5 sec
  failover mode     = YES

[ Polling Parameter of each interface ]
Name   Hostname/Polling Parameter
+-----+-----+-----+-----+-----+
sha0   swhub1,swhub2
  hub-hub poll     = OFF
  interval(idle)   = 2( 60) sec
  times            = 3 times
  max_retry        = 5 retry
  repair_time      = 5 sec
  failover mode    = YES
```

| Name | Hostname/Polling Parameter |
|------|-----------------------------|
| sha1 | swhub3,swhub4 |
| | hub-hub poll = ON |
| | interval(idle) = 4(60) sec |
| | times = 5 times |
| | max_retry = 5 retry |
| | repair_time = 5 sec |
| | failover mode = YES |

[Notes]

No modification is applied to polling feature of RIP mode and GS/SURE Linkage mode.

F.3.2.3 strhanet command

[Contents]

If there is more than one virtual interface failed to activate when attempting to activate the virtual interface, error messages will be produced according to the number of virtual interfaces encountered the failure.

[Changes]

Before modification

This command did not generate an error message for every virtual interface.

The following message will be displayed when enabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0,sha1
hanet: 00000: information: normal end.
```

After modification

Now, this command generates an error message for every virtual interface.

The following message will be displayed when enabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0,sha1
hanet: 00000: information: normal end. name=sha0
hanet: 00000: information: normal end. name=sha1
```

[Notes]

You can verify which virtual interface has encountered a failure while running the command.

F.3.2.4 stphanet command

[Contents]

If there is more than one virtual interface failed to inactivate when attempting to inactivate the virtual interface, error messages will be produced according to the number of virtual interfaces encountered the failure.

[Changes]

Before modification

This command did not generate an error message for every virtual interface.

The following message will be displayed when disabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0,sha1
hanet: 00000: information: normal end.
```

After modification

Now, this command generates an error message for every virtual interface.

The following message will be displayed when disabling multiple virtual interfaces.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0,sha1
hanet: 00000: information: normal end. name=sha0
hanet: 00000: information: normal end. name=sha1
```

[Notes]

You can verify which virtual interface has encountered a failure while running the command.

F.3.2.5 dsppoll command

[Contents]

This command displays polling information of each virtual interface on HUB monitoring function. This command only displays polling parameters of one virtual interface.

[Changes]

Before modification

This command did not display the polling parameters of each virtual interface.

The polling status would be displayed as follows.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
Polling Status      = ON
inter(idle)         = 5( 60)
times               = 5
retry               = 5
repair_time         = 5
FAILOVER Status     = YES

Status  Name  Mode  Primary Target/Secondary Target          HUB-HUB
+-----+-----+-----+-----+-----+-----+-----+
  ON   sha0   d    swhub1(ON)/swhub2(WAIT)                   OFF
  ON   sha1   d    swhub3(ON)/swhub4(WAIT)                   ACTIVE
```

After modification

Now, this command displays the polling parameters of each virtual interface.

The polling status would be displayed as follows.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
+-----+-----+-----+-----+-----+-----+-----+
sha0  Polling Status      =      ON
      Primary Target(status) = swhub1(ON)
      Secondary Target(status) = swhub2(WAIT)
      HUB-HUB status        =      OFF
      interval(idle)       =      2( 60)  times          =      3
      repair_time          =      5        retry          =      5
      FAILOVER Status      =      YES
+-----+-----+-----+-----+-----+-----+-----+
sha1  Polling Status      =      ON
```



```

Primary Target(status) = swhub3(ON)
Secondary Target(status) = swhub4(WAIT)
HUB-HUB status = ACTIVE
interval(idle) = 4( 60) times = 5
repair_time = 5 retry = 5
FAILOVER Status = YES
-----+
# /opt/FJSVhanet/usr/sbin/dspoll -n sha0

Polling Status = ON
interval = 2
idle = 60
times = 3
retry = 5
repair_time = 5
failover mode = YES
Status Name Mode Primary Target/Secondary Target HUB-HUB
-----+-----+-----+-----+-----+
ON sha0 d swhub1(ON)/swhub2(WAIT) OFF

```

[Notes]

- If you are using an application that references the output of dspoll command, you must be aware that the output will be different. However, adding '-n' command allows outputting the polling parameter of each virtual interface in the same format before the modification.
- In the case of displaying polling target's parameters using '-c' option (as it has been the usual way of displaying the polling parameter), there are no changes made.

F.3.3 Other incompatibles

F.3.3.1 Activation timing of GS/SURE linkage mode on the cluster system

[Contents]

On an environment where GS/SURE Linkage mode is operating on the cluster system, activate a standby node of a virtual interface (operation mode 'n') from the system startup.

[Changes]

Before modification

During the system starts up, the virtual interface on standby node (operation mode 'n') will not be activated. Instead, the physical interface will be activated.

After modification

During the system starts up, the virtual interface on standby node (operation mode 'n') will be activated. But, the physical interface will not be activated.

[Notes]

You need to pay attention to applications which are aware of the interface name during the communication. Previously, physical interface names have interface names according to each NIC type, such as "hme0" or "hme1", on the standby node. However, they are activated by a virtual interface name, such as "sha1" or "sha2" activate from this version.

F.3.3.2 Verifying the network address

[Contents]

During system configuration or activation of virtual interfaces, Redundant Line Control function now verifies for the consistency of network address for configured virtual IP address and physical IP address. In the case where invalid network address of virtual or physical IP address is configured, it will output the following warning.

Warning:

hanet: 35800: warning: the same network addresses are inappropriate.

Note

Before the hanetconfig command defines virtual interfaces, please define sub-net mask as a /etc/inet/netmasks file. A warning message may be output when sub-net mask is not being defined in advance.

[Changes]

Before modification

It did not check for the consistency of network address for the configured IP addresses.

| Network Address | Redundant Mode | Results | |
|---|----------------------|-----------------------|--------------------|
| Network address of each interface (physical interface, virtual interface, etc.) is consistent | NIC Switching mode | Valid configuration | No warning message |
| | Fast Switching mode | Invalid configuration | |
| | RIP mode | | |
| | GS/SURE linkage mode | | |

After modification

Verifies for the consistency of network address for the configured IP addresses.

| Network Address | Redundant Mode | Results | |
|---|----------------------|-----------------------|----------------------------------|
| Network address of each interface (physical interface, virtual interface, etc.) is consistent | NIC Switching mode | Valid configuration | No warning message |
| | Fast Switching mode | Invalid configuration | Outputs warning message (No.358) |
| | RIP mode | | |
| | GS/SURE linkage mode | | |

[Notes]

- If warning message (No.358) is displayed while running the following commands, check the IP address or net mask value (/etc/netmasks) configured on the physical and virtual interfaces to find no mistake is set. Note that, command process continues execution regardless of the warning messages.
 - /opt/FJShanet/usr/sbin/hanetconfig create
 - /opt/FJShanet/usr/sbin/hanetconfig modify
 - /opt/FJShanet/usr/sbin/hanetconfig copy
 - /opt/FJShanet/usr/sbin/strhanet
 - /opt/FJShanet/usr/sbin/hanetnic add
 - /opt/FJShanet/usr/sbin/hanethvrsc create
- When the definition error of a network address is detected at the time of system starting or RMS starting, a warning message may be output to syslog instead of a standard error (stderr).

F.3.3.3 Logical number of NIC switching mode

[Contents]

In NIC switching mode (logical IP takeover), logical interfaces to which take over IP addresses are added are changed.

[Changes]

Before modification

Logical interface names to which take over IP addresses are added are assigned in the order of definition for virtual interfaces.

After modification

Logical interface names to which take over IP addresses are added are automatically assigned in the order of activation by the operating system.

F.4 Changes from Redundant Line Control function 4.1A30 to version 4.1A40

The following table shows a list of changes.

Table F.4 List of changes from Redundant Line Control function 4.1A30 to 4.1A40

| Category | Item | Version |
|------------------------|---|----------------------------------|
| Incompatible command | None | - |
| Incompatible functions | Check for consistency between Solaris Zones and network configuration | PRIMECLUSTER GLS 4.1A40 or later |
| | Reserve takeover virtual interface for fast switching mode | PRIMECLUSTER GLS 4.1A40 or later |

F.4.1 New command

There are no new commands for Redundant Line Control function 4.1A40.

F.4.2 Incompatible command

No commands in the Redundant Line Control function 4.1A40 are incompatible from the previous versions.

F.4.3 Other incompatibles

F.4.3.1 Check for consistency between Solaris Zones and network configuration

[Contents]

If the shared-IP zone is already set on the system in fast switching or NIC switching mode, check consistency between the shared-IP zone and network configuration.

If one of the following warning messages is output during environment settings, it is necessary to check the network configuration in the shared-IP zone.

Messages:

```
hanet: 36301: warning: IP address is already defined in zones. zone=<zone_name>
hanet: 36401: warning: interface name is defined in zones. zone=<zone_name>
hanet: 36501: warning: secondaryIF is specified in zones. zone=<zone_name>
```



See

For corrective action against each message, see "A.1.2 Error output message (numbers 100 to 500)".

[Changes]

Before modification

The network configuration in the Solaris Zones are not recognized.

After modification

Consistency between the Solaris Zones and network configuration is checked.

[Notes]

- Consistency between the Solaris Zones and network configuration will be checked regardless of zone startup or stop if the zone is already set on the system.
- Consistency between the Solaris Zones and network configuration will not be checked if the network is configured first then the zone is set on the system.

F.4.3.2 Reserve takeover virtual interface for fast switching mode

[Contents]

If the virtual interface in fast switching is registered as a cluster takeover resource with the "hanethvrsc" command, it will use the logical ID No.65 or later like "shaX:65" and "shaX:66".

If the virtual interface in fast switching is specified for multiple zones, the logical ID will be the same as that for the takeover virtual interface. However, the logical virtual interfaces like "shaX:65" and "shaX:66" will be generated in advance when the Redundant Line Control function is started then the cluster takeover virtual interface will automatically be reserved. So, the same logical ID will not be used for multiple zones, and the cluster takeover virtual interface can be used.

[Changes]

Before modification

When the virtual interface and take over IP address are set with the "hanethvrsc" command, the takeover virtual interfaces like "shaX:65" and "shaX:66" will not be reserved.

See the following output example of the "ifconfig" command after the virtual interface and take over IP address settings.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ffffffff
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.100.10 netmask ffffffff broadcast 192.168.100.255
    ether XX:XX:XX:XX:XX:XX
hme1: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 192.168.101.10 netmask ffffffff broadcast 192.168.101.255
    ether XX:XX:XX:XX:XX:XX
hme2: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
    inet 192.168.102.10 netmask ffffffff broadcast 192.168.102.255
    ether XX:XX:XX:XX:XX:XX
cip0: flags=10080c1<UP,RUNNING,NOARP,PRIVATE,IPv4> mtu 1500 index 6
    inet 192.168.1.1 netmask ffffffff
sha0: flags=1000863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
    inet 192.168.200.10 netmask ffffffff broadcast 192.168.200.255
    ether XX:XX:XX:XX:XX:XX
```

After modification

When the virtual interface and take over IP address are set with the "hanethvrsc" command, the take over virtual interfaces like "shaX:65" and "shaX:66" will automatically be reserved.

See the following output example of the "ifconfig" command after the virtual interface and take over IP address settings.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 192.168.100.10 netmask ffffffff broadcast 192.168.100.255
    ether XX:XX:XX:XX:XX:XX
hme1: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 192.168.101.10 netmask ffffffff broadcast 192.168.101.255
    ether XX:XX:XX:XX:XX:XX
hme2: flags=1000863<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 4
    inet 192.168.102.10 netmask ffffffff broadcast 192.168.102.255
    ether XX:XX:XX:XX:XX:XX
cip0: flags=10080c1<UP,RUNNING,NOARP,PRIVATE,IPv4> mtu 1500 index 6
    inet 192.168.1.1 netmask ffffffff00
sha0: flags=1000863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
    inet 192.168.200.10 netmask ffffffff00 broadcast 192.168.200.255
    ether XX:XX:XX:XX:XX:XX
sha0:65: flags=1000862<BROADCAST,NOTRAILERS,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
    inet 0.0.0.0 netmask 0
```



The "ifconfig" command outputs the takeover virtual interface (sha0:65). The environment settings and operation of a cluster system are the same as before.

[Notes]

- When a cluster takeover virtual interface is registered, it will be reserved regardless of availability of zones.
- The generated takeover virtual interface is "down", and "0.0.0.0" is allocated to the IP address. The take over IP address is allocated during RMS startup then the interface will be "up".

F.5 Changes from Redundant Line Control function 4.1A40 to version 4.2A00

There is no change.

F.6 Changes from Redundant Line Control function 4.2A00 to version 4.3A10

The following table shows a list of changes.

Table F.5 List of changes from Redundant Line Control function 4.2A00 to 4.3A10

| Category | Item | Version |
|------------------------|---------------------------------|----------------------------------|
| New command | None | PRIMECLUSTER GLS 4.3A10 or later |
| Incompatible commands | dsppoll command | PRIMECLUSTER GLS 4.3A10 or later |
| | hanetpoll command | PRIMECLUSTER GLS 4.3A10 or later |
| Incompatible functions | Link status monitoring function | PRIMECLUSTER GLS 4.3A10 or later |
| | User command execution function | PRIMECLUSTER GLS 4.3A10 or later |

| Category | Item | Version |
|----------|------------------------|----------------------------------|
| | Virtual gateway | PRIMECLUSTER GLS 4.3A10 or later |
| | Standby patrol | PRIMECLUSTER GLS 4.3A10 or later |
| | RIP mode | PRIMECLUSTER GLS 4.3A10 or later |
| | Self-checking function | PRIMECLUSTER GLS 4.3A10 or later |

F.6.1 New command

F.6.1.1 hanetgw command

[Contents]

Commands to set, delete, and display virtual gateways required when using GS/SURE linkage mode are added. For details, see "[7.16 hanetgw Command](#)".

[Changes]

Before modification

Commands to set, delete, and display virtual gateways required when using GS/SURE linkage mode were not provided.

After modification

Commands to set, delete, and display virtual gateways required when using GS/SURE linkage mode are added.

F.6.2 Incompatible commands

In Redundant Line Control function 4.3A10, the following commands are incompatible commands from the previous versions.

In addition, please refer to "[Chapter 7 Command reference](#)" about the details of each command.

F.6.2.1 dsppoll command

[Contents]

For the monitoring information for each virtual interface, this changes the status displayed with "Polling Status."

[Changes]

Before modification

If there is even just one enabled HUB monitoring, the "Polling Status" will be displayed as ON.

If there is not even one enabled HUB monitoring, the "Polling Status" will be displayed as OFF.

After modification

If the HUB monitoring for the specified virtual interface is enabled, the "Polling Status" will be displayed as ON.

If the HUB monitoring for the specified virtual interface is disabled, the "Polling Status" will be displayed as OFF.

F.6.2.2 hanetpoll command

[Contents]

The condition for settings to be enabled is changed in the case that parameters of the HUB monitoring function are set to the specific virtual interface by using the -n option of the hanetpoll on command.

[Changes]

Before modification

If parameters of the HUB monitoring function are changed after adding the definition of the virtual interface, the settings are enabled after restarting the Redundant Line Control function.

After modification

If parameters of the HUB monitoring function are changed after adding the definition of the virtual interface, the settings are enabled immediately.

F.6.3 Other incompatibles

F.6.3.1 Link status monitoring function

[Contents]

Enabling the link status monitoring function in NIC switching mode allows NICs to be changed without waiting for a time out from the HUB monitoring (HUB to HUB monitoring) when a NIC link is down.

Moreover, to detect an error by the transfer path monitoring and switch NICs, check the link status of the target beforehand. If the target is in the link down state and the state continues for 5 seconds or longer (when the standby patrol is set: 2.5 seconds or longer), restrict switching NICs.

This function is enabled by the -l option of the hanetpoll command.

[Changes]

Before modification

Even when the transmission route fails when a NIC link is down, the NIC is not changed until the failure is detected by the HUB monitoring (HUB to HUB monitoring).

If an error is detected by the transfer path monitoring, switching is performed regardless of whether the link status of the target NIC.

After modification

When the transmission route fails when a NIC link is down, the NIC is changed without waiting for the failure detection by the HUB monitoring (HUB to HUB monitoring).

When an error is detected by the transfer path monitoring, restrict switching if the target NIC is in the link down state.

F.6.3.2 User command execution function (Setup file for NIC switching mode)

[Contents]

In NIC switching mode (Logical IP takeover), you can execute any command along with activation and inactivation of physical interfaces.

[Changes]

Before modification

In NIC switching mode (Logical IP takeover), scripts are not called on activation and inactivation of physical interfaces.

After modification

In NIC switching mode (Logical IP takeover), scripts are called on activation and inactivation of physical interfaces.

F.6.3.3 User command execution function (Setup file of the service for Redundant Line Control function)

[Contents]

The configuration file for Redundant Line Control function was added. For details see "[3.6.10 Setting User command execution function.](#)"

[Changes]

Before modification

There is no corresponding script.

After modification

- /etc/opt/FJSVhanet/script/service.sh

You can start or restart an arbitrary service or application in conjunction with the transfer path monitoring service for Redundant Line Control function (svc:/network/fjsvhanet-poll) or the service for Redundant Line Control function (svc:/network/fjsvhanet).

- /etc/opt/FJSVhanet/script/monitor

You can start or restart an arbitrary service or application in conjunction with the self-checking function.

F.6.3.4 Virtual gateway

[Contents]

By setting a virtual gateway in GS/SURE linkage mode, applications for which local addresses cannot be fixed to virtual IP addresses become available.

[Changes]**Before modification**

The requirement for user applications that can be operated in this mode is as follows:

- The virtual IP address of Redundant Line Control function is set so that it is fixed as a local IP address using the bind function or others.

Thus, the Internet basic commands of Solaris such as ftp, telnet, and rlogin cannot be used in this mode.

After modification

The requirement for user applications that can be operated in this mode is as follows:

- Application using TCP/IP

F.6.3.5 Standby patrol

[Contents]

Specification of the MAC address which is used for the standby patrol can be omitted.

[Changes]**Before modification**

You need to specify the MAC address when setting the standby patrol.

After modification

If you do not specify the MAC address when setting the standby patrol, the MAC address is automatically set.

F.6.3.6 RIP mode

[Contents]

RIP mode is removed.

[Changes]**Before modification**

You can use RIP mode and Fast switching/RIP mode.

After modification

You cannot use RIP mode and Fast switching/RIP mode.

F.6.3.7 Self-checking function

[Contents]

This function periodically monitors the state of the control daemon and virtual driver by the self-checking function.

[Changes]

Before modification

The state of the control daemon and virtual driver are not monitored.

After modification

The state of the control daemon and virtual driver are monitored. If an error occurred in operation, the error can be notified to the user. Moreover, if the control daemon is stopped, it is automatically restarted.

F.6.3.8 Change of the error output message (205)

[Contents]

The error output message (205) is changed.

[Changes]

Before modification

```
20501: operation error: mode can't be changed for dual stack inteface.
```

After modification

```
20501: operation error: mode can't be changed for dual stack interface.
```

F.7 Changes from Redundant Line Control function 4.3A10 to version 4.3A20

The following table shows a list of changes.

Table F.6 List of changes from Redundant Line Control function 4.3A10 to 4.3A20

| Category | Item | Version |
|-----------------------|----------------------|----------------------------------|
| New command | None | - |
| Incompatible command | None | - |
| Incompatible function | Collecting materials | PRIMECLUSTER GLS 4.3A20 or later |

F.7.1 New command

There is no new command for Redundant Line Control function 4.3A20.

F.7.2 Incompatible command

No commands in the Redundant Line Control function 4.3A20 are incompatible from the previous versions.

F.7.3 Other incompatibilities

F.7.3.1 Collecting materials

[Contents]

"Virtual NIC mode information: rvnetinfo/" is added to the type of the examination materials collected by the material collection command.

[Changes]

Before modification

There is no "Virtual NIC mode information: rvnetinfo/" for the type of the examination material collected by the material collection command.

After modification

"Virtual NIC mode information: rvnetinfo/" is included for the type of the examination material.

F.8 Changes from Redundant Line Control function 4.3A20 to version 4.3A40

The following table shows a list of changes.

Table F.7 List of changes from Redundant Line Control function 4.3A20 to 4.3A40

| Category | Item | Version |
|-----------------------|----------------------------|----------------------------------|
| New command | None | - |
| Incompatible command | None | - |
| Incompatible function | Kernel Zones are supported | PRIMECLUSTER GLS 4.3A40 or later |

F.8.1 New command

There is no new command for Redundant Line Control function 4.3A40.

F.8.2 Incompatible command

No commands in the Redundant Line Control function 4.3A40 are incompatible from the previous versions.

F.8.3 Other incompatibilities

F.8.3.1 Kernel Zones

[Contents]

Kernel Zones are supported. For the support set for Redundant Line Control function, see "[C.3 Support Set for Each Redundant Line Switching Mode.](#)"

[Changes]

Before modification

Kernel Zones are unsupported.

After modification

Kernel Zones are supported.

F.9 Changes from Redundant Line Control function 4.3A40 to version 4.5A00

The following table shows a list of changes.

Table F.8 List of changes from Redundant Line Control function 4.3A40 to 4.5A00

| Category | Item | Version |
|--------------|------|---------|
| New commands | None | - |

| Category | Item | Version |
|------------------------|--|---------------------------------|
| Incompatible commands | hanetparam command | PRIMECLUSTER GL 4.5A00 or later |
| | hanetpoll command | PRIMECLUSTER GL 4.5A00 or later |
| Incompatible functions | Change the installation directory | PRIMECLUSTER GL 4.5A00 or later |
| | Initial settings for link status monitoring | PRIMECLUSTER GL 4.5A00 or later |
| | Initial setting values for the standby interface inactivation method | PRIMECLUSTER GL 4.5A00 or later |
| | Detecting hang-up of the ping command | PRIMECLUSTER GL 4.5A00 or later |
| | Output messages to the console | PRIMECLUSTER GL 4.5A00 or later |
| | Fujitsu hot standby protocol | PRIMECLUSTER GL 4.5A00 or later |
| | Changing the startup timing of the HUB monitoring function | PRIMECLUSTER GL 4.5A00 or later |
| | Self-check function | PRIMECLUSTER GL 4.5A00 or later |

F.9.1 New commands

There are no new commands for Redundant Line Control function 4.5A00.

F.9.2 Incompatible commands

In Redundant Line Control function 4.5A00, the following commands are incompatible commands from the previous versions.

In addition, please refer to "[Chapter 7 Command reference](#)" about the details of each command.

F.9.2.1 hanetparam command

[Contents]

The initial setting of the '-d' option (the inactivation method of the standby interface) of the hanetparam command is changed to "plumb."

[Changes]

Before modification

The '-d' option for the hanetparam command is initially set to "unplumb."

After modification

The '-d' option of the hanetparam command is initially set to "plumb."

F.9.2.2 hanetpoll command

[Contents]

The initial setting of the '-I' option (the link based failure detection settings) of the hanetpoll on command is changed to "yes."

[Changes]

Before modification

The '-I' option of the hanetpoll on command is initially set to "no."

After modification

The '-I' option of the hanetpoll on command is initially set to "yes."

F.9.3 Other incompatible items

F.9.3.1 Changing the installation directory

[Contents]

The installation directory of the package was changed from "/opt" to "/etc/opt."

[Changes]

Before modification

The installation directory of the package is "/opt."

After modification

The installation directory of the package is "/etc/opt."

Also, the actual command path maintains the compatibility by creating symbolic link to the previous modification of installation directory.

F.9.3.2 Initial settings for link status monitoring

[Contents]

If the HUB monitoring function is set, the link status monitoring function is enabled.

[Changes]

Before modification

The link status monitoring function is in inactive status and NIC link down is not detected.

After modification

The link status monitoring function is in active status and NIC link down is detected.

F.9.3.3 Initial setting values for the standby interface inactivation method

[Contents]

The initial setting of the standby interface inactivation method is "plumb."

[Changes]

Before modification

Initial is set to "unplumb" and the standby NIC is in "unplumb" status.

After modification

Initial is set to "plumb" and the standby NIC is in "down" status.

F.9.3.4 Detecting hang-up of the ping command

[Contents]

In the following monitoring functions, a hang-up of the ping command can be detected.

- HUB monitoring function in NIC switching mode
- Remote host monitoring function in GS/SURE linkage mode

[Changes]

Before modification

When the ping command hangs, an error in the route cannot be detected.

After modification

When the ping command hangs, an error in the route is detected. The operation after the route error is detected is the same as the operation after an error is detected in each communication mode.

In the user command execution function of the NIC switching mode, to be able to determine the type of error detected by the HUB monitoring function, added param2 to the argument when executing user commands.

For user command execution function of NIC switching mode, refer to "(2) When detected an error in a transfer route" in "3.6.10.1 Settings for NIC switching mode" for details.

F.9.3.5 Output messages to the console

[Contents]

Changes were made so that the following messages will not be output on the console. However, you can change the settings so that these messages are output to the console as in the settings of previous versions.

- Messages output when the virtual interface of the NIC switching mode is activating or deactivating.
- Messages output when the takeover virtual interface for all redundant modes is activating or deactivating.

[Changes]

Before modification

Messages are output both in the system log and the console.

After modification

Messages are only output in the system log.

If you want messages to be output also in the console as it was previously, add "disable_console" parameter to the following settings file and set its value to "0."

/etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
# Each entry is of the form:
#
# <param> <value or string>
#
observ_msg                0          # suppress observe message
transition_mode           0          # resource status transition mode
logicalif_takeover_type   1          # takeover Zone and RAC interface
disable_console           0 <- Add parameter and set to "0"
```

F.9.3.6 Fujitsu hot standby protocol

[Contents]

Changed the procedures for if message transmission failed when using Fujitsu hot standby protocol in GS/SURE linkage mode.

[Changes]

Before modification

The following error message is output.

```
ERROR: 80590: internal error.(*) [sock.c(***)]
```

After modification

The following error message is output.

```
WARNING: 93200: cannot send fhsp message. (dest=hostip, code)
```

See "[A.1.3 Console output messages \(numbers 800 to 900\)](#)" for details on the messages.

F.9.3.7 Changing the startup timing of the HUB monitoring function

[Contents]

The startup timing of the HUB monitoring function during system startup was changed to enable faster detection of transfer route failures.

[Changes]

Before modification

Could not detect a transfer route failure after the zones service (svc:/system/zones) was started.

The settings file (service.sh) for Redundant Line Control function service of the user command execution function will be executed after the zones service has been started.

After modification

Changed so that transfer route failures can be detected before the remote disk service (NFS client, iSCSI initiator) has been started.

The timing for the execution of the settings file (service.sh) for the transmission path redundancy function of the user command execution function is done earlier.

If using a settings file, see "[C.6.1.7 Example of configuration with GS/SURE linkage mode](#)" and modify the script.

F.9.3.8 Self-check function

[Contents]

The driver hang up detection time for the self-check function is set to 60 seconds.

Tuning a driver hang up detection time has become possible. See "[G.3.3.4 A virtual driver hang up was detected by the Self-Check function](#)" for details.

[Changes]

Before modification

- The driver hang up detection time for the self-check function is fixed at 15 seconds.
- Tuning of the driver hang up detection time is not possible.

After modification

- The initial value for the driver hang up time for the self-check function is 60 seconds..
- Tuning of the driver hang up detection time is possible.

F.10 Changes from Redundant Line Control function 4.5A00 to version 4.5A10

There is no change.

Appendix G Notice of supplemental information

This appendix provides supplemental information regarding GLS.

G.1 Changing Methods of Activating and Inactivating Interface

This section describes how to activate or deactivate network interfaces controlled through redundant line control.

G.1.1 Using NIC switching mode in shared-IP zone

If you use the virtual interface in NIC switching mode from the shared-IP zone, it is necessary to change the method of deactivating standby physical interfaces to "plumb" by executing the following command (however for 4.5A00 or later, default setting is "plumb"):

```
# /opt/FJShanet/usr/sbin/hanetparam -d plumb
```



The setting value is enabled when

- the system is rebooted,
- the virtual interfaces are deactivated or activated
- NIC is switched



The changed value will be enabled in all the virtual interfaces in NIC switching.

G.2 Frequently asked questions and answers

In this chapter frequently asked questions and answers for when using the Redundant Line Control function will be given.

G.2.1 I want to change the netmask settings or the IP address in the host file without changing the GLS definitions for the cluster system.

Follow the procedure below to do the changes.

1. Stop RMS

Execute the following command on any node.

```
# hvshut -a
```

2. To make sure that the GLS service does not start, start the OS in single user mode.
3. Change the netmask by correcting `/etc/inet/netmask` or by using the `ipadm(1m)` command, and change the IP address in the `/etc/inet/hosts` file.
4. Restart the OS in multi-user mode.
5. Check that GLS is operating normally.
Check that a GLS error message has not been output in the system log.
6. Check that the netmask and IP address changed in step 3. has been changed correctly.

G.3 Troubleshooting

The cause of the frequently occurred trouble when using a Redundant Line Control function and how to deal with it are explained in this section.

G.3.1 Communication as expected cannot be performed (Common to IPv4 and IPv6)

G.3.1.1 A default gateway is not set valid

Phenomenon:

A default gateway defined using the route command or /etc/defaultrouter file at activation of a system is not valid.

Cause and how to deal with:

The setting of a default gateway defined by the route command or /etc/defaultrouter is set in svc:/network/routing-setup service at activation of a system. At this time, when an interface of the same segment as that of the specified router, or when not activated, it is not possible to set a default gateway. In a Redundant Line Control function, a virtual interface is activated at activation of a userApplication in cluster operation. Therefore, occasionally not possible to set a default gateway.

Fast switching mode:

When using a virtual interface as a sending interface to a default gateway in cluster operation, change the timing to activate a virtual interface by a hanetparam command.

NIC switching mode:

When using a physical IP address takeover function, and also when not activating an interface in a standby node, it is not possible to use a physical interface as a sending interface to a default gateway.

GS/SURE linkage mode:

It is not possible to use a virtual interface as a sending interface to a default gateway in cluster operation.

G.3.1.2 Fails to activate a system or an interface in the NIS environment

Phenomenon:

The following message is displayed and activation of a system or an interface hangs up.

```
ypbind[xxxx]: [ID xxxxxx daemon.error] NIS server not responding for domain
"domain_name"; still trying
```

Cause and how to deal with:

When a system that a Redundant Line Control function works is set as an NIS client, occasionally not possible to connect NIS server temporarily due to the process to deactivate an interface executed by a Redundant Line Control function. In such a case, if set a netmask to an interface by an ifconfig command, occasionally the process to activate a system or an interface hangs up because an ifconfig command waits for the connection with NIS server to get a subnet mask.

Be sure to set as follows when using a Redundant Line Control function in the NIS environment.

To specify "files" first in /etc/nsswitch.conf to refer "netmasks".

[Example of setting]

```
netmasks: files
```

or

```
netmasks: files [NOTFOUND=return] nis
```


As to accessing NIS server, design a network not to use an interface that is the target of control in a Redundant Line Control function (activation/deactivation) as possible.

G.3.1.3 Automatic address configuration lags behind for IPv6

Phenomenon:

Automatic stateless address configuration for IPv6 may not operate instantly when activating IPv6. As a consequence, it takes time to add site-local/global addresses.

Cause and how to deal with:

When activating an interface for IPv6, a link-local address is added to the physical interface to activate the physical interface. To instantly create site-local/global address by the automatic stateless address configuration, it transmits the "router solicitation message" to the adjacent router to request for router advertisement message from the router. However, once the interface activates, if spanning tree protocol (STP) is running on the HUB, it takes time to hold a communication. Thus it may fail to request router advertisement messages. Because IPv6 router transmits the router advertisement message periodically and automatic stateless address automatic configuration runs after certain amount of time, it is possible to hold a communication of site-local/global addresses. Nevertheless, if the time interval parameter of transmitting the router advertisement message is set for a considerably long time, it may consume a long time until the automatic stateless address configuration starts and to hold a communication. In such case, either establish a link for operation NIC and standby NIC or modify the router setting so that a router transmits the router advertisement message within a few minutes interval.

G.3.1.4 Fails to communicate with GS in hot standby configuration

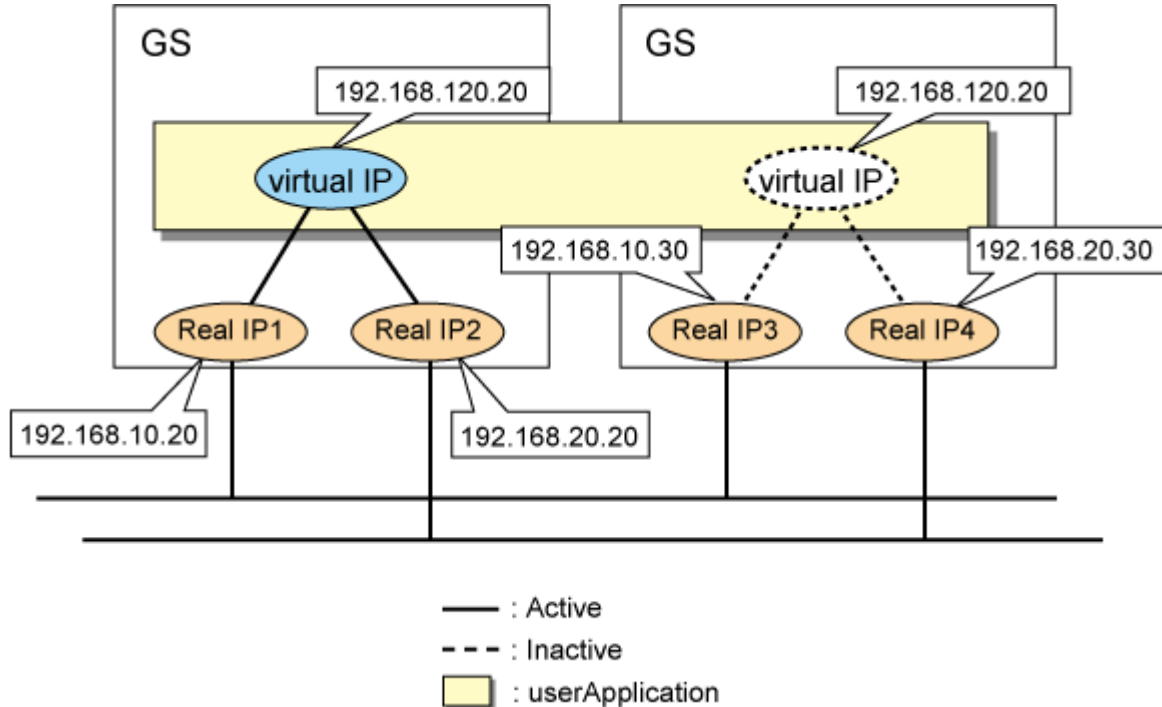
Phenomenon:

Communication with GS in hot standby configuration fails.

Cause and how to deal with:

The cause is that the setting for hanetobserv command has an error.

If GS's IP address moves between nodes as follows, execute the "hanetobserv create" command for each GS node.

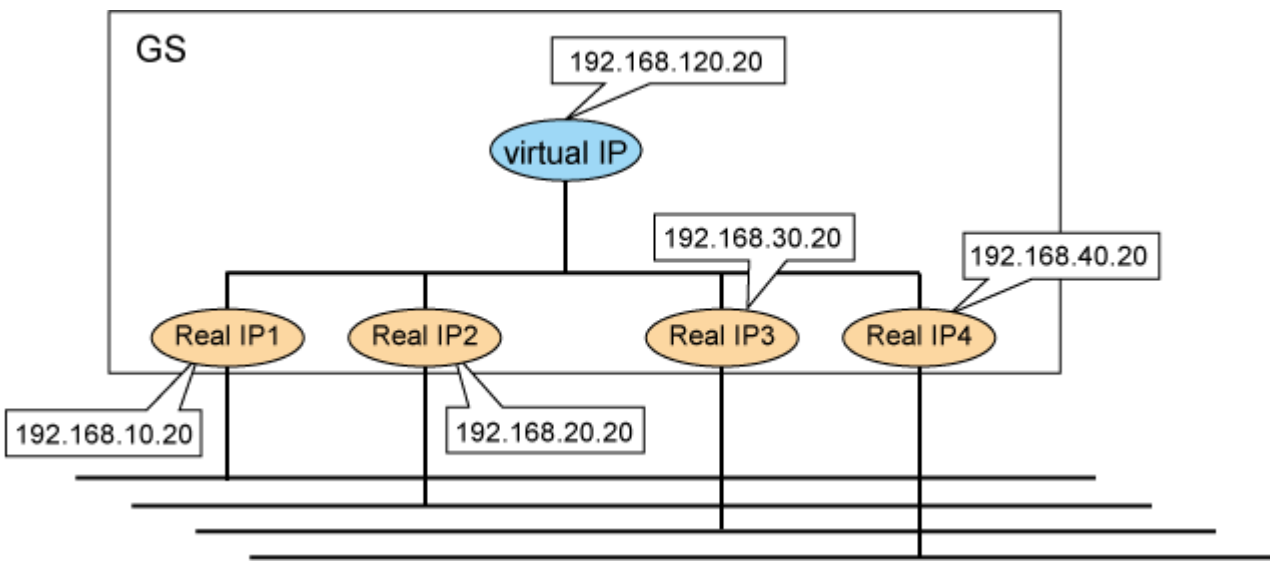


```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.20,192.168.20.20 -m on -r on
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.30,192.168.20.30
# /opt/FJSVhanet/usr/sbin/hanetobserv print
Destination Host Virtual Address POLL RIP NIC Address(:PMgroupID)
```

| Destination | Host | Virtual Address | POLL | RIP | NIC Address(:PMgroupID) |
|-------------|----------------|-----------------|------|-----|--|
| GS | 192.168.120.20 | | ON | ON | 192.168.10.20,192.168.20.20 192.168.10.30,192.168.20.30 |

If you create the settings as follows, one node is set as the communication target. If you want to perform this in a cluster configuration, execute the command for each node one by one. Note that the difference between the settings mentioned above and the settings here is whether the IP addresses in the "NIC Address" field that are displayed by the "hanetobserv print" command are separated by commas. Commas indicate that a communication target is a single node with four IP addresses. (192.168.10.20,192.168.20.20,192.168.30.20,192.168.40.20)

```
# /opt/FJShanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.20,192.168.20.20,192.168.30.20,192.168.40.20 -m on -r on
# /opt/FJShanet/usr/sbin/hanetobserv print
Destination Host Virtual Address POLL RIP NIC Address(:PMgroupID)
-----+-----+-----+-----+-----+-----+
GS          192.168.120.20  ON   ON   192.168.10.20,192.168.20.20,
          192.168.30.20,192.168.40.20
```



G.3.2 Virtual interface or the various functions of Redundant Line Control function cannot be used

G.3.2.1 An interface of NIC switching mode is not activated

Phenomenon:

The following message is output and activation of an interface fails.

```
hanet: ERROR: 85700: polling information is not defined. Devname = sha0(0)
```

Cause and how to deal with:

In NIC switching mode, switching interfaces inside a node and between nodes is controlled using a failure monitoring function. Therefore, NIC switching mode does not work only by defining the information of a virtual interface using a hanetconfig create command. Necessary to set the monitor-to information by a hanetpoll create command. When the monitor-to information is not set, a take over IP address is not activated either. Activation of a userApplication fails in cluster operation.

When using a logical address takeover function, and also when sharing a physical interface, necessary to have the monitor-to information in a unit of information of each virtual interface. In such a case, duplicate the information of a virtual interface and the monitor-to information that defined initially using a hanetconfig copy command and a hanetpoll copy command.

G.3.2.2 It does not failback at the time of the restoration detection by standby patrol in NIC switching mode

Phenomenon:

The following messages display during recovering process of standby patrol in NIC switching mode. As a result, it fails to instantly switch back from the secondary interface to the primary interface.

```
hanet: INFO: 88500: standby interface recovered. (sha1)
hanet: INFO: 89700: immediate exchange to primary interface is canceled. (sha1)
```

Cause and how to deal with:

After switching from the primary interface to the secondary interface due to transfer path failure, if a standby patrol recovers prior to elapsed link up delay time (default is 60 sec), the switching process between the primary and secondary interface may loop infinitely. To prevent from this symptom, the above messages will display to stop the switching process for the primary interface. The main reason of covering this issue in this section is to prevent infinite loop of switching interfaces when setting routes for monitoring and instead of HUBs.

G.3.2.3 Error detection message displays for standby patrol in NIC switching mode

Phenomenon:

The following message is output and activation of an interface fails.

```
hanet: WARNING: 87500: standby interface failed.
```

Cause and how to deal with:

On the network where VLAN switch exists on the transfer path monitored via standby patrol function, this error occurs if the following two circumstances take place:

- 1) Connecting a redundant NIC to a port of disparate VLAN identifier.
- 2) Connecting one of a redundant NIC or both redundant NICs to tagged member port of the switch.

The VLAN switch cannot communicate in between the ports where VLAN identifiers are disparate. Therefore, when connecting redundant NIC to disparate VLAN identifier, transmitting the monitoring frame fails between standby NIC and operation NIC, consequentially outputting 875 message. Additionally, even if VLAN identifiers are the same port and this port is set to tag member, and in the condition where the NIC does not support tagged VLAN (IEEE802.1Q compliance), it still fails to retrieve tag frame from the switch. Once again, transmitting the monitoring frame fails outputting 875 message. To rectify this problem, double check the VLAN configuration of the switch and make sure VLAN identifier is identical on the port connecting redundant NIC. If the NIC you are using does not support tagged VLAN, set the port of the switch as non-tag member.

G.3.2.4 Solaris Zones cannot be started

Symptom

If the virtual interface in fast switching or physical interface in NIC switching is specified for the network setting of the shared-IP zone, the following error message will be output and zone startup will fail:

```
# zoneadm -z zone0 boot
could not verify net address=192.168.80.10 physical=sha0: No such device or
address
zoneadm: zone zone0 failed to verify

or

# zoneadm -z zone0 boot
zoneadm: zone 'zone0': hme0:1: could not bring interface up: address in use by
zone 'global': Cannot assign requested address
zoneadm: zone 'zone0': call to zoneadmd failed
```

Cause and workaround

If the specified interface does not exist in the zone network setting or the IP address same as that specified for the zone network setting, the zone cannot be started. Check if the specified interface or IP address already exists using the "ifconfig(1M)" command. If you are using NIC switching, check if the method of deactivating the standby interface can be used in the zone. For details, see "7.6 hanetparam Command" and "G.1 Changing Methods of Activating and Inactivating Interface".

Information

If a zone is installed, and interfaces for the zone do not exist, zone installation will fail. You need to activate the interfaces specified for the zone network settings before zone installation.

G.3.2.5 Services of Redundant Line Control function cannot be started (when NIC failed)

Phenomenon:

When rebooting the system in the case of NIC or system board failure, the following message is output and services for Redundant Line Control function may not started.

```
Failed to plumb IPv4 interface(s): hme0
svc.startd[7]: svc:/network/physical:default: Method "/lib/svc/method/net-physical" failed with exit status 96.
svc.startd[7]: network/physical:default misconfigured: transitioned to maintenance
(see 'svcs -xv' for details)
```

Cause and how to deal with:

If rebooting the system while a failure occurs when multiple system boards exist or when NICs with multiple ports are used as shown in the following configuration, starting the network service (svc:/network/physical) fails because IP addresses cannot be assigned. In this case, network services including Redundant Line Control function (svc:/network/fjsvhanet) will not start.

Figure G.1 Configuration of NIC switching mode before change (For Solaris 10)

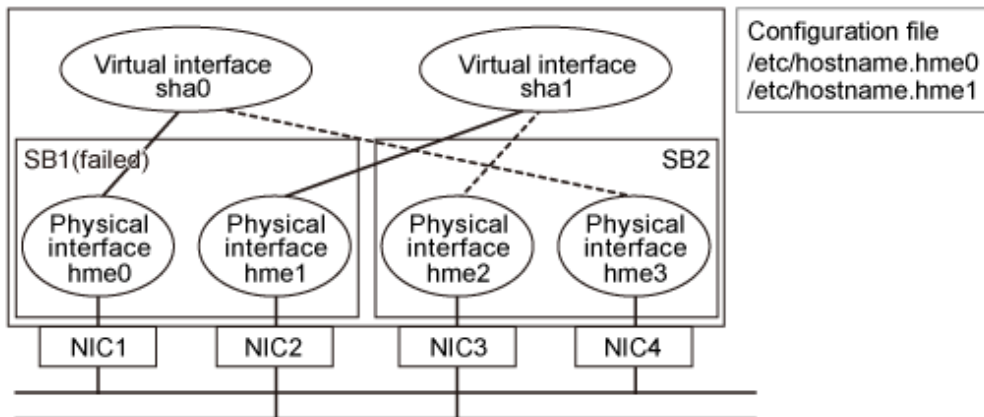
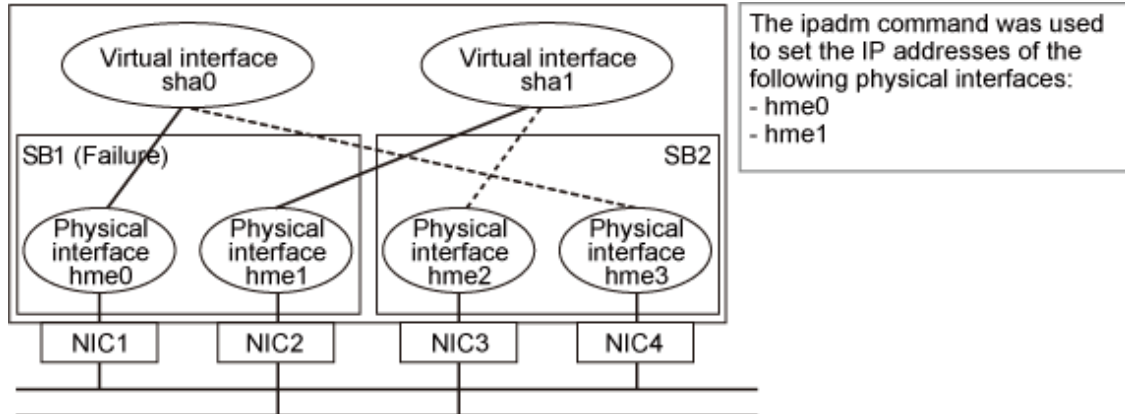


Figure G.2 Configuration of NIC switching mode before change (For Solaris 11 or later)



When rebooting the system with a failure of NIC or system boards, change the configuration of the IP address set to the physical interface with a failure so that the IP address will be set to a physical interface without any failure before rebooting the system, or restore the service using the `svcadm(1M)` command.

Recovery procedure

1. Assign the IP address set to the physical interface with a failure to a physical interface without any failure.

1-1) For Solaris 10

```
# mv /etc/hostname.hme0 /etc/hostname.hme3
# mv /etc/hostname.hme1 /etc/hostname.hme2
```

1-1) For Solaris 11 or later

```
# /usr/sbin/ipadm delete-ip hme0
# /usr/sbin/ipadm create-ip hme3
# /usr/sbin/ipadm create-addr -T static -a host11/24 hme3/v4
# /usr/sbin/ipadm delete-ip hme1
# /usr/sbin/ipadm create-ip hme2
# /usr/sbin/ipadm create-addr -T static -a host12/24 hme2/v4
```

2. Reboot the system or restore the network service.

```
# /usr/sbin/shutdown -y -i6 -g0
```

Or,

```
# svcadm clear svc:/network/physical:default
```



See

For details on the `svcadm(1M)` command and `ipadm(1M)` command, refer to the Solaris manual.

Change process to recommended environment

If the IP address set to a physical interface is assigned only for one system board in the case of [Figure G.1 Configuration of NIC switching mode before change \(For Solaris 10\)](#), it is recommended to change the environment for the Primary interface for each system board as shown in [Figure G.3 Configuration of NIC switching mode after change \(For Solaris 10\)](#).

Figure G.3 Configuration of NIC switching mode after change (For Solaris 10)

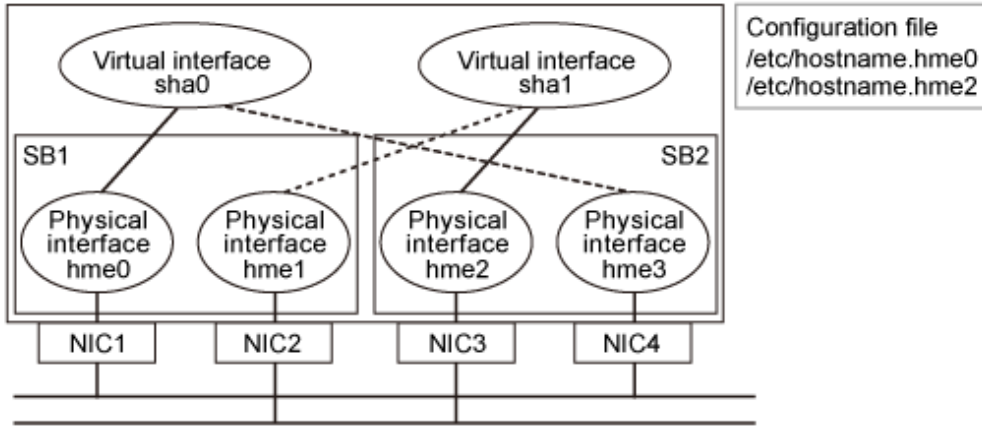
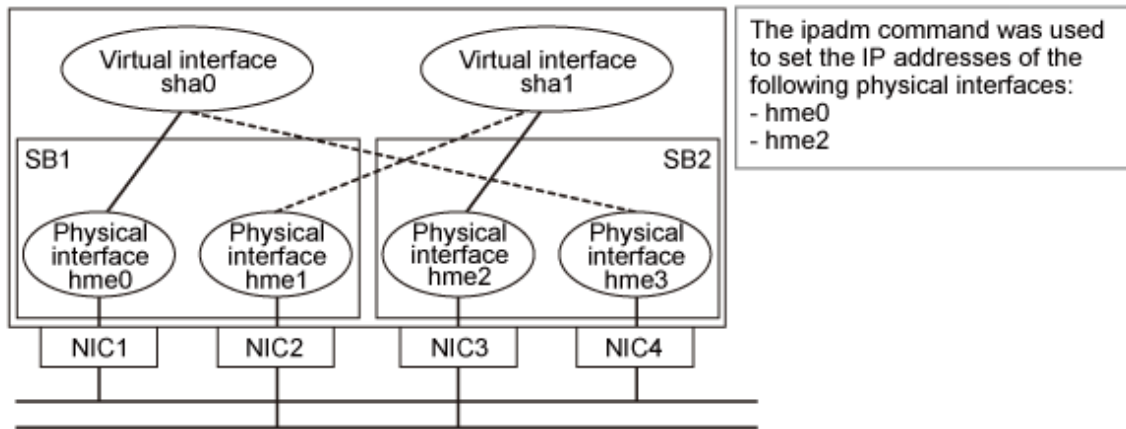


Figure G.4 Configuration of NIC switching mode after change (For Solaris 11 or later)



Procedure for setting up is as follows:

1. Stop the HUB monitoring function.

```
# /opt/FJShanet/usr/sbin/hanetpoll off
```

2. Deactivate all virtual interfaces.

```
# /opt/FJShanet/usr/sbin/stphanet
```

3. Change the configuration information.

Switch the redundant physical interfaces (Primary:hme1 and Secondary:hme2) in sha1 by executing the hanetconfig modify command.

```
# /opt/FJShanet/usr/sbin/hanetconfig modify -n sha1 -t hme2,hme1
```

4. Change the configuration so that IP addresses set to physical interfaces will be distributed for each system board. If the recovery procedure has been performed and the configuration is changed so that IP addresses set to physical interfaces will be distributed for each system board, this step is not required.

1-1) For Solaris 10

Rename the /etc/hostname.*** file.

In accordance with switch of redundant physical interfaces, rename the file from /etc/hostname.hme1 to /etc/hostname.hme2.

```
# mv /etc/hostname.hme1 /etc/hostname.hme2
```

1-1) For Solaris 11 or later

```
# /usr/sbin/ipadm delete-ip hme1
# /usr/sbin/ipadm create-ip hme2
# /usr/sbin/ipadm create-addr -T static -a host12/24 hme2/v4
```

5. Reboot the system.

```
# /usr/sbin/shutdown -y -g0 -i6
```

G.3.2.6 Services of Redundant Line Control function cannot be started (when inconsistency of file system occurred)

Phenomenon:

When /opt cannot be mounted at system startup in the Solaris 10 OS, the following message will be output and the services for Redundant Line Control function may not start.

```
hanet: ERROR: 98400: file system is inconsistent. (details)
```

Cause and how to deal with:

Since the inconsistency of the /opt file system was detected at the startup of GLS service, the startup stopped. Make sure that the inconsistency of the /opt file system is resolved and /opt is mounted. After that, perform one of the actions:

- Starting the system again
- Starting GLS service

```
# svcadm clear fjsvhanet
```

If the operation is not started normally after starting GLS service, the TCP/IP application that uses Redundant Line Control function may have failed to start. Start the system again.

G.3.2.7 Fails to activate a virtual interface in NIC switching mode for IPv6

Phenomenon:

The phenomenon is described using the following definition as an example.

```
Example)
# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol]

Name           Hostname           Mode MAC Adder/Phys ip Interface List
+-----+-----+-----+-----+-----+
[IPv6]

Name           Hostname/prefix           Mode Interface List
+-----+-----+-----+-----+
sha0           fc00:199::1/64           d   net3,net4
```

[Phenomenon 1]

A virtual interface fails to be activated in NIC switching mode for IPv6.

The strhanet command fails, an error message (*1) is output, and the virtual interface is not activated (*2).

In addition, a link-local address is not set for the primary interface in use (*3).

```

# /opt/FJSVhanet/usr/sbin/strhanet
hanet: 22310: operation error: failed to activate interface. name=sha0 (*1)
#
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
[IPv6]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
sha0      Inactive  d   OFF  net3(OFF),net4(OFF) (*2)
#
# /usr/sbin/ifconfig net3 inet6
net3: flags=120002000860<NOTRAILERS,RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu 1500
index 7
      inet6 ::/0 (*3)

```

[Phenomenon 2]

When NICs are switched by using the hanetnic change command, a switching target interface fails to be activated.

The hanetnic change command is successfully completed (*4), but net 4, which is a switching target interface, is not set to ON (*5). In addition, a link-local address is not set for the secondary interface in use (*6).

```

# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
[IPv6]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
sha0      Active   d   OFF  net3(ON),net4(OFF)
#
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0
hanet: 00000: information: normal end. (*4)
#
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
[IPv6]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
sha0      Active   d   OFF  net3(OFF),net4(OFF) (*5)
#
# /usr/sbin/ifconfig net4 inet6
net4: flags=120002000860<NOTRAILERS,RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu 1500
index 8
      inet6 ::/0 (*6)

```

Moreover, when NICs are switched at the time of error detection by the HUB monitoring function, the switching target interface similarly fails to be activated.

Note that Phenomenon 1 and Phenomenon 2 occur when hanetparam -d is set to Plumb.

```

# /opt/FJSVhanet/usr/sbin/hanetparam print
.....

```



```
NIC switching mode(d)          :Plumb
.....
```

Cause and how to deal with:

The cause of Phenomenon 1 and Phenomenon 2 is that an interface is not correctly set by using the ipadm command when defining the virtual interface.

Set the interface correctly by using the ipadm command.

- Setting the primary interface

Set the following.

```
# /usr/sbin/ipadm create-ip net3
# /usr/sbin/ipadm create-addr -T addrconf netX/v6 (*7)
```

When Plumb is set for hanetparam -d, it is necessary to set (*7).

If (*7) is not set, the virtual interface fails to be activated.

- Setting the secondary interface

The secondary interface does not need to be set like the primary interface.

[Phenomenon 1]

Only the ipadm create-ip command is executed in the primary interface setting.

Execute the ipadm create-addr command as shown below to make sure that the (*8) and (*9) link-local addresses are set.

After making sure of the settings, activate the virtual interface.

```
# /usr/sbin/ipadm
NAME          CLASS/TYPE STATE      UNDER  ADDR
.....
net3          ip          down      --      --
.....
# /usr/sbin/ipadm create-addr -T addrconf net3/v6
#
# /usr/sbin/ipadm
NAME          CLASS/TYPE STATE      UNDER  ADDR
.....
net3          ip          ok        --      --
  net3/v6     addrconf   ok        --      fe80::xxxx:xxxx:xxxx:xxxx/10(*8)
.....
#
# /usr/sbin/ifconfig net3 inet6
net3: flags=120002004860<NOTRAILERS,RUNNING,MULTICAST,DHCP,IPv6,PHYSRUNNING> mtu
1500 index 7
      inet6 fe80::xxxx:xxxx:xxxx:xxxx/10 (*9)
#
# /opt/FJSVhanet/usr/sbin/strhanet
hanet: 00000: information: normal end. name=sha0
#
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol]
Name          Status  Mode CL  Device
+-----+-----+-----+-----+
[IPv6]
Name          Status  Mode CL  Device
+-----+-----+-----+-----+
sha0          Active  d    OFF  net3(ON),net4(OFF)
#
# /usr/sbin/ifconfig -a6
```

```

.....
net3: flags=120002004861<UP,NOTRAILERS,RUNNING,MULTICAST,DHCP,IPv6,PHYSRUNNING> mtu
1500 index 7
    inet6 fe80::xxxx:xxxx:xxxx:xxxx/10
    ether xx:xx:xx:xx:xx:xx
net3:1: flags=120002000861<UP,NOTRAILERS,RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu
1500 index 7
    inet6 fc00:199::1/64
.....

```

[Phenomenon 2]

The ipadm create-ip command is mistakenly executed in the secondary interface setting.

Execute the ipadm delete-ip command as below to confirm that the setting was deleted (*10).

After making sure of the deletion, start the operation again.

```

# /usr/sbin/ipadm
NAME          CLASS/TYPE STATE      UNDER  ADDR
.....
net4          ip         down      --      --
.....
#
# /usr/sbin/ipadm delete-ip net4
#
# /usr/sbin/ipadm
NAME          CLASS/TYPE STATE      UNDER  ADDR
.....
net4 setting is not displayed.(*10)
.....
#
# /opt/FJSVhanet/usr/sbin/resethanet -s
hanet: 00000: information: normal end.
#
# /usr/sbin/ipadm
NAME          CLASS/TYPE STATE      UNDER  ADDR
.....
net4          ip         down      --      --
  net4/v6     addrconf  down      --      fe80::xxxx:xxxx:xxxx:xxxx/10
.....
#
# /usr/sbin/ifconfig -a6
.....
net3: flags=120002004861<UP,NOTRAILERS,RUNNING,MULTICAST,DHCP,IPv6,PHYSRUNNING>
mtu 1500 index 7
    inet6 fe80::xxxx:xxxx:xxxx:xxxx/10
    ether xx:xx:xx:xx:xx:xx
net3:1: flags=120002000861<UP,NOTRAILERS,RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu
1500 index 7
    inet6 fc00:199::1/64
net4: flags=100002000840<RUNNING,MULTICAST,IPv6,PHYSRUNNING> mtu 1500 index 8
    inet6 fe80::xxxx:xxxx:xxxx:xxxx/10
    ether xx:xx:xx:xx:xx:xx

```

G.3.3 Failure occurs during operation (Common to both Single and Cluster system)

G.3.3.1 Switching takes place in NIC switching mode regardless of failure at the monitoring end

Phenomenon:

Even though there is no error in network devices, the following message is output and HUB monitoring ends abnormally.

```
hanet: ERROR: 87000: polling status changed: primary polling failed.
(hme0,target=192.13.71.20)
hanet: ERROR: 87100: polling status changed: secondary polling failed.
(hme1,target=192.13.71.21)
```

Cause and how to deal with:

In NIC switching mode, it may take time before transmission becomes possible due to establishing a data link at Ethernet level following activation of an interface or the STP (Spanning Tree Protocol) transfer delay timer. Then, the status will not change to allow for immediate transmission even if the interface is activated. Generally, after the activation of the interface, the process establishing a data link will finish within several seconds, but in the instance of setting up the use of the STP, it may take 30 to 50 seconds until the status becomes to allow for transmission due to the STP transfer delay timer.

Therefore, if using the hanetpoll on command to shorten the link up completion waiting time (default value: 60 seconds), ping monitoring fails and switching occurs.

In such a case, extend the time to wait for linking up (default value: 60 seconds) by the hanetpoll on command according to the transfer delay time.

On the HUB where STP is running, possible next connection could take twice as the transfer delay time (normally 30 sec) after linked up. Standard link up latency of operating STP can be derived from the equation below.

For verifying STP transfer delay time, see the manual of HUB you are using.

```
link up latency > STP transfer delay time x 2 + monitoring period x number of
monitoring
```



To operate ping monitoring over the system that runs firewall, configure the firewall so that ping can pass through the firewall. Otherwise, it fails to operate ping monitoring.

The firewall settings must be the same for both of the primary and secondary interfaces.

G.3.3.2 Takes time to execute an operation command or to activate a userApplication

Phenomenon:

Takes time to execute an operation command of a Redundant Line Control function.

Takes time to activate a userApplication or to switch nodes at the cluster operation.

Cause and how to deal with:

When a host name or an IP address specified in the information of a virtual interface, the monitor-to information, etc. is not described in /etc/inet/hosts file, or when "files" are not specified at the top in an address solution of /etc/nsswitch.conf, occasionally it takes time to process an internally executed name-address conversion. Therefore, it takes time to execute a command, or for the cluster state to change. Check that all IP addresses and host names to use in a Redundant Line Control function are described in /etc/inet/hosts, and that /etc/inet/hosts is referred first at name-address conversion.

G.3.3.3 TCP connection is not divided in GS/SURE linkage mode

Phenomenon:

Even though TCP communication by a virtual IP is executed in GS/SURE linkage mode, the number of the connections is not shown when displayed how the connection is divided using a dsphanet command.

```
# /opt/FJSVhanet/usr/sbin/dsphanet -c
Name  IFname Connection
+-----+-----+-----+
sha0   sha2      -
        sha1      -
sha10  sha12     -
        sha11     -
```

Cause and how to deal with:

When dividing TCP connection in GS/SURE linkage mode, necessary to define the information of the other system with a hanetobserv command. Any protocol other than TCP is not divided. UDP and ICMP are sent according to the route information.

G.3.3.4 A virtual driver hang up was detected by the Self-Check function

Phenomenon:

A virtual driver hang up was detected by the Self-Check function.

Cause and how to deal with:

The Self-Check function starts the processes for the monitoring. If this process did not work for more than 60 seconds due to high system load, it might mistakenly detect a driver hang up.

After the hang up detection message has been output, if the status is displayed normally when using the dsphanet command, the driver is not hung up.

Mistaken hang up prevention can be prevented by extending the driver hang up detection time.

Follow the procedure below to extend the hang up detection time.

1. Edit the settings file and set the detection time.

/etc/opt/FJSVhanet/config/mond.conf

```
drv_resp 120 <- Add a parameter and set a value.
```

drv_resp: virtual driver hang up detection time (in seconds)

A value from 1 to 3600 can be specified.

When the additional line is not set, 60 is set by default.

The virtual driver hang up detection cannot be disabled.

2. Reboot the system.

```
# /usr/sbin/shutdown -y -g0 -i6
```

G.3.3.5 ping command to HUB monitoring destination hangs

Phenomenon:

The following error message is output to syslog and NICs are switched.

```
ERROR: 93100: hangup of ping command has been detected. (target=HUB monitoring destination IP address)
```

Cause and how to deal with:

This phenomenon occurs when the ping command that is executed by ping monitoring of the HUB monitoring function does not complete within 30 seconds.

It is considered to have been caused by the defective NIC or temporarily high-load OS.

If it is caused by the temporarily high-load OS, edit the following file and extend the hang up detection time of the ping command.

File: /etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
# Each entry is of the form:
#
# <param> <value or string>
#
observ_msg          0      # suppress observe message
transition_mode     0      # resource status transition mode
logicalif_takeover_type 1    # takeover Zone and RAC interface
ping_hang_detect_time 90    <- Add a parameter and set a value.
```

ping_hang_detect_time: ping command hang up detection time (in seconds)

A value from 5 to 300 can be specified.

Setting 0 disables the ping hang detection function.

When the additional line is not set, 30 is set by default.

G.3.4 Failure occurs during operation (In the case of a Cluster system)

G.3.4.1 Node switching is not executed in Fast switching mode

Phenomenon:

Failover between clusters (job switching between nodes) is not executed in Fast switching mode at cluster operation.

Cause and how to deal with:

In Fast switching mode, it is decided that an error occurred in a transfer route when a response from all other systems in communication was cut off. Therefore, node switching is not executed when all cables are pulled out or when the power of all HUBs is not turned on. When the following message is often displayed, check the cables or HUBs.

```
unix: NOTICE: SUNW,hme1: No response from Ethernet network : Link Down - cable problem?
```

G.3.5 Failure occurs when using IPv6 address (Common to both Single and Cluster system)

G.3.5.1 Automatic address configuration malfunctions while using standby interface in NIC switching mode

Phenomenon:

If IPv6 virtual interface for NIC switching mode is used on the system operating as an IPv6 router, automatic stateless address configuration in the corresponding network ceases to function after switching the interface in the node. As a result, it cannot hold a communication with site-local/global address.

Cause and how to deal with:

In order to use IPv6 virtual interface for NIC switching mode in the system operating as an IPv6 router, both operation and standby NIC must contain the same configuration information in `/etc/inet/ndpd.conf` configuration file.

The following is an example of `/etc/inet/ndpd.conf` under situation in which operation NIC is `hme1`, standby NIC is `hme2`, and distributed network prefix is `fec0:1::0/64`.

```
ifdefault AdvSendAdvertisements true # Every interface sends a router
advertisement.
prefix fec0:1::0/64 hme0 # hme0 sends Prefix "fec0:1::0/64".
prefix fec0:2::0/64 hme1 # hme1 sends Prefix "fec0:2::0/64".
```

G.3.6 Failure occurs while using IPv6 address (In the case of a Cluster system)

G.3.6.1 Fails to activate IPv6 takeover address

Phenomenon:

Outputs the following message and fails to activate IPv6 take over IP address.

```
ifconfig: Duplicate address detected on link hme1 for address fec0:1380::100.
Code 1
```

Cause and how to deal with:

If an IPv6 address is overlapping with the other systems, when attempting to activate an interface, the address overlap detection function causes to stop the activation of a take over IP address. Be sure to check the other systems for overlapping IP addresses.

G.3.7 Resuming connection lags after switching (Common to both Single and Cluster system)

G.3.7.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode

Phenomenon:

When switching interface from operation NIC to standby NIC in NIC switching mode where HUB in the network is running Spanning Tree Protocol (STP), it takes roughly 30 seconds to hold a communication with standby NIC.

Cause and how to deal with:

In the HUB where STP is running, establishing link by activating an interface does not necessary mean to acquire communication instantly. In such environment, after a link has established on the port where NIC is connected, transmitting data is temporary constrained by transmission delay timer (Forward-time). In order to establish a communication instantly after switching to standby NIC,

use the standby patrol. Standby patrol establishes a link regularly in both operation and standby NIC, so that the transmitting data would not be constrained by transmission delay timer (Forward-time) of STP.

G.3.8 Incorrect operation by the user

G.3.8.1 Accidentally deleted the virtual interface with ifconfig command

Phenomenon:

Unable recover the virtual interface of a Fast switching mode deleted with ifconfig command by accident.

Cause and how to deal with:

There would be no guarantee on system behavior, if a virtual interface (Fast switching mode) is disabled or deleted. In order to recover a virtual interface, follow the procedure below:

[Example 1]

Accidentally executing "ifconfig sha0 unplumb" against a virtual interface sha0 for Fast switching mode.

```
If IPv4 address is being used:
# ifconfig sha0 plumb IPv4 address up

IPv6 address is being used:
# ifconfig sha0 inet6 plumb
# ifconfig sha0:2 inet6 plumb IPv6 address (Execute only if a logical virtual
interface is configured)
# ifconfig sha0 inet6 up
# ifconfig sha0:2 inet6 up (Execute only if a logical virtual interface is
configured)
```

[Example 2]

Accidentally executing "ifconfig sha0 down" against a virtual interface sha0 for Fast switching mode.

```
If IPv4 address is being used:
# ifconfig sha0 up

IPv6 address is being used:
# ifconfig sha0 inet6 up
# ifconfig sha0:2 inet6 up (Execute only if a logical virtual interface is
configured)
```



See

.....
In the case of a cluster system, a virtual interface is restored automatically. In addition, please refer to "[2.3.4 Interface status monitoring feature](#)" automatically about the virtual interface which can be restored.
.....

G.3.9 System in Solaris Zones

G.3.9.1 Patch application fails

Symptom:

When a patch is applied with the "patchadd" command after the system is rebooted in single user mode, the following error message is output then patch application fails.

```
Preparing checklist for local zone check...

Checking local zones...
```

```
Booting local zone zone0 for patch check...
ERROR: unable to boot zone: problem running </usr/sbin/zoneadm> on zone
<zone0>: Error 0
could not verify net address=192.168.80.10 physical=sha0: No such device or
address
zoneadm: zone zone0 failed to verify

Can not boot local zone zone0
```

Corrective action:

If a Solaris Zone exists on the system, consistency with a non-global zone will be checked at the time of patch application. If the non-global zone is used in the high-reliability network through redundant line control, a consistency error will occur then patch application will fail. It is necessary to apply the patch using the following steps:

[Procedure]

1. Start the system in multi-user mode.
2. Check that the redundant line control function is activated.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
```

3. Change the mode from multi-user to single user mode using the "init" command.

```
# init s
```

4. Apply the patch.

```
# patchadd "<Patch-ID>"
```

G.3.10 SMF service using the GLS virtual IP

G.3.10.1 Startup of the service or connection to the server fails in SMF service using the GLS virtual IP address

Phenomenon:

In SMF service using the virtual IP address of Redundant Line Control function, startup of the service or connection to the server fails.

Cause and how to deal with:

The cause is that SMF service (routing or name service) requiring the virtual IP address is started up without waiting the service for Redundant Line Control function, which activates the virtual IP address.

If the service uses the virtual IP address, set as the service starts up after the virtual IP address is activated.

For details, see "[3.6.10.3 Settings of the service for Redundant Line Control function](#)".

Glossary

Active interface

An interface currently used for communication.

[Related article] Standby interface

Automatic fail-back function

A function to automatically fail back without any operator when the failed LAN recovered. See a standby patrol function (automatic fail-back if a failure occurs) or a standby patrol function (immediate automatic fail-back) for the detail.

Cluster failover function (failover function)

A function to fail over between clusters if all physical interfaces bundled by a virtual interface caused an error or if an active node panicked or hung when operating clusters.

DR

Dynamic Reconfiguration

Dynamic switching function

A function to switch to a standby interface while an active interface is active.

ESF

Enhanced Support Facility

Fast switching mode

Fast switching mode keeps the communication alive during transfer route failure and increases the total throughput by multiplexing transfer routes between servers on the same network.

Global zone

A global zone is the global view of the Solaris operating environment. There is always one global zone per Solaris instance. Each software partition that is created within the Solaris instance can be managed and controlled in the global zone.

[Related article] Solaris Zones, Non-global zone (Zone)

GS/SURE linkage mode

GS/SURE linkage mode multiplexes transfer routes between global server/SURE SYSTEM and ExINCA lies on the same network. This mode provides functionality of transfer route failover during transfer route failure in which implements high availability.

HUB monitoring function

A function to monitor from an active interface to a HUB connected to an active interface. It switches to a standby interface if detected an error.

[Related article] Inter-HUB monitoring function, Line monitoring

HUB-to-HUB monitoring function

A function to monitor an error in the connection between the HUBs (cascade connection). The monitoring range is from an active interface to a HUB connected to an active interface, and to the one connected to a standby interface. This function includes the monitoring range of a HUB monitoring function. However, it does not monitor a standby interface.

[Related article] HUB monitoring function

LAN

Local area network

LAN card

The same meaning as that of NIC.

Line monitoring

The same meaning as that of HUB monitoring function.

[Related article] Inter-HUB monitoring function

Logical interface

A logical interface created in a different name to the same one physical interface. For instance, a logical interface to a physical interface eth0 is eth0:X (X is 0, 1, 2...)

[Related article] Logical IP address

Logical IP address (logical IP)

An IP address assigned to a logical interface.

[Related article] Logical interface

Logical IP address takeover function

A function to take over a logical IP address from cluster to cluster. It is possible to take over a logical IP address if switching from an active node to a standby node occurred between clusters. A physical IP address is not taken over in this case.

Logical virtual interface

Logical virtual interface is a logical interface created as distinguished name for a virtual interface. For example, a logical virtual interface for the virtual interface sha0 is represented as sha0:X (X refers to 2,3..64).

Note that if X becomes larger than 65, they are then used as a takeover virtual interface on a cluster environment.

Monitoring frame

A Monitoring frame is a unique frame GLS handles to monitor the transfer paths. Fast switching mode uses this feature to monitor associate host. For NIC switching mode, it uses this feature as standby patrol function to monitor standby interfaces.

[Related article] Standby patrol function, HUB monitoring function, Inter-HUB monitoring function

NIC

Stands for Network Interface Card. Also called a LAN card.

NIC sharing function

A function to create more than one piece of configuration information by sharing the NIC if the adding physical IP address is the same in all NICs and configuration information. Use this function to assign more than one IP to a pair of the redundant NICs. Use this to execute cluster mutual standby operation as well.

NIC switching mode

A mode to realize high reliability by exclusively using a redundant NIC and switching when an error occurred. It is necessary to connect a redundant NIC in the same network in this mode.

Non-global zone (Zone)

Each non-global zone has a security boundary around it. The security boundary is maintained by allowing zones to only communicate between themselves using networking APIs.

[Related article] Solaris Zones, Global zone

PHP

PCI Hot Plug

Physical interface

An interface created for the NIC equipped with in a system.

[Related article] [Physical interface](#)

Physical IP address (physical IP)

An IP address assigned to a physical interface.

[Related article] [Physical interface](#)

Physical IP address takeover function

Physical IP address takeover function is a function that takes over physical IP addresses between redundant NICs. On a cluster operation, it consists with two separate functions, they are Physical IP address takeover function I and IP address takeover function II.

Physical IP address takeover function I

This function takes over physical IP addresses between a cluster environment. Apply hanetconfig command with -e option before creating a virtual interface. It could takeover the physical IP address when switching occurs from operation node and standby node on cluster environment. Moreover, it activates physical interface on standby node of the cluster.

Physical IP address takeover function II

This function takes over physical IP addresses between a cluster environment. Apply hanetconfig command without -e option before creating a virtual interface. It could takeover the physical IP address when switching occurs from operation node and standby node on cluster environment. Moreover, it does not activate physical interface on standby node of the cluster.

Primary interface

An interface to use for communication initially in NIC switching mode.

[Related article] [Secondary interface](#)

Real interface

The same meaning as that of a physical interface.

Redundant Line Control function

A function to realize high reliability of communication by making a network line redundant.

RMS

Reliant Monitor Services.

RMS Wizard

A software package composed of various configuration and administration tools used to create and manage applications in an RMS configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

Secondary interface

An interface initially standing by in NIC switching mode. It switches from a standby interface to an active interface if an error occurred in a primary interface.

SIS

Stands for Scalable Internet Services.

Solaris Zones

Solaris Zones isolate software applications and services using flexible, software-defined boundaries. This software partitioning enables administrators to easily create many private execution environments in a single instance of the Solaris Operating System. It also enables dynamic control of applications and resource priorities. For details, see the "Solaris 10 manual".

Standby interface

An interface currently not used for communication, but to be used after switched.

[Related article] Active interface

Standby patrol function

A function to monitor the status of a standby interface in NIC switching mode. Monitoring a standby interface regularly detects a failure of NIC switching in advance. Standby patrol is to send a monitoring frame from a standby interface to an active interface and monitor its response. The monitoring range is from a standby interface to a HUB connected to a standby interface, a HUB connected to an active interface, and an active interface. This includes the monitoring range of an inter-HUB monitoring function. Therefore, it is not necessary to use an inter-HUB monitoring function when using a standby patrol function. The monitoring range of inter-HUB monitoring is from an active interface to a HUB connected to an active interface and the one connected to a standby interface, without including a standby interface.

[Related article] Standby patrol function (automatic fail-back if a failure occurs), Standby patrol function (immediate automatic fail-back)

Standby patrol function (automatic fail-back if a failure occurs)

A standby patrol function to automatically incorporate the failed interface as a standby interface when it recovered. This function automatically incorporates the failed primary interface as a standby interface when it recovered. This makes it possible to fail back to a primary interface if an error occurred in a secondary interface.

[Related article] Standby patrol function, Standby patrol function (immediate automatic fail-back)

Standby patrol function (immediate automatic fail-back)

A standby patrol function to fail back immediately after the failed interface recovered. When the failed primary interface recovered, this function immediately fails it back as an active interface. A secondary interface is incorporated as a standby interface in this case.

[Related article] Standby patrol function, Standby patrol function (automatic fail-back if a failure occurs)

Tagged VLAN (IEEE802.1Q)

Tagged VLAN attaches an identifier called a "tag" to communication packets of each network allow to build multiple virtual networks on the same physical line.

Tagged VLAN interface

Tagged VLAN interface is a logical interface generated from a NIC that supports Tagged VLAN functionality (IEEE802.1Q).

Takeover virtual interface

Takeover virtual interface is an interface of GLS, which takes over an interface between the cluster nodes. Takeover virtual interface is configured with a logical virtual interface containing logical number of 65 or later.

User command execution function

This refers execution of a command manually operated by the user.

[Related article] NIC switching mode, GS/SURE linkage mode

Virtual gateway

A virtual gateway used in GS/SURE linkage mode. By setting a virtual gateway, a virtual IP is automatically selected as a local IP address used for communication.

Virtual interface

An interface created for a Redundant Line Control Function to deal with a redundant NIC as one virtual NIC. The virtual interface name is described as shaX (X is 0, 1, 2...)

[Related article] Virtual IP address

Virtual IP address (virtual IP)

An IP address assigned to a virtual interface.

[Related article] [Virtual interface](#)

Virtual NIC mode

This mode enables the highly reliable communication by exclusively using a pair of the NICs which were grouped on the same network as a single virtual interface.

VLAN

Virtual LAN

Web-Based Admin View

This is a common base enabling use of the Graphic User Interface of PRIMECLUSTER. This interface is in Java. For details, see "PRIMECLUSTER Installation and Administration Guide".

XSCF

eXtended System Control Facility

Index

| | | | | | |
|--|-----|-----------------------|--|---|--------------------|
| | [A] | | | | [N] |
| Active interface..... | | 603 | | NIC..... | 604 |
| Automatic fail-back function..... | | 41,603 | | NIC sharing function..... | 604 |
| | [C] | | | NIC switching mode..... | 1,16,64,68,604 |
| Cloning environment..... | | 555 | | Non-global zone (Zone)..... | 604 |
| Cluster failover function (failover function)..... | | 603 | | | |
| | [D] | | | | [P] |
| DR..... | | 122,143,284,603 | | PHP..... | 132,143,604 |
| dsphanet Command..... | | 208 | | physical interface..... | 28,30,44 |
| dsppoll Command..... | | 232 | | Physical interface..... | 605 |
| Dynamic Reconfiguration..... | | 115 | | Physical IP address..... | 605 |
| Dynamic switching function..... | | 603 | | Physical IP address takeover function..... | 367,605 |
| | [E] | | | Physical IP address takeover function I..... | 389,605 |
| ESF..... | | 603 | | Physical IP address takeover function II..... | 393,605 |
| | [F] | | | Primary interface..... | 605 |
| Fast switching mode..... | | 1,12,64,67,603 | | | |
| Fault monitoring function..... | | 13,17,24 | | | [R] |
| | [G] | | | Real interface..... | 605 |
| Global zone..... | | 603 | | Redundant Line Control function..... | 57,120,186,247,605 |
| GS/SURE connection function..... | | 2,473,475,476,480,483 | | resethanet Command..... | 243 |
| GS/SURE linkage mode..... | | 2,21,64,70,603 | | RMS Wizard..... | 605 |
| | [H] | | | | |
| hanetbackup Command..... | | 239 | | | [S] |
| hanetconfig Command..... | | 194 | | Secondary interface..... | 605 |
| hanetgw Command..... | | 245 | | Self-checking function..... | 60 |
| hanethvrsc Command..... | | 241 | | Sharing physical interface..... | 91 |
| hanetnic Command..... | | 236 | | SIS..... | 605 |
| hanetobserv Command..... | | 212 | | Solaris Zones..... | 589,605 |
| hanetparam Command..... | | 220 | | Standby interface..... | 606 |
| hanetpoll Command..... | | 224 | | Standby patrol function..... | 40,102,606 |
| hanetrestore Command..... | | 240 | | Standby patrol function (automatic fail-back if a failure occurs) | 606 |
| HUB-to-HUB monitoring feature..... | | 32,33 | | Standby patrol function (immediate automatic failback)..... | 606 |
| HUB-to-HUB monitoring function..... | | 603 | | stphanet Command..... | 207 |
| HUB monitoring function..... | | 31,91 | | stpctl Command..... | 239 |
| HUB monitoring function..... | | 92,603 | | strhanet Command..... | 205 |
| | [I] | | | strctl Command..... | 238 |
| Interface status monitoring feature..... | | 56 | | Switching function..... | 14,19 |
| | [L] | | | | |
| LAN..... | | 603 | | | [T] |
| LAN card..... | | 604 | | Tagged VLAN..... | 606 |
| Line monitoring..... | | 604 | | Tagged VLAN interface..... | 56,57,116,178,606 |
| Logical interface..... | | 604 | | Takeover virtual interface..... | 183,184,606 |
| Logical IP address..... | | 604 | | TCP relay function..... | 3,478 |
| Logical IP address takeover function..... | | 604 | | | |
| Logical virtual interface..... | | 289,311,334,604 | | | [U] |
| logical virtual interfaces..... | | 30 | | User command execution function..... | 45,103 |
| | [M] | | | User command execution..... | 606 |
| Monitoring frame..... | | 604 | | | |
| | | | | | [V] |
| | | | | Virtual gateway..... | 606 |
| | | | | virtual interfaces..... | 26 |
| | | | | virtual interface..... | 36 |
| | | | | Virtual interface..... | 606 |
| | | | | Virtual IP address (virtual IP)..... | 607 |
| | | | | Virtual NIC mode..... | 2,607 |
| | | | | VLAN..... | 607 |

[W]
Web-Based Admin View.....607

[X]
XSCF.....607