


# **FUJITSU Software**

## **PRIMECLUSTER Global Link Services**

A horizontal band featuring a red abstract graphic with flowing, curved lines and bright light flares, creating a sense of motion and energy.

# **Configuration and Administration**

## **Guide 4.3**

### **Redundant Line Control Function**

Linux

J2UZ-7781-05ENZ0(03)  
September 2016

# Preface

---

## Purpose

This document describes the installation, configuration, operation, and maintenance of PRIMECLUSTER Global Link Services (hereafter 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.

### [Chapter 7 Command references](#)

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 redundant network control.

### [Appendix C Operation on the Virtual Machine Function \(For RHEL5\)](#)

This appendix explains how to operate GLS on the virtual machine function (for RHEL5).

### [Appendix D Operation on the Virtual Machine Function \(for RHEL6\)](#)

This appendix explains how to operate GLS on the virtual machine function (for RHEL6).

### [Appendix E Operation on VMware](#)

This appendix explains how to operate GLS on VMware.

### [Appendix F Trouble shooting](#)

This section explains the potential causes and solutions when trouble occurs while using a Redundant Line Control Function.

### [Appendix G Check list](#)

This appendix describes items to be checked before operating GLS. Using this checklist before operation can reduce the risk of incorrect settings.

## Appendix H Changes from previous versions

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

## Glossary

This section explains terms related to Redundant Line Control Function.

## Related Documentation

Refer to the following manuals as necessary.

- PRIMECLUSTER Concepts Guide
- PRIMECLUSTER Installation and Administration Guide
- PRIMEQUEST 1000 Series Administration Manual
- PRIMEQUEST 2000 Series Administration Manual
- PRIMEQUEST 1000 Series Tool Reference
- PRIMEQUEST 2000 Series Tool Reference
- OSIV VTAM-G TISP HANDBOOK (V10)

## Notational convention

The document conforms to the following notational conventions:



Point

Text that requires special attention



Note

Information that users should be cautious of



Example

Describes operation using an example



Information

Information that users can refer to



See

Manuals users find workable

## Abbreviations

In this document, the following product name is written by abbreviation.

Product names	Abbreviations	
Red Hat Enterprise Linux 5	RHEL5	RHEL

Product names	Abbreviations	
Red Hat Enterprise Linux 6	RHEL6	
PRIMEQUEST 1000 Series Virtual Machine Function	Virtual Machine Function	
Linux Virtual Machine Function		
RHEL5-Xen Virtual Machine Function		
PRIMEQUEST 2000/1000 Series	PRIMEQUEST	

## 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.

Linux is a registered trademark of Linus Torvalds.

Red Hat is a registered trademark of Red Hat, Inc. in the U.S. and other countries.

Ethernet is a trademark of Fuji Xerox Corporation.

PRIMECLUSTER is a registered trademark of Fujitsu Limited.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Other product names that appear in this manual are product names, trademarks, or registered trademarks of respective companies.

## Date of publication and edition

February 2014, Sixth edition April 2014, 6.1 edition November 2015, 6.2 edition September 2016, 6.3 edition
--

## Using for application requiring high-security:

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

- |   |
|---|
| <ul style="list-style-type: none"> <li>- No part of this document may be reproduced or copied without permission of FUJITSU LIMITED.</li> <li>- The contents of this document may be revised without prior notice.</li> </ul> |
|---|

All Rights Reserved, Copyright (C) FUJITSU LIMITED 2008-2016.

## Revision History

Revision	Location	Edition
Modified the name of PRIMEQUEST.	All	6.1

Revision	Location	Edition
Added description about SR-IOV.	2.10.2 Duplicated operation by Fast switching mode 2.10.4 Duplicated operation via Virtual NIC mode 2.10.5 Duplicated operation via GS linkage mode D.3.2 Support set for each redundant line switching mode E.3.2 Support set for each redundant line switching mode	
Modified the reference manuals.	6.4.2.1 Addition procedure 6.4.2.2 Removal procedure 6.4.2.3 Swapping procedure	
Added the note about LLDP on a physical interface.	2.10.4 Duplicated operation via Virtual NIC mode	6.2
Added the descriptions for setting neighboring switches to the monitoring destination information.	2.10.5 Duplicated operation via GS linkage mode 3.10.1.1 Setting the monitoring destination information B.8.5 Example of the Cluster system (1:1 Standby) B.8.6 Example of the Cluster system on remote network(1:1 Standby) B.8.7 Example of the Cluster system (Mutual Standby)	
Added the note when bundling the bonding interface.	3.3.3 Virtual NIC mode	
Added the descriptions for the monitoring method of the self-checking function.	3.11.2.2 Error detection of the self-checking function	
Added the note when registering two or more GIs resources to one cluster application.	5.1 Outline of Cluster System Support	
Changed descriptions for the create and delete commands.	7.15 hanetobserv Command	
Changed the descriptions for the message numbers 974 and 976.	A.1.3 Console output messages (numbers 800 to 900)	
Added the descriptions when neighboring switches are set to the monitoring destination information.	G.6.5 Maintenance procedure performed when the communication target stopped	
Added the note for GS hot-standby configuration.	2.1.4.5 Notes	6.3
Corrected the note for the length of the net mask for GS linkage mode.	2.10.5 Duplicated operation via GS linkage mode	
Added the note for GS hot-standby configuration.	2.10.5 Duplicated operation via GS linkage mode	
Added the note when the remote host is using hot-standby configuration.	3.10.1.1 Setting the monitoring destination information	
Changed "Action" of message numbers 169 and 170.	A.1.2 Error output message (numbers 100 to 700)	
Changed "Action" of message number 897.	A.1.3 Console output messages (numbers 800 to 900)	
Added the TNOTIFY command to the glossary.	Glossary	

# Contents

---

Chapter 1 Overview.....	1
1.1 What is redundant line control?.....	1
1.1.1 Functional comparison.....	3
1.1.2 Criteria for selecting redundant line control methods.....	5
1.2 Redundant line control effects.....	6
1.3 System Configuration.....	6
Chapter 2 Feature description.....	10
2.1 Overview of Functions.....	10
2.1.1 Fast switching mode.....	10
2.1.1.1 Fault monitoring function.....	11
2.1.1.2 Switching function.....	12
2.1.1.3 Connectable remote host.....	13
2.1.1.4 Available application.....	13
2.1.1.5 Notes.....	14
2.1.2 NIC switching mode.....	14
2.1.2.1 Fault monitoring function.....	15
2.1.2.2 Switching function.....	17
2.1.2.3 Connectable remote host.....	19
2.1.2.4 Available application.....	19
2.1.2.5 Notes.....	19
2.1.3 Virtual NIC mode.....	19
2.1.3.1 Fault monitoring function.....	21
2.1.3.2 Switching function.....	22
2.1.3.3 Connectable remote host.....	22
2.1.3.4 Available application.....	22
2.1.4 GS linkage mode.....	22
2.1.4.1 Fault monitoring function.....	25
2.1.4.2 Switching function.....	26
2.1.4.3 Connectable remote host.....	26
2.1.4.4 Available applications.....	26
2.1.4.5 Notes.....	27
2.2 Interface structure.....	27
2.2.1 Configuring multiple virtual interfaces.....	27
2.2.2 Sharing physical interface.....	28
2.2.2.1 Using Fast switching mode.....	28
2.2.2.2 Using NIC switching mode.....	29
2.2.2.3 Using GS linkage mode.....	30
2.2.2.4 Notices.....	30
2.2.3 Configuring multiple logical virtual interfaces.....	30
2.2.4 Configuring single physical interface.....	32
2.2.5 Configuring Tagged VLAN interfaces.....	32
2.2.5.1 Redundant Line Control function using Tagged VLAN interface.....	33
2.3 Monitoring function of Fast switching mode.....	36
2.3.1 Communication target monitoring.....	36
2.4 Monitoring function of NIC switching mode.....	37
2.4.1 HUB monitoring function.....	37
2.4.1.1 Not using HUB-to-HUB monitoring feature.....	38
2.4.1.2 Using HUB-to-HUB monitoring feature.....	39
2.4.2 Standby patrol function.....	41
2.4.3 Automatic fail-back function.....	41
2.5 Monitoring function of Virtual NIC mode.....	44
2.5.1 Link status monitoring function.....	44
2.5.2 Network monitoring function.....	44
2.6 Monitoring function of GS linkage mode.....	45

2.6.1 Communication target monitoring.....	46
2.7 Other monitoring functions.....	46
2.7.1 Interface status monitoring feature.....	46
2.7.2 Self-checking function.....	47
2.8 Linkage functions.....	47
2.8.1 Cluster fail-over when entire transfer routes fails.....	48
2.8.1.1 Cluster fail-over of Fast switching mode.....	49
2.8.1.2 Cluster fail-over of NIC switching mode.....	49
2.8.1.3 Cluster fail-over of Virtual NIC mode.....	50
2.8.1.4 Cluster fail-over of GS linkage mode.....	51
2.8.2 User command execution function.....	51
2.9 Maintenance function.....	58
2.9.1 Dynamically adding/deleting/switching physical interface.....	59
2.9.2 Active maintenance of NIC (PCI card).....	61
2.10 Notes.....	62
2.10.1 General.....	62
2.10.2 Duplicated operation by Fast switching mode.....	62
2.10.3 Duplicated operation via NIC switching mode.....	63
2.10.4 Duplicated operation via Virtual NIC mode.....	63
2.10.5 Duplicated operation via GS linkage mode.....	64
<b>Chapter 3 Environment configuration.....</b>	<b>66</b>
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 Virtual NIC mode.....	69
3.1.2.4 GS linkage mode.....	71
3.1.2.5 Configuration of individual mode.....	72
3.1.2.6 Upper limit of configuration.....	76
3.2 System Setup.....	77
3.2.1 Setup kernel parameters.....	78
3.2.2 Network configuration.....	78
3.2.2.1 Setup common to modes.....	78
3.2.2.2 System setup in Fast switching mode.....	85
3.2.2.3 System setup in NIC switching mode.....	86
3.2.2.4 System setup in Virtual NIC mode.....	87
3.2.2.5 System setup in GS linkage mode.....	87
3.2.3 Setting up the system log.....	88
3.3 Additional system setup.....	89
3.3.1 Fast switching mode.....	89
3.3.2 NIC switching mode.....	90
3.3.3 Virtual NIC mode.....	90
3.3.4 GS linkage mode.....	93
3.3.5 Setting parameter for individual mode.....	94
3.4 Changing system setup.....	94
3.4.1 Fast switching mode.....	94
3.4.2 NIC switching mode.....	96
3.4.3 Virtual NIC mode.....	102
3.4.4 GS linkage mode.....	111
3.4.5 Note on changing configuration information.....	114
3.5 Deleting configuration information.....	114
3.5.1 Fast switching mode.....	114
3.5.2 NIC switching mode.....	114
3.5.3 Virtual NIC mode.....	115
3.5.4 GS linkage mode.....	115

3.5.5 Note on deleting configuration information.....	115
3.6 Configuring interfaces.....	115
3.6.1 Configuring multiple virtual interfaces.....	115
3.6.2 Sharing physical interface.....	116
3.6.3 Multiple logical virtual interface definition.....	116
3.6.4 Single physical interface definition.....	117
3.6.5 Transfer route multiplexing with Tagged VLAN interface.....	117
3.6.5.1 Operating tagged VLAN interface on Fast switching mode.....	117
3.6.5.2 Operating tagged VLAN interface on NIC switching mode.....	118
3.6.5.3 Operating tagged VLAN interface on Virtual NIC mode.....	121
3.7 Setting monitoring function of Fast switching mode.....	121
3.7.1 Communication target monitoring function.....	121
3.7.1.1 Setting the monitoring destination information.....	121
3.7.1.2 Setting the monitoring interval.....	121
3.7.1.3 Setting the message output when a monitoring error occurs.....	122
3.8 Setting monitoring function of NIC switching mode.....	122
3.8.1 HUB monitoring.....	122
3.8.1.1 Creating monitoring information.....	122
3.8.1.2 Enabling HUB monitoring function.....	122
3.8.1.3 Transfer route error detection time for NIC switching mode.....	124
3.8.2 Standby patrol function.....	129
3.8.2.1 Setting what to be monitored.....	129
3.8.2.2 Setting monitoring interval.....	129
3.8.2.3 Setting error monitoring interval.....	129
3.8.3 Setting parameters for each virtual interface.....	129
3.9 Setting monitoring function of Virtual NIC mode.....	131
3.9.1 Link status monitoring function.....	131
3.9.2 Network monitoring function.....	131
3.9.2.1 Disabling the network monitoring function.....	131
3.9.2.2 Setting the monitoring destination information.....	131
3.9.2.3 Enabling the network monitoring function.....	131
3.9.2.4 Transfer route error detection time for network monitoring function.....	131
3.9.2.5 Transfer route recovery detection time for network monitoring function.....	133
3.10 Setting monitoring function of GS linkage mode.....	135
3.10.1 Monitoring the remote host.....	135
3.10.1.1 Setting the monitoring destination information.....	135
3.10.1.2 Transfer route error detection time in GS linkage mode.....	142
3.10.1.3 Transfer route recovery detection time in GS linkage mode.....	143
3.11 Setting other monitoring function.....	145
3.11.1 Interface status monitoring feature.....	145
3.11.2 Self-checking feature.....	145
3.11.2.1 How to set up the self-checking function.....	145
3.11.2.2 Error detection of the self-checking function.....	145
3.12 Setting Linkage function.....	147
3.12.1 Cluster switching behavior for failure of all the transfer paths.....	147
3.12.2 Setting user command execution function.....	147
3.12.2.1 Settings for NIC switching mode.....	149
3.12.2.2 Settings for GS linkage mode.....	154
3.12.2.3 Settings for Self-checking function.....	156
3.13 Setting Maintenance function.....	157
3.13.1 Setting dynamic addition/deletion/switching function of physical interfaces.....	157
3.13.1.1 Dynamic addition of physical interfaces.....	157
3.13.1.2 Dynamic deletion of physical interfaces.....	157
3.13.1.3 Dynamic switching of physical interfaces.....	157
3.13.2 Active maintenance of NIC (PCI card).....	157
Chapter 4 Operation.....	158



4.1 Starting and Stopping Redundant Line Control Function.....	158
4.1.1 Starting Redundant Line Control Function.....	158
4.1.2 Stopping Redundant Line Control Function.....	158
4.2 Activating and Inactivating Virtual Interfaces.....	158
4.2.1 Activating virtual interfaces.....	159
4.2.2 Inactivating virtual interfaces.....	159
4.3 Displaying Operation Status.....	159
4.4 Displaying Monitoring Status.....	159
4.5 Recovery Procedure from Line Failure.....	159
4.5.1 Recovery procedure from line failure in Fast switching mode and GS linkage mode .....	160
4.5.2 Recovery procedure from line failure in NIC switching mode.....	160
4.5.3 Recovery procedure from line failure in Virtual NIC mode.....	160
4.6 Backing up and Restoring Configuration Files.....	160
4.6.1 Backing up Configuration Files.....	160
4.6.2 Restoring Configuration Files.....	160
Chapter 5 GLS operation on cluster systems.....	162
5.1 Outline of Cluster System Support.....	162
5.2 Configuration for Cluster system.....	163
5.2.1 Adding configuration.....	164
5.2.2 Modifying configuration for Cluster system.....	165
5.2.3 Deleting configuration.....	165
5.3 Configuration for user application.....	167
5.3.1 Monitoring resource status of standby node.....	167
5.3.1.1 Preface.....	167
5.3.1.2 Configuration.....	167
5.3.1.3 Recovering from a resource failure in Standby node.....	167
5.4 Operation on cluster systems.....	168
5.4.1 Active Standby (Fast switching mode).....	168
5.4.1.1 Starting.....	168
5.4.1.2 Switching.....	168
5.4.1.3 Fail-back.....	170
5.4.1.4 Stopping.....	170
5.4.2 Active Standby (NIC switching mode).....	171
5.4.2.1 Starting.....	171
5.4.2.2 Switching.....	174
5.4.2.3 Fail-back.....	178
5.4.2.4 Stopping.....	179
5.4.3 Active Standby (Virtual NIC mode).....	181
5.4.3.1 Starting.....	181
5.4.3.2 Switching.....	182
5.4.3.3 Fail-back.....	183
5.4.3.4 Stopping.....	184
5.4.4 Active Standby (GS linkage mode).....	184
5.4.4.1 Starting.....	184
5.4.4.2 Switching.....	185
5.4.4.3 Fail-back.....	187
5.4.4.4 Stopping.....	187
5.4.5 Mutual standby (Fast switching mode).....	187
5.4.5.1 Starting.....	187
5.4.5.2 Switching.....	188
5.4.5.3 Fail-back.....	188
5.4.5.4 Stopping.....	188
5.4.6 Mutual standby (NIC switching mode).....	188
5.4.6.1 Starting.....	188
5.4.6.2 Switching.....	188
5.4.6.3 Fail-back.....	190

5.4.6.4 Stopping.....	190
5.4.7 Mutual standby (Virtual NIC mode).....	190
5.4.7.1 Starting.....	190
5.4.7.2 Switching.....	190
5.4.7.3 Fail-back.....	191
5.4.7.4 Stopping.....	191
5.4.8 Mutual standby (GS linkage mode).....	191
5.4.8.1 Starting.....	191
5.4.8.2 Switching.....	191
5.4.8.3 Fail-back.....	192
5.4.8.4 Stopping.....	192
5.4.9 Cascade (Fast switching mode).....	192
5.4.9.1 Starting.....	192
5.4.9.2 Switching.....	193
5.4.9.3 Fail-back.....	194
5.4.9.4 Stopping.....	195
5.4.10 Cascade (NIC switching mode).....	195
5.4.10.1 Starting.....	195
5.4.10.2 Switching.....	198
5.4.10.3 Fail-back.....	202
5.4.10.4 Stopping.....	202
5.4.11 Cascade (Virtual NIC mode).....	205
5.4.11.1 Starting.....	205
5.4.11.2 Switching.....	206
5.4.11.3 Fail-back.....	207
5.4.11.4 Stopping.....	208
5.5 Tagged VLAN interface multiplexing on cluster system.....	208
5.5.1 Active standby (Fast switching mode).....	208
5.5.2 Active standby (NIC switching mode).....	209
5.5.3 Active Standby (Virtual NIC mode).....	210
5.5.4 Mutual Standby (Fast switching mode).....	210
5.5.5 Mutual Standby (NIC switching mode).....	211
5.5.6 Mutual Standby (Virtual NIC mode).....	212
5.5.7 Cascade (Fast switching mode).....	212
5.5.8 Cascade (NIC switching mode).....	213
5.5.9 Cascade (Virtual NIC mode).....	213
Chapter 6 Maintenance.....	215
6.1 Redundant Line Control Function Troubleshooting Data to be Collected.....	215
6.1.1 Command to collect materials.....	215
6.1.2 Collecting packet traces.....	220
6.2 HUB maintenance.....	220
6.2.1 Swapping HUB procedure (Fast switching mode / GS linkage mode).....	220
6.2.2 Swapping HUB procedure (NIC switching mode / IP address remains unchanged).....	221
6.2.3 Swapping HUB procedure (NIC switching mode / IP address is changed).....	222
6.2.4 Swapping HUB procedure (Virtual NIC mode / IP address remains unchanged).....	223
6.2.5 Swapping HUB procedure (Virtual NIC mode / IP address is changed).....	224
6.3 NIC maintenance (for RHEL5).....	225
6.3.1 Shutdown maintenance of NIC.....	225
6.3.2 Active maintenance of NIC.....	227
6.3.2.1 Addition procedure.....	228
6.3.2.2 Removal procedure.....	235
6.3.2.3 Swapping procedure.....	240
6.4 NIC maintenance (for RHEL6).....	249
6.4.1 Shutdown maintenance for a NIC.....	249
6.4.2 Active maintenance of NIC.....	250
6.4.2.1 Addition procedure.....	251

6.4.2.2 Removal procedure.....	256
6.4.2.3 Swapping procedure.....	260
Chapter 7 Command references.....	271
7.1 hanetconfig Command.....	271
7.2 strhanet Command.....	281
7.3 stphanet Command.....	283
7.4 dsphanet Command.....	285
7.5 hanetmask Command.....	287
7.6 hanetparam Command.....	290
7.7 hanetpoll Command.....	295
7.8 dsppoll Command.....	304
7.9 hanetnic Command.....	305
7.10 strptl Command.....	308
7.11 stpptl Command.....	308
7.12 hanetpathmon Command.....	309
7.13 dsppathmon Command.....	315
7.14 hanetgw Command.....	316
7.15 hanetobserv Command.....	318
7.16 dspobserv Command.....	324
7.17 hanethvrsc Command.....	325
7.18 hanetbackup Command.....	330
7.19 hanetrestore Command.....	330
7.20 resethanet Command.....	331
Appendix A Messages and corrective actions.....	333
A.1 Messages Displayed by Redundant Line Control Function.....	333
A.1.1 Information message (number 0) .....	334
A.1.2 Error output message (numbers 100 to 700) .....	334
A.1.3 Console output messages (numbers 800 to 900).....	356
A.2 Messages Displayed in the Cluster System Logs.....	367
Appendix B Examples of configuring system environments.....	370
B.1 Example of configuring Fast switching mode (IPv4) .....	370
B.1.1 Example of the Single system.....	370
B.1.2 Example of the Single system in Logical virtual interface.....	372
B.1.3 Configuring virtual interfaces with tagged VLAN.....	375
B.1.4 Example of the Cluster system (1:1 Standby).....	379
B.1.5 Example of the Cluster system (Mutual Standby) .....	382
B.1.6 Example of the Cluster system (N:1 Standby) .....	385
B.1.7 Example of the Cluster system (Cascade) .....	389
B.2 Example of configuring Fast switching mode (IPv6) .....	393
B.2.1 Example of the Single system.....	393
B.2.2 Example of the Single system in Logical virtual interface.....	396
B.2.3 Configuring virtual interfaces with tagged VLAN.....	399
B.2.4 Example of the Cluster system (1:1 Standby) .....	404
B.2.5 Example of the Cluster system (Mutual standby) .....	408
B.2.6 Example of the Cluster system (N:1 Standby) .....	412
B.2.7 Example of the Cluster system (Cascade).....	417
B.3 Example of configuring Fast switching mode (IPv4/IPv6) .....	422
B.3.1 Example of the Single system.....	422
B.3.2 Example of the Single system in Logical virtual interface.....	426
B.3.3 Configuring virtual interfaces with tagged VLAN.....	430
B.3.4 Example of the Cluster system (1:1 Standby).....	436
B.3.5 Example of the Cluster system (Mutual standby).....	440
B.3.6 Example of the Cluster system (N:1 Standby).....	444
B.3.7 Example of the Cluster system (Cascade).....	450
B.4 Example of configuring NIC switching mode (IPv4).....	456

B.4.1 Example of the Single system without NIC sharing.....	456
B.4.2 Example of the Single system with NIC sharing.....	459
B.4.3 Example of the Single system in Takeover physical IP address (pattern II).....	463
B.4.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching).....	465
B.4.5 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching).....	470
B.4.6 Configuring virtual interfaces with tagged VLAN (Physical IP takeover, Asynchronous switching).....	475
B.4.7 Example of the Cluster system (1:1 Standby).....	479
B.4.8 Example of the Cluster system (Mutual standby) without NIC sharing.....	483
B.4.9 Example of the Cluster system (Mutual standby) with NIC sharing.....	487
B.4.10 Example of the Cluster system in Takeover physical IP address (pattern I).....	491
B.4.11 Example of the Cluster system in Takeover physical IP address (pattern II).....	494
B.4.12 Example of the Cluster system (Cascade).....	498
B.4.13 Example of the Cluster system (NIC non-redundant).....	502
B.5 Example of configuring NIC switching mode (IPv6).....	505
B.5.1 Example of the Single system without NIC sharing.....	505
B.5.2 Example of the Single system with NIC sharing.....	508
B.5.3 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching).....	511
B.5.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching).....	515
B.5.5 Example of the Cluster system (1:1 Standby).....	518
B.5.6 Example of the Cluster system (Mutual standby) without NIC sharing.....	521
B.5.7 Example of the Cluster system (Mutual standby) with NIC sharing.....	525
B.5.8 Example of the Cluster system (Cascade).....	529
B.6 Example of configuring NIC switching mode (IPv4/IPv6).....	532
B.6.1 Example of the Single system without NIC sharing.....	533
B.6.2 Example of the Single system with NIC sharing.....	536
B.6.3 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching).....	539
B.6.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching).....	544
B.6.5 Example of the Cluster system (1:1 Standby) without NIC sharing.....	549
B.6.6 Example of the Cluster system (Mutual Standby) without NIC sharing.....	553
B.6.7 Example of the Cluster system (Mutual Standby) with NIC sharing.....	558
B.6.8 Example of the Cluster system (Cascade).....	562
B.7 Example of configuring Virtual NIC mode.....	567
B.7.1 Example of the Single system.....	567
B.7.2 Configuring virtual interfaces with tagged VLAN.....	569
B.7.3 Example of the Cluster system (1:1 Standby).....	572
B.7.4 Example of the Cluster system (Mutual Standby).....	575
B.7.5 Example of the Cluster system (Cascade).....	577
B.7.6 Example of the Cluster system (No IP takeover).....	581
B.8 Example of configuring GS linkage mode .....	583
B.8.1 Example of the Single system.....	583
B.8.2 Example of the Single system on remote network.....	585
B.8.3 Example of the Single system (GS Hot-standby).....	588
B.8.4 Example of the Single system (GS Load Sharing).....	591
B.8.5 Example of the Cluster system (1:1 Standby).....	593
B.8.6 Example of the Cluster system on remote network(1:1 Standby).....	597
B.8.7 Example of the Cluster system (Mutual Standby).....	602
Appendix C Operation on the Virtual Machine Function (For RHEL5).....	607
C.1 Virtual machine function overview.....	607
C.2 Configuration of the virtual machine function.....	607
C.3 Virtual network design.....	609
C.3.1 Concept of network configuration in the virtual machine function.....	609
C.3.2 Support set for each redundant line switching mode.....	609
C.3.3 Flow for selecting the virtual network configuration in each redundant line switching mode.....	609
C.3.4 Details on each configuration.....	612
C.4 Operation of redundant line switching mode on the virtual machine function.....	618
C.4.1 Configuration for creating a highly reliable network of guest domains with GLS on domain-0 (Configuration 1).....	618

C.4.2 Configuration for creating a highly reliable network on guest domains of a single system (Configuration 2).....	621
C.4.3 Configuration for creating a highly reliable network on guest domains of a cluster system (Configuration 3).....	627
C.5 Setting up redundant line switching mode on the virtual machine function (Fast switching mode and NIC switching mode).....	627
C.5.1 Setting up the virtual network on the host OS.....	627
C.5.2 Assigning the IP address, setting the transfer route and others (for host OS).....	629
C.5.3 Setting up GLS (for host OS).....	629
C.5.4 Settings for creating a highly reliable network of guest domains (guest OSes) using GLS on domain-0 (host OS).....	630
C.5.5 Setting up GLS on guest domains (guest OSes).....	630
C.6 Setting up redundant line switching mode on the virtual machine function (Virtual NIC mode).....	630
C.6.1 Assigning the IP address, setting the transfer route and others (for host OS).....	631
C.6.2 Setting up GLS (for host OS).....	631
C.6.3 Setting up the virtual network on the host OS (Configuration 1).....	631
C.6.4 Setting up the virtual network on the host OS (Configuration 2 and Configuration 3).....	633
C.6.5 Setting up GLS on guest domains (guest OSes).....	634
C.7 Examples of configuration setup (Fast switching mode and NIC switching mode).....	634
C.7.1 Setup example for creating a highly reliable network of guest domains using GLS on domain-0 (Untagged VLAN and single network configuration).....	634
C.7.2 Setup example for creating a highly reliable guest domains using GLS on domain-0 (Untagged VLAN and multiple network configuration).....	638
C.7.3 Setup example for creating a highly reliable domains using GLS on domain-0 (Tagged VLAN and multiple network configuration).....	644
C.7.4 Setup example for achieving high reliability using GLS on each guest domain of a cluster system.....	648
C.8 Examples of configuration setup (Virtual NIC mode).....	649
C.8.1 Setup example for creating a highly reliable network of guest domains using GLS on domain-0 (Untagged VLAN and single network configuration).....	649
C.8.2 Setup example for creating a highly reliable guest domains using GLS on domain-0 (Untagged VLAN and multiple network configuration).....	652
C.8.3 Setup example for creating a highly reliable domains using GLS on domain-0 (Tagged VLAN and multiple network configuration).....	653
C.8.4 Setup example for achieving high reliability using GLS on each guest domain of a cluster system.....	654
Appendix D Operation on the Virtual Machine Function (for RHEL6).....	656
D.1 Virtual Machine Function Overview.....	656
D.2 Configuration of the Virtual Machine Function.....	656
D.3 Virtual Network Design in Virtual Machine Function.....	656
D.3.1 Concept of network configuration in the virtual machine function.....	656
D.3.2 Support set for each redundant line switching mode.....	657
D.3.3 Flow for selecting the virtual network configuration in each redundant line switching mode.....	657
D.3.4 Details on each configuration.....	657
D.4 Operation of Redundant Line Switching Mode on the Virtual Machine Function.....	659
D.4.1 Configuration for creating a highly reliable network of KVM guests on the KVM host (Configuration 1).....	659
D.4.2 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2).....	660
D.4.3 Configuration for creating a highly reliable network on each KVM guest of a cluster system (Configuration 3).....	661
D.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function.....	661
D.5.1 Setting up the virtual network on the host OS.....	662
D.5.2 Assigning the IP address, setting the transfer route and others (for host OS).....	662
D.5.3 Setting up GLS (for host OS).....	662
D.5.4 Sample configurations for the virtual bridge.....	662
D.5.5 Setting up GLS on guest domains (guest OSes).....	664
D.6 Examples of Configuration Setup.....	664
D.6.1 Setup example for creating a highly reliable network of guest domains on KVM hosts (Untagged VLAN).....	664
D.6.2 Setup example for creating a highly reliable network of guest domains on KVM hosts (Tagged VLAN).....	666
D.6.3 Setup example for achieving high reliability using GLS on each guest domain of a cluster system.....	668
D.6.4 Setup example for creating a highly reliable network of guest domains on KVM hosts in a cluster system.....	672
Appendix E Operation on VMware.....	675
E.1 VMware Overview.....	675
E.2 Configuration of VMware.....	675

E.3 Virtual Network Design in VMware.....	675
E.3.1 Concept of network configuration in VMware.....	675
E.3.2 Support set for each redundant line switching mode.....	676
E.4 Operation of Redundant Line Switching Mode on VMware.....	676
E.4.1 Configuration for creating a highly reliable network on guest OSES in a single system.....	676
E.4.2 Configuration for creating a highly reliable network on guest OSES in a cluster system.....	678
E.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function.....	678
E.6 Examples of Configuration Setup.....	678
E.6.1 Setup example for creating a highly reliable network of guest OSES.....	678
E.6.2 Setup example for creating a highly reliable network of guest OSES in a cluster system.....	679
Appendix F Trouble shooting.....	680
F.1 Communication as expected cannot be performed (Common to IPv4 and IPv6) .....	680
F.1.1 The route information set by a route command is deleted.....	680
F.1.2 Automatic address configuration lags behind for IPv6.....	680
F.1.3 Communication is not switched in the event of HUB monitoring error in Virtual NIC mode.....	680
F.2 Virtual interface or the various functions of Redundant Line Control Function cannot be used.....	682
F.2.1 An interface of NIC switching mode is not activated.....	682
F.2.2 It does not failback at the time of the restoration detection by standby patrol in NIC switching mode.....	683
F.2.3 Error detection message displays for standby patrol in NIC switching mode.....	683
F.3 Failure occurs during operation (Common to both Single and Cluster system).....	684
F.3.1 Error messages(870) and corresponding actions for HUB monitoring.....	684
F.3.2 Error messages(875) and corresponding actions for standby patrol.....	687
F.3.3 Switching takes place in NIC switching mode regardless of failure at the monitoring end.....	691
F.3.4 Takes time to execute an operation command or to activate a cluster service.....	691
F.3.5 Unable to communicate using virtual IP addresses after configuring a firewall.....	692
F.3.6 Virtual driver hang detected by Self-checking function.....	693
F.4 Failure occurs during operation (In the case of a Cluster system).....	694
F.4.1 Node switching is not executed in Fast switching mode.....	694
F.5 Resuming connection lags after switching (Common to both Single and Cluster system).....	694
F.5.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode.....	694
F.6 Incorrect operation by the user.....	695
F.6.1 Accidentally deleted the virtual interface with ifconfig command.....	695
Appendix G Check list.....	696
G.1 Checkpoint list.....	696
G.2 Setup common to modes.....	697
G.2.1 Network configuration.....	697
G.2.2 VLAN Setup.....	698
G.2.3 Redundant network configuration.....	699
G.2.4 Firewall settings.....	699
G.2.5 IP address settings.....	700
G.2.6 Subnet mask settings.....	701
G.2.7 Hotplug settings.....	702
G.2.8 Hostname settings.....	702
G.2.9 Distribution procedure after settings change.....	703
G.2.10 Procedure for network device maintenance.....	703
G.2.11 Network device rate settings.....	704
G.2.12 Application.....	705
G.3 Fast switching mode.....	705
G.3.1 Network address.....	705
G.3.2 Node configuration.....	706
G.4 NIC switching mode.....	707
G.4.1 Monitoring destination selection.....	707
G.4.2 Monitoring time adjustment.....	708
G.4.3 Network cable.....	708
G.4.4 Static route settings.....	708
G.5 Virtual NIC mode.....	709

G.5.1 Interface setting file.....	709
G.5.2 Monitoring destination selection.....	709
G.5.3 Monitoring time adjustment.....	710
G.5.4 Network cable.....	710
G.6 GS linkage mode.....	711
G.6.1 Network address.....	711
G.6.2 Communication target setting.....	714
G.6.3 Network device settings.....	715
G.6.4 Monitoring time adjustment.....	716
G.6.5 Maintenance procedure performed when the communication target stopped.....	716
G.6.6 PTF of the communication target.....	718
Appendix H Changes from previous versions.....	719
H.1 Changes from Redundant Line Control function 4.0A20 to version 4.1A20.....	719
H.1.1 New commands.....	719
H.1.2 Incompatible commands.....	719
H.1.3 Incompatible functions.....	721
H.2 Changes from Redundant Line Control function 4.1A20 to version 4.1A30.....	722
H.2.1 New commands.....	722
H.2.2 Incompatible commands.....	722
H.2.3 Incompatible functions.....	722
H.3 Changes from Redundant Line Control function 4.1A30 to version 4.1A40.....	724
H.4 Changes from Redundant Line Control function 4.1A40 to version 4.2A00.....	724
H.4.1 New commands.....	724
H.4.2 Incompatible commands.....	724
H.4.3 Incompatible functions.....	724
H.5 Changes from Redundant Line Control function 4.2A00 to version 4.2A30.....	724
H.5.1 New commands.....	725
H.5.2 Incompatible commands.....	725
H.5.3 Incompatible functions.....	725
H.6 Changes from Redundant Line Control function 4.2A30 to version 4.3A00.....	726
H.6.1 New commands.....	726
H.6.2 Incompatible commands.....	727
H.6.3 Incompatible functions.....	727
H.7 Functional Improvements in Redundant Line Control function 4.3A00.....	728
H.7.1 New commands.....	728
H.7.2 Incompatible commands.....	728
H.7.3 Incompatible functions.....	730
H.8 Changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10.....	732
H.8.1 New commands.....	732
H.8.2 Incompatible commands.....	733
H.8.3 Incompatible functions.....	735
H.9 Changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20.....	737
H.9.1 New commands.....	738
H.9.2 Incompatible commands.....	738
H.9.3 Incompatible functions.....	738
H.10 Changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30.....	739
H.10.1 New commands.....	739
H.10.2 Incompatible commands.....	739
H.10.3 Incompatible functions.....	740
Glossary.....	742
Index.....	747

# Chapter 1 Overview

This chapter discusses the concept of the redundant line control function provided by 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:

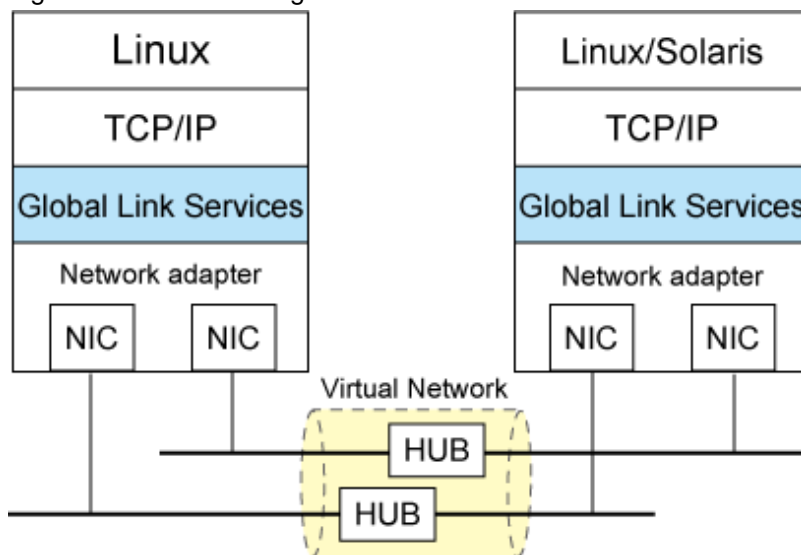
### Fast switching mode

In Fast switching mode, a redundant transmission route between Linux servers or Solaris 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 PRIMEQUEST, PRIMERGY, SPARC M10, SPARC Enterprise, PRIMEPOWER, and other systems where GLS's Fast switching mode is running.

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

Moreover, you can use a single transfer path. For details, refer to ["2.2.4 Configuring single physical interface"](#).

Figure 1.1 Fast switching mode



### NIC switching mode

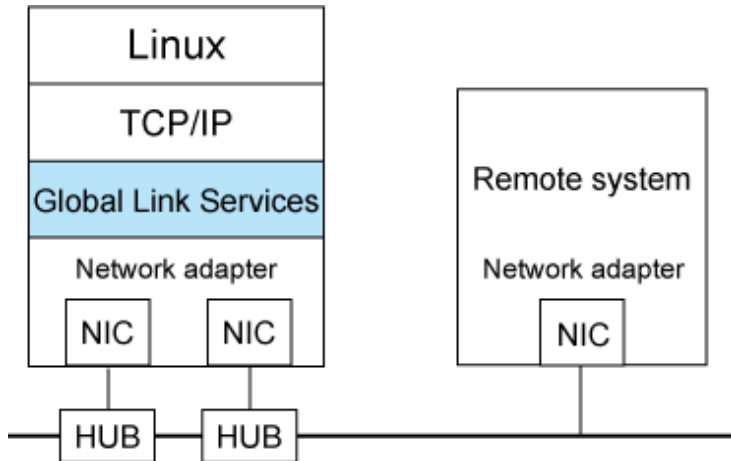
In NIC switching mode, redundant NICs (LAN cards) are connected to each other on the same network and used exclusively. If one transmission route fails, ongoing communications will be switched to the other transmission route. There are no restrictions on remote systems to communicate with.

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

Moreover, you can use a single physical interface. For details, refer to ["2.2.4 Configuring single physical interface"](#).



Figure 1.2 NIC switching mode



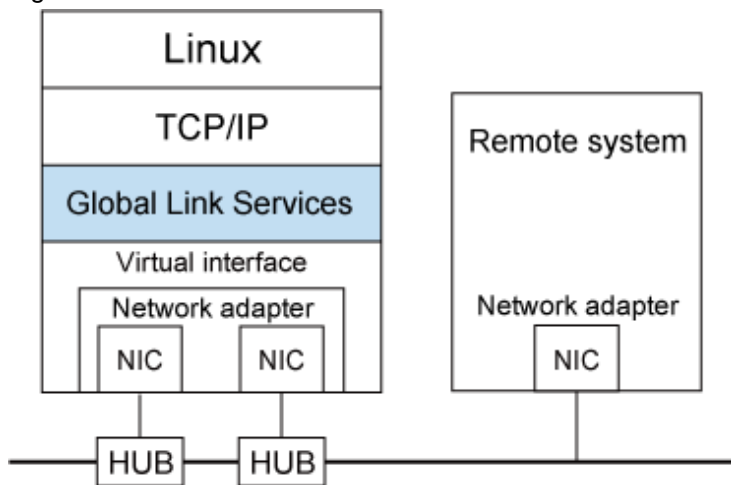
### Virtual NIC mode

In Virtual NIC mode, communication is performed by generating a virtual interface so that multiple physical NICs (LAN cards) can be seen as one logical NIC. In this mode, switching transfer routes is controlled by exclusive use of redundant NICs. 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 Virtual NIC mode can be used to communicate with any hosts on the other networks beyond the router.

Moreover, you can use a single physical interface. For details, refer to ["2.2.4 Configuring single physical interface"](#).

Figure 1.3 Virtual NIC mode

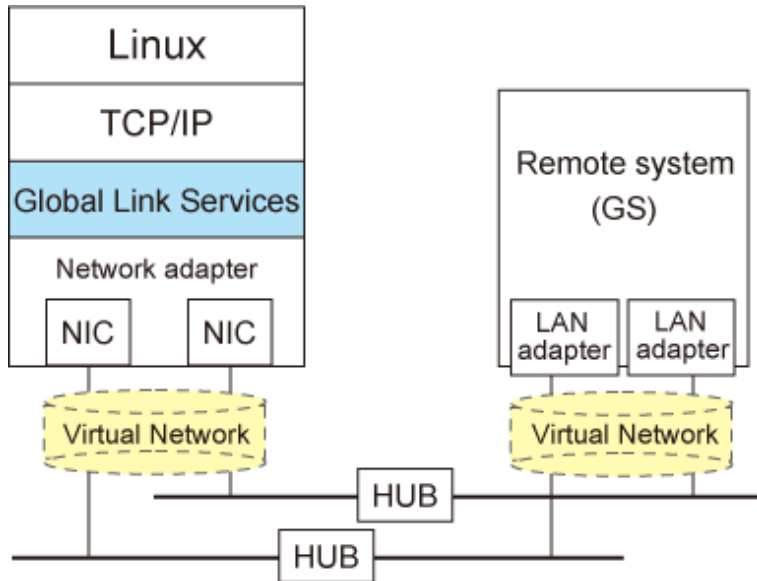


### GS linkage mode

GS linkage mode enables the system to control lines by using a Fujitsu method for high-reliability communication between the system and Global Server. 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. The compatible hosts are Global Server and PRIMEQUEST or PRIMERGY where GLS's GS linkage mode is running.

Note that GS linkage mode can be used to communicate with any hosts on other networks connected to the router. You can use a single physical interface as well. For details, see ["2.2.4 Configuring single physical interface"](#). (Hereafter, GS refers to Global Server).

Figure 1.4 GS linkage mode



### 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, switch/HUB, remote host	NIC, cable, switch/HUB
	Fault monitoring	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.	Monitors switch/HUB using the ping command. If the switch/HUB communication is disrupted, a transmission route failure will be detected.
		Failure detection time	5 to 10 seconds (Default)	<ul style="list-style-type: none"> <li>- When an error is detected by ping: 22 to 27 seconds (Default)</li> <li>- When a NIC link down is detected: 2 to 7 seconds (Default)</li> </ul>
	Recovery monitoring	Monitoring recovery 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.	If a monitoring framework is sent from a standby NIC to an operating NIC, and the standby NIC receives a reply from the operating NIC within a specified time, transmission route recovery will be detected.

Redundant line switching method			Fast switching mode	NIC switching mode
		Recovery detection time	1 to 5 seconds (Default)	About 1 to 30 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.	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 disconnection of the failed route 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		PRIMEQUEST, PRIMERGY, SPARC M10, SPARC Enterprise, PRIMEPOWER, and other systems where GLS's Fast switching mode is running	Arbitrary host
	IP address		IPv4 address, IPv6 address	IPv4 address, IPv6 address

Table 1.2 Function comparison (2)

Redundant line switching method			Virtual NIC mode	GS 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 them concurrently. A stream of data is sent on a TCP connection.
Fault monitoring	Detectable failures		NIC, cable, switch/HUB	NIC, cable, HUB, router, remote host (system failure, etc)
	Fault monitoring	Monitoring method	<p>Link status monitoring: Monitors the link status of a physical NIC. If the link is down, the line is considered to be faulty.</p> <p>Network monitoring: Monitors the connectivity between active NIC/standby NIC and switch/HUB. If no response is received within a specified period of time, the line is considered to be faulty.</p>	Monitors a remote host using the ping command. If the communication is disrupted, a transmission route failure will be detected.
		Failure detection time	- When a NIC link down is detected (Link status	25 to 30 seconds. (Default)

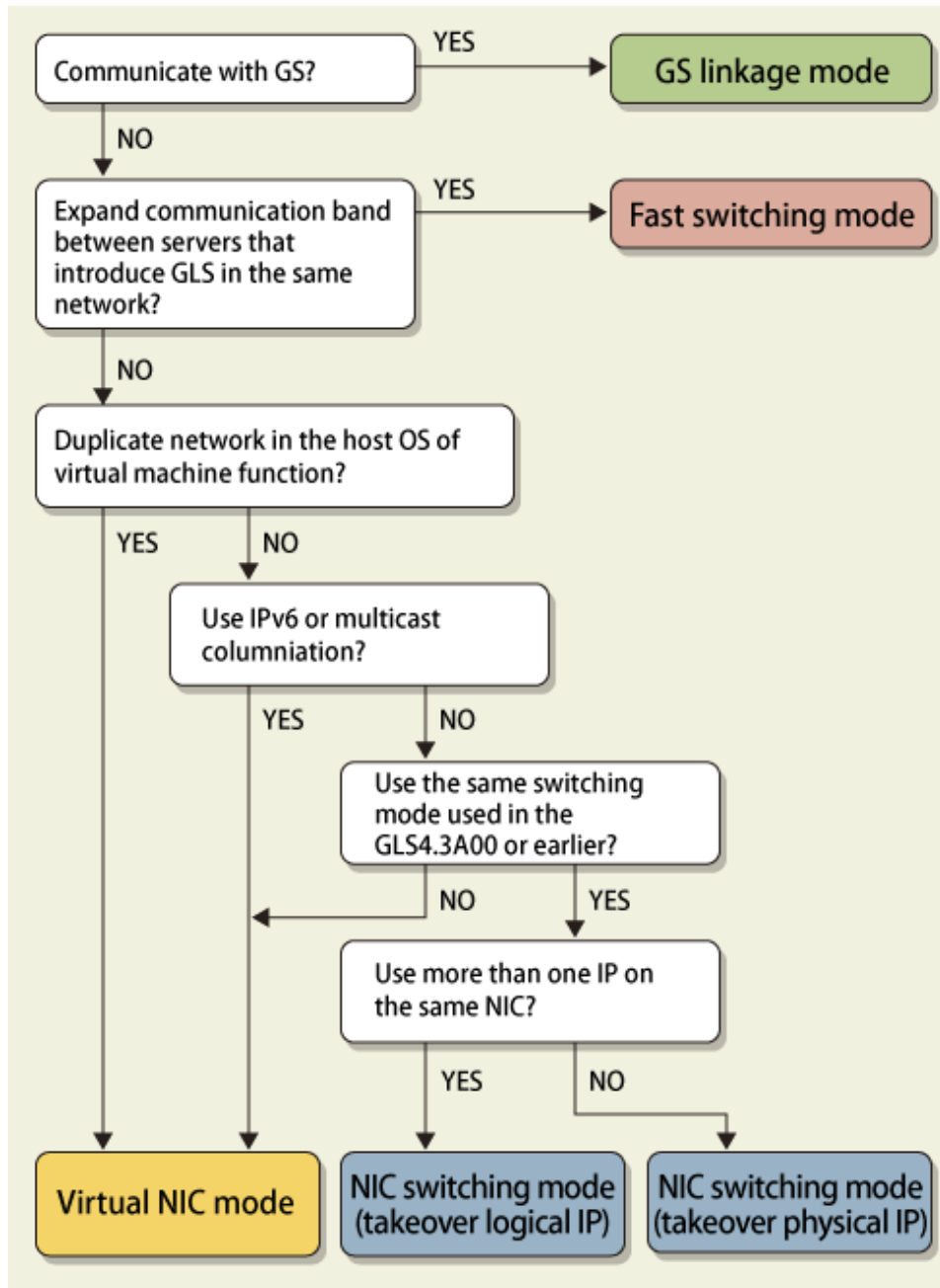
Redundant line switching method			Virtual NIC mode	GS linkage mode
			monitoring): About 1 second  - Network monitoring: 14 to 17 seconds (Default)	
	Recovery monitoring	Recovery monitoring method	If a monitoring framework is sent from a standby NIC to an operating NIC, and the standby NIC receives a reply from the operating NIC, 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.
		Detectable recovery time	3 to 5 seconds. (Default)	1 to 5 seconds. (Default)
	Fault monitoring start/stop		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.	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 deactivates NIC of a failed transmission route and activates a standby NIC. Manual switching operation is also allowed with the operational command.	Automatically disconnects a failed transmission route and uses the other transmission route. Manual switching operation is not supported.
	Switchback		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.	If a failed transmission route is recovered, it will automatically join communication. Manual rejoining is not supported.
Conditions	Remote hosts		Arbitrary host	GS (Global Server), PRIMEQUEST, PRIMERGY
	IP addresses		IPv4 address, IPv6 address	IPv4 address

### 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 1.5 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 1.5 Redundant line control method decision flow chart



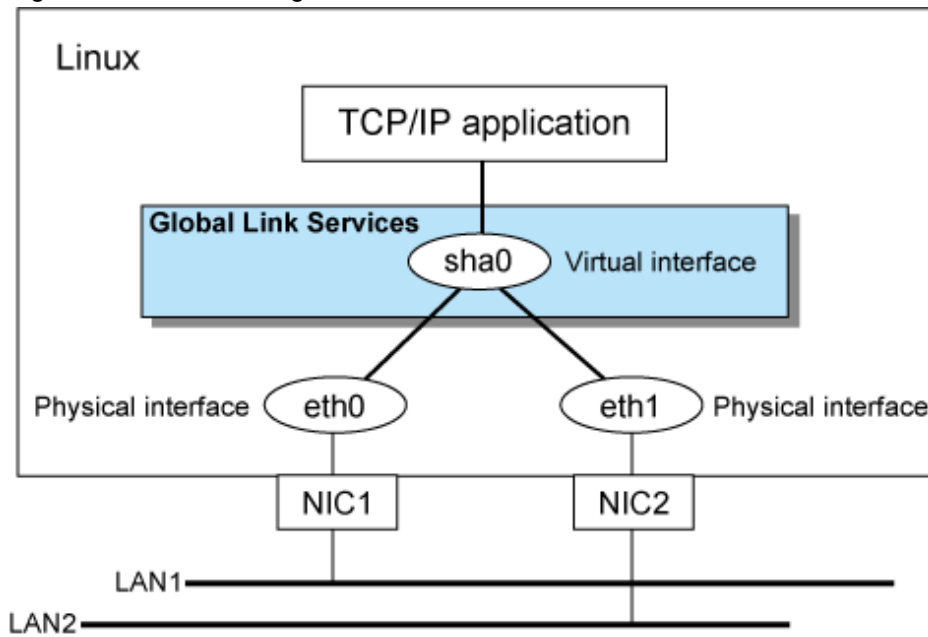
## 1.2 Redundant line control effects

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

## 1.3 System Configuration

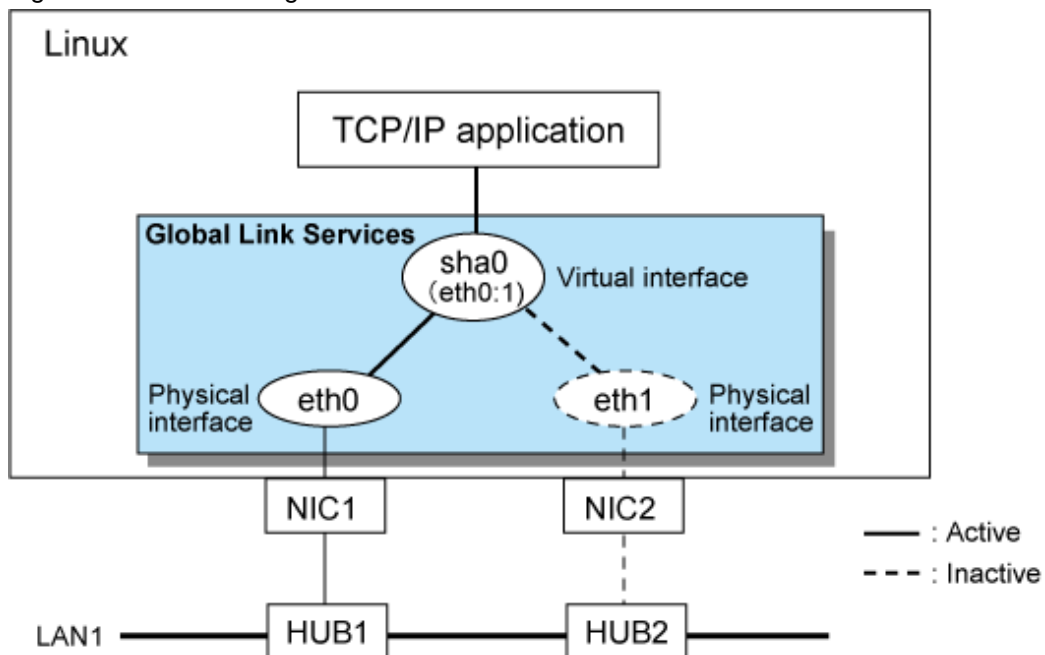
## Fast switching mode

Figure 1.6 Fast switching mode



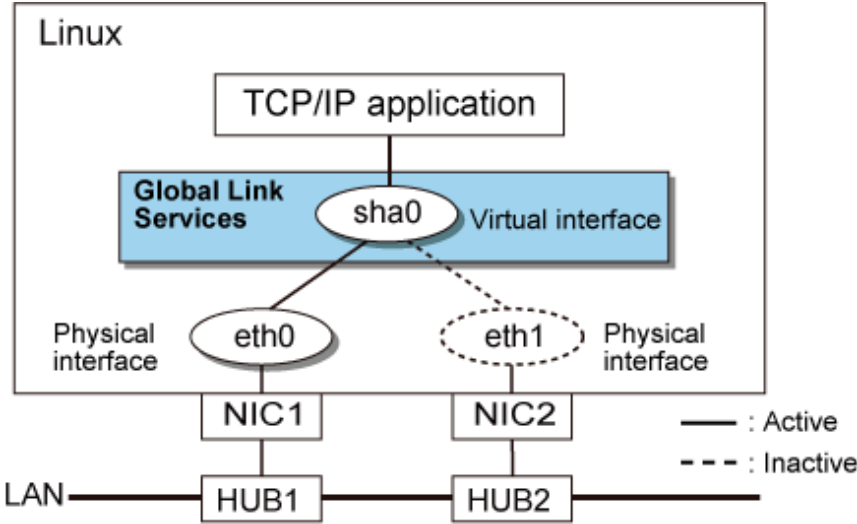
## NIC switching mode

Figure 1.7 NIC switching mode



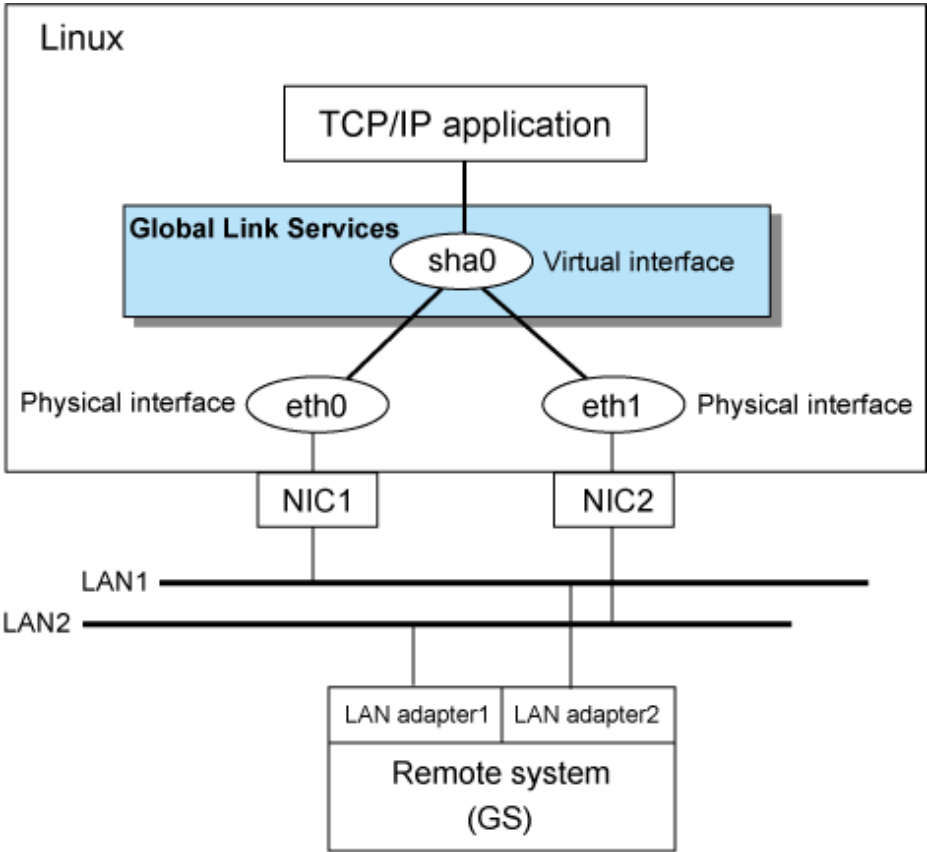
# Virtual NIC mode

Figure 1.8 Virtual NIC mode



# GS linkage mode

Figure 1.9 GS linkage mode



Redundant Line Control function consists of the following components:

Component	Description
Main unit	- PRIMEQUEST

Component		Description
		- PRIMERGY
NIC (Network Interface Cards)		The following Fujitsu adapters or cards can be used: <ul style="list-style-type: none"> <li>- On-board LAN card</li> <li>- LAN cards supported by PRIMEQUEST and PRIMERGY</li> </ul>
Switch/HUB (NIC switching mode, Virtual NIC mode)		IP address information must be configured for switch/HUB, e.g. switch/HUB with SNMP agent
Operating system (OS)		For details about the operating system supported by the redundant line control function, see the GLS Installation Guide.
Interfaces	Physical interface	Generated by each NIC. (e.g. ethX).
	Tagged VLAN interface	Interface (e.g. eth0.2, eth1.3) that is generated through tagged VLAN (IEEE 802.1Q).  In Virtual NIC mode, a tagged VLAN interface (e.g. sha0.X) is generated on a virtual interface for redundant communication of a tagged VLAN.
	Virtual interface	Generated through redundant line control (e.g. sha0 and sha1). Network applications can communicate using a virtual IP address assigned to the virtual interface.  In NIC switching mode, 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.
Network number	Fast switching mode GS linkage mode	A different network number is assigned to each physical interface and a virtual interface.  In <a href="#">Figure 1.6 Fast switching mode</a> , three network numbers must be prepared for the three interfaces.
	NIC switching mode	Only one number is assigned to each network. No virtual interface is generated
	Virtual NIC mode	Only one number is assigned to each network to connect NIC to the same segment.
IP address	Fast switching mode	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.
	NIC switching mode	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.
	Virtual NIC mode	Both IPv4 address and IPv6 address can be used as an address form.
	GS linkage mode	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.



## Chapter 2 Feature description

This chapter outlines the functions and features of GLS.

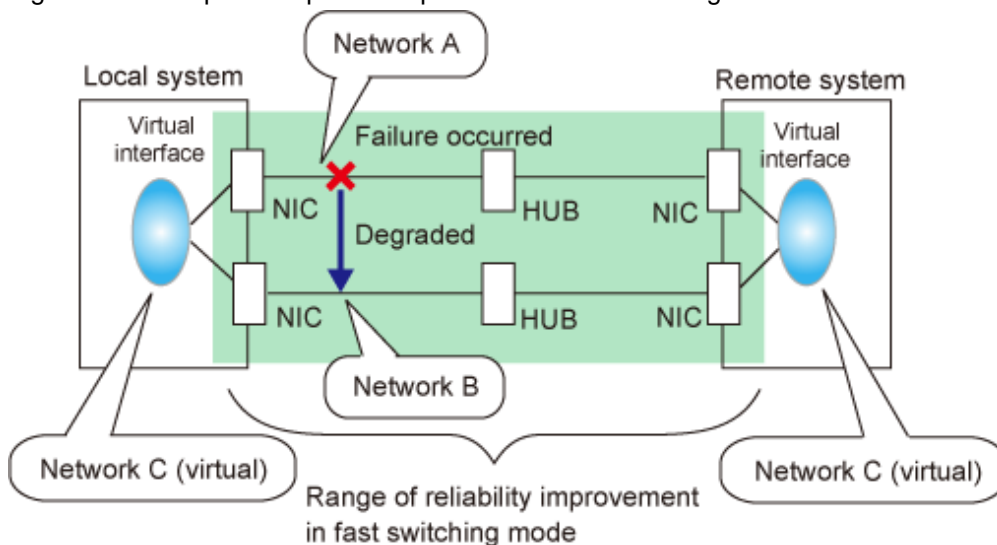
### 2.1 Overview of Functions

#### 2.1.1 Fast switching mode

In this mode, each of 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 conduct communication with the remote system, irrespective of the physical network redundant configuration, 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.

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.

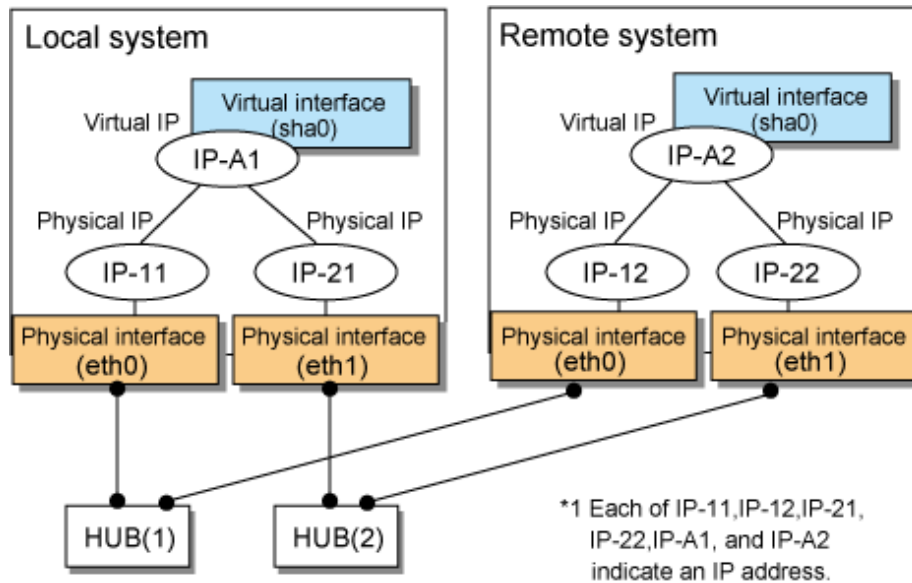
##### Recommended application areas

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 eth0 and eth1) 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

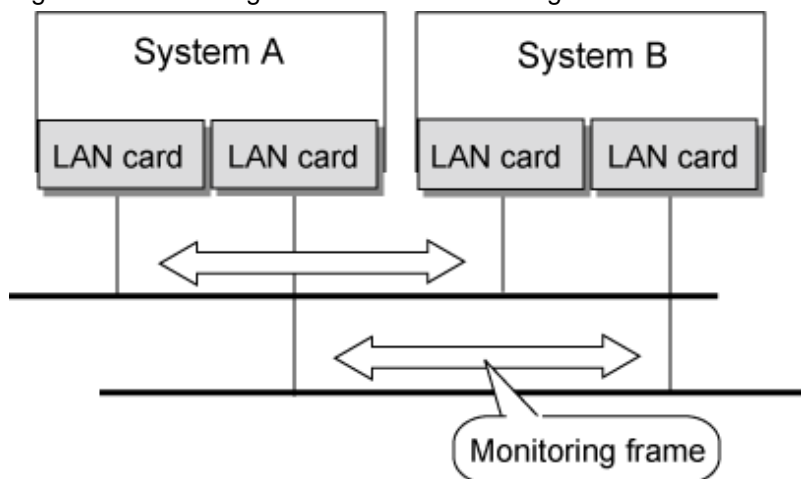
Indicates a source IP address to be allocated to the virtual interface for communication with the remote hosts. Available IP addresses are IPv4 and IPv6 address.

### 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 each NIC unit that the other device equips.

Figure 2.3 Monitoring method in Fast switching mode



The path is monitored by sending/receiving monitoring frames.

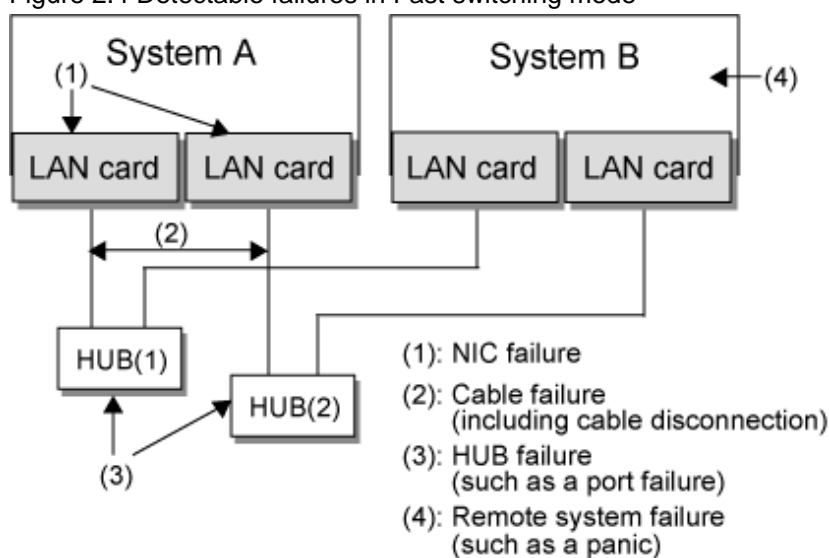
#### Switching time

If a failure occurs in a multiplexed line, it takes approximately 10 seconds to disconnect the line.

#### 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

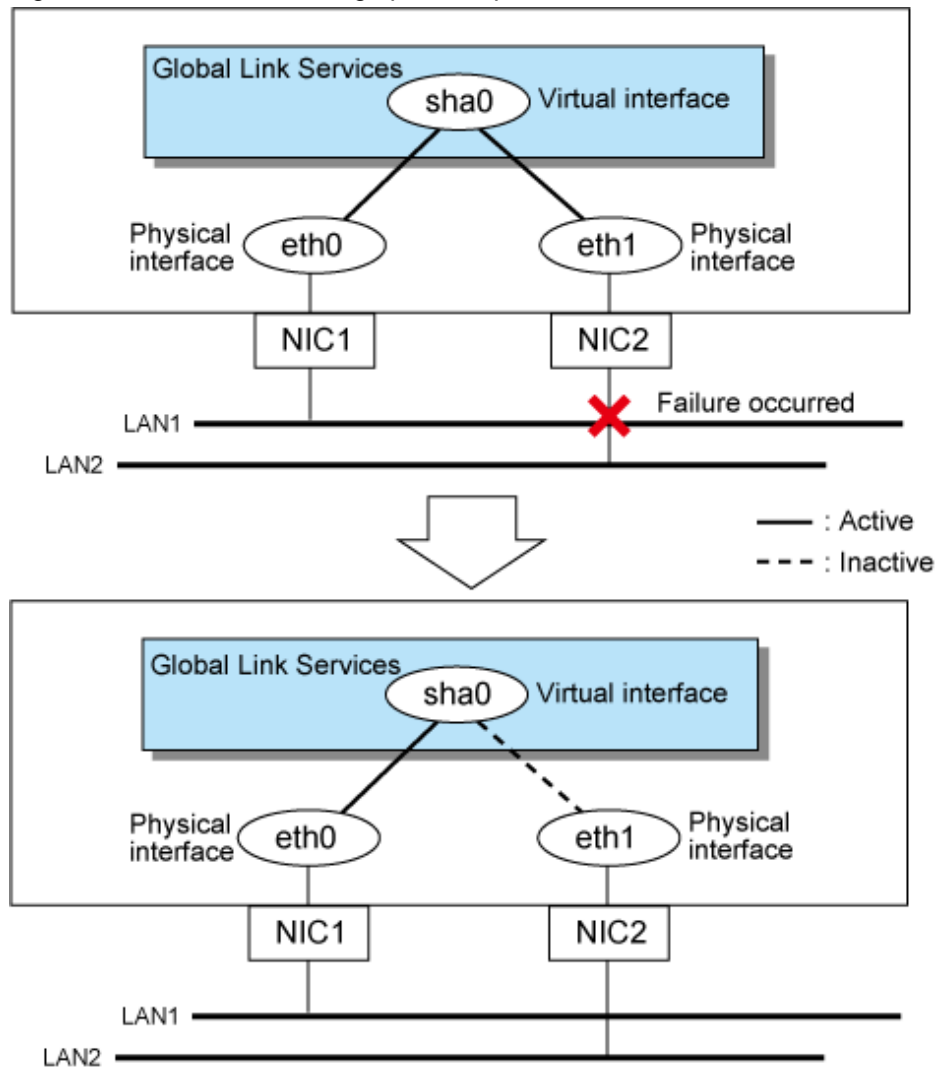
Monitoring is started automatically when the virtual interface is activated. Monitoring is automatically stopped when the virtual interface is inactivated. In cluster operation, the system allows each node to be started or stopped independently.

### 2.1.1.2 Switching function

#### Switching operation

A line whose failure is detected is automatically avoided, and the only normal line takes over the communication. 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:

- PRIMEQUEST
- PRIMERGY
- SPARC M10
- SPARC Enterprise
- PRIMEPOWER

### 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.

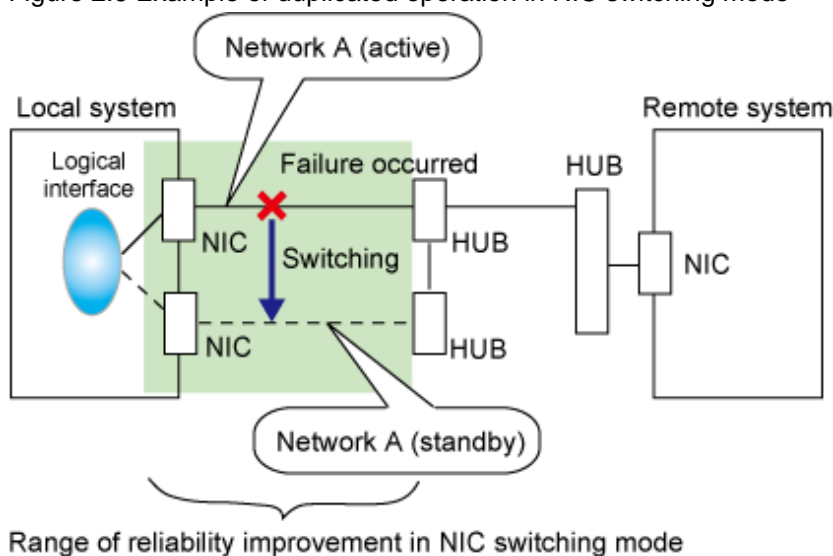
### 2.1.1.5 Notes

- 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.

## 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 eth0 and eth1, the takeover interface becomes eth0:1 and eth1:1. 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.

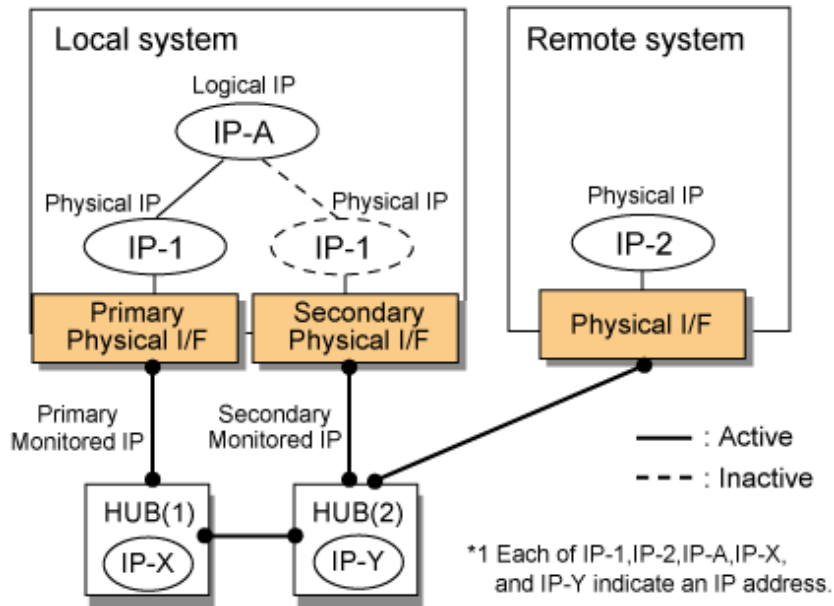
### Recommended application areas

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 addresses 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

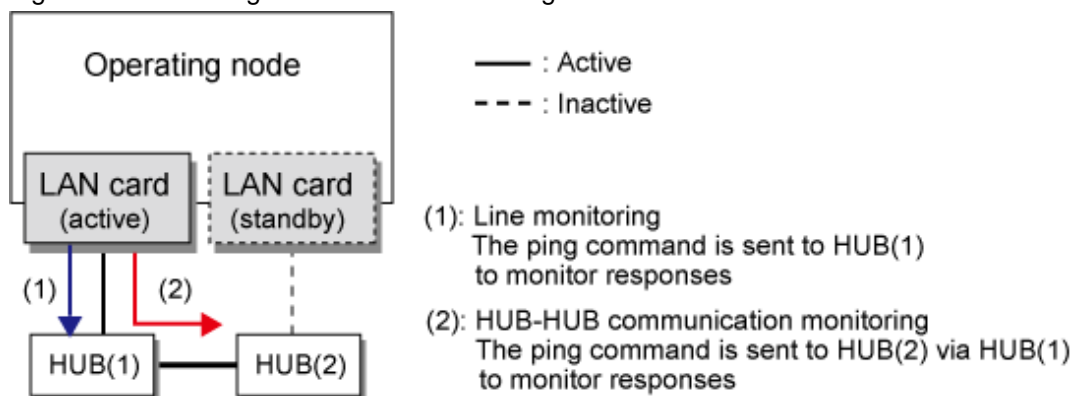
### Fault monitoring

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 (For details, see "[2.4.1 HUB monitoring function](#)").

If a failure is detected in the NIC currently operating, the system switches to the standby NIC and monitoring similarly 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

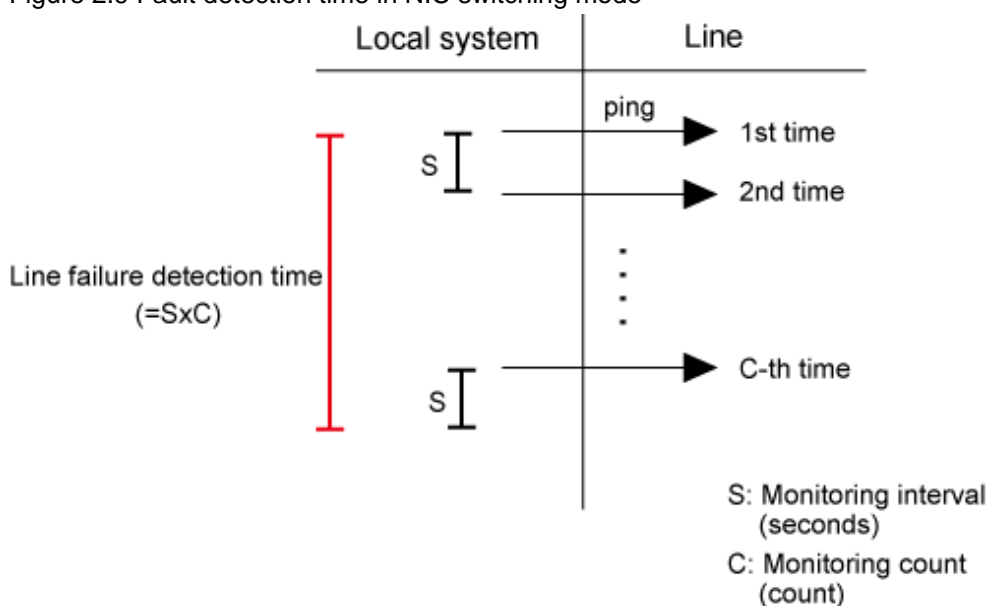


### Switching time

The approximate switching time of a line is represented by [monitoring interval (sec) x monitoring 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.

Even if the ping command failed immediately after started monitoring, it does not regard 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 a value is smaller than [monitoring interval (sec) X monitoring count], the time set for linkup is ignored and the time set by this [monitoring interval (sec) X monitoring count] is adopted.

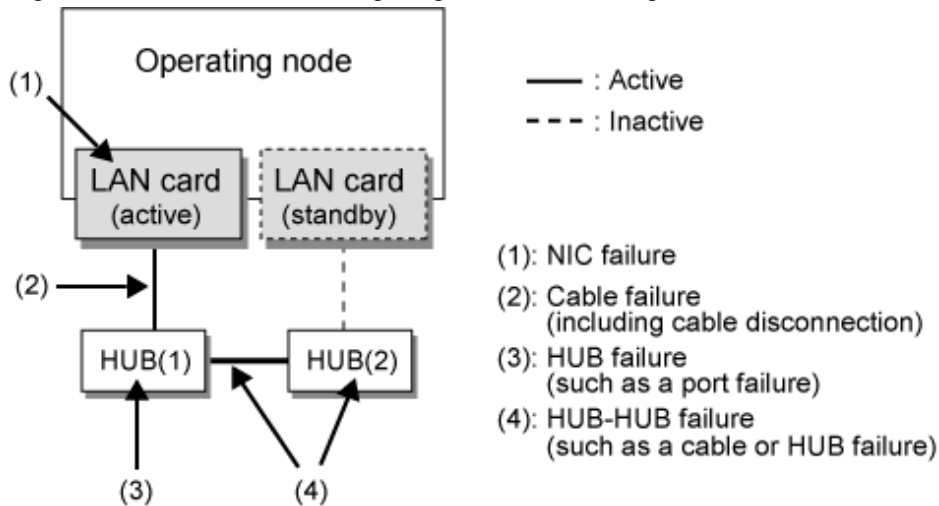
Figure 2.9 Fault detection time in NIC switching mode



### Detectable failures

The following failures can be detected:

Figure 2.10 Effective monitoring range in NIC switching mode



Because the failures (1) - (3) appear to be the same failure, a type of the failure cannot be specified. 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, the MAC address and IP addresses (physical IP and logical IP) are taken over and then an ARP request packet is broadcast, 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.

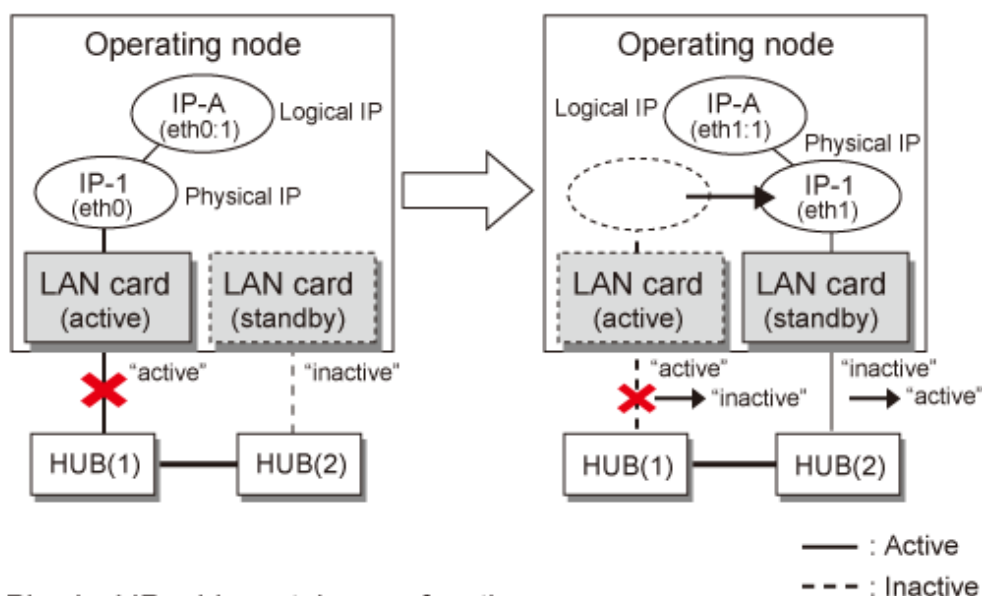
[Figure 2.11 Outline of switching operation performed when a failure occurs in NIC switching mode](#) shows an example of node internal switching.

When a failure is detected, a message to notify a failure to the system log is output. If a failure occurs when HUB-to-HUB communication monitoring is enabled, a message to notify a failure to the system log is output when a failure occurs between HUBs.

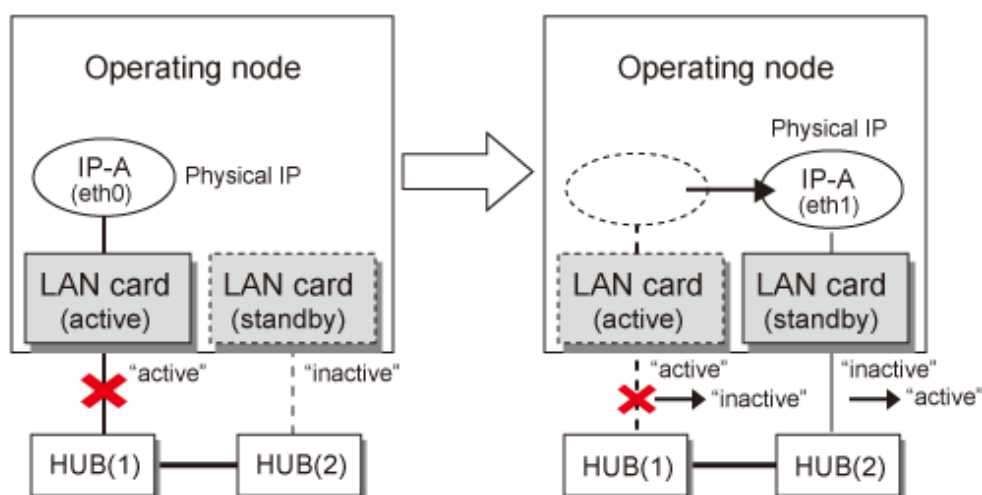


Figure 2.11 Outline of switching operation performed when a failure occurs in NIC switching mode

- 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.

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

Furthermore, if in any case entire redundant NIC encounters failure, the monitoring process terminates. In such case, you must switch the NIC via `hanetnic change` command or restart the process via `hanetpoll off/on` command after recovering the network as required.



See

For details on these commands, see the following:

- ["7.7 hanetpoll Command"](#)
- ["7.9 hanetnic 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

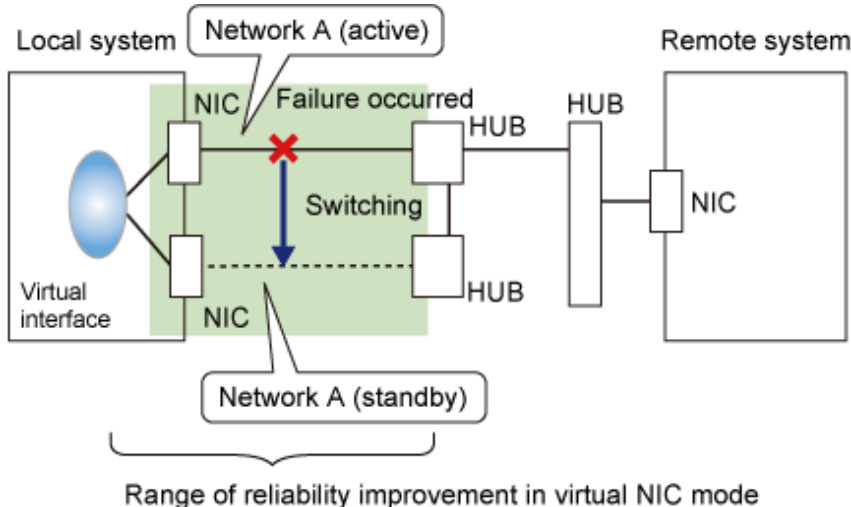
- If assigning IPv4 address to the virtual interface, IPv4 address must be assigned to all the redundant physical interfaces.
- If assigning IPv6 address to the virtual interface, IPv6 address must be assigned to all the redundant physical interfaces.
- If assigning both IPv4 and IPv6 to the virtual 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.
- If a UDP application uses a virtual IP address of GLS, you have to be cautious about the following points.
  - If, when switching NICs, data communication for the superior application fails due to any of the following symptoms:
    - Loss of the transmitted packet
    - The "sendto(2)" function for data communication returned an "ENETUNREACH" error number, or "bind(2)" returned an "EADDRNOTAVAIL" error number

Retry the operation when an error of the superior application occurs.

## 2.1.3 Virtual NIC mode

In this mode, multiple physical NICs (LAN cards) connected on the same network are connected and switching control of lines is performed based on the exclusive use. Also, a virtual interface is generated so that multiple NICs can be seen as one logical NIC. A TCP/IP application can conduct communication with the remote system, irrespective of the physical network redundant configuration, by using an IP address set in this virtual interface as its own IP address of the local system.

Figure 2.12 Example of duplicated operation in Virtual NIC 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.

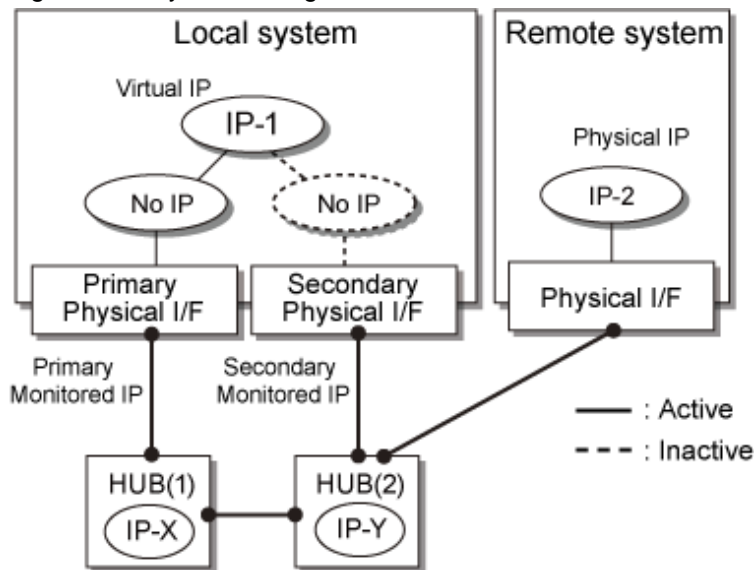
## Recommended application areas

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 2.13 System configuration in Virtual NIC 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. An IP address is not set.

### Secondary physical interface

Indicates the physical interface to be used after switching when a line failure is detected in the Primary physical interface. An IP address is not set.

### Virtual IP

Indicates a local IP address for communication with the remote device. In Virtual NIC mode, it is possible to use both IPv4 and IPv6 addresses as an address form. This IP is set for a virtual interface.

### Primary monitored IP

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

By default, the MAC address of the virtual interface uses the MAC address of the primary physical interface. While the virtual interface is being activated, the MAC addresses of the primary physical interface, secondary physical interface, and virtual interface become the same. For the virtual interface, any MAC address can be set. For details, see "3.3.3 Virtual NIC mode."

### 2.1.3.1 Fault monitoring function

#### Fault monitoring

In Virtual NIC mode, link statuses of LAN cards and network communication statuses are both monitored.

##### - Link status monitoring function

This function monitors the Ethernet link statuses of all duplicated LAN cards. When a link down occurred with a LAN card on the active side, a failover to a LAN card on the standby side is performed.

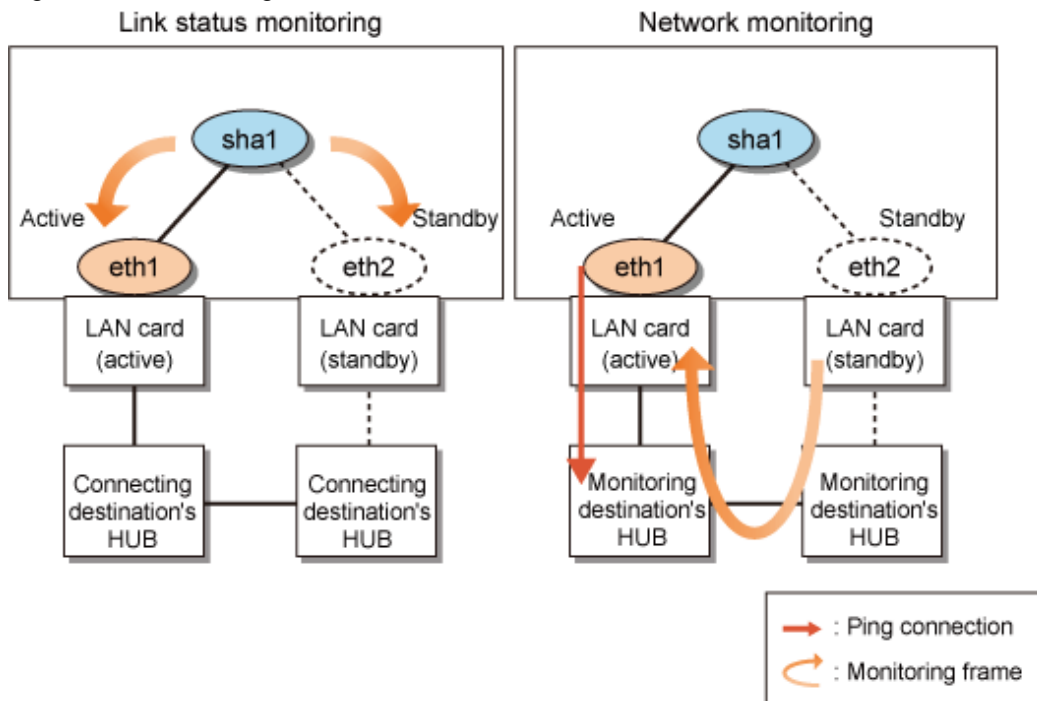
##### - Network monitoring function

This function uses two methods listed below to monitor the network status to which a virtual interface is connected.

Type	Monitoring method
HUB monitoring	A ping is sent periodically from active NICs to the switch/HUB to check whether the switch/HUB is operating normally.
Standby patrol	A monitoring frame (proprietary Ethernet frame) is sent periodically from standby NICs to active NICs. This function checks that there is no error in active NICs and standby NICs, as well as in network devices on the transfer path between NICs.

When a failure without link down has occurred in a network device and an error is detected by both monitoring methods, a failover to a standby NIC is performed. Likewise, failbacks can be effected automatically after detecting that the network has recovered.

Figure 2.14 Monitoring method in Virtual NIC mode



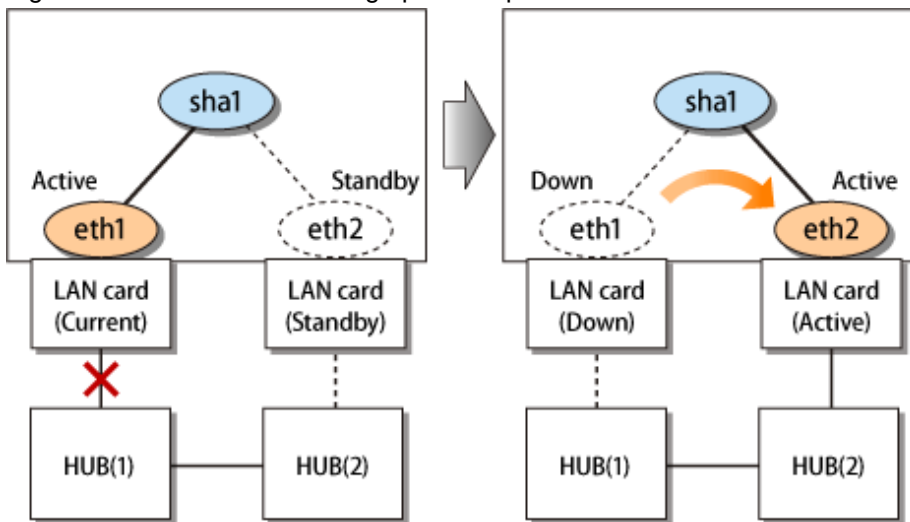
### 2.1.3.2 Switching function

#### 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, the MAC address and IP addresses are taken over and then broadcast packet, in which the MAC address of the local node is set as the source, is sent. This operation notifies switch of a transfer path to HUB.

In addition, when a failure is detected, a message is output to notify an error to the system log.

Figure 2.15 Outline of switching operation performed when a failure occurs in Virtual NIC mode



#### 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.

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

### 2.1.3.3 Connectable remote host

Any system can be connected.

### 2.1.3.4 Available application

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

- Application using the TCP or UDP.

## 2.1.4 GS 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 2.16 Example of duplicated operation in GS linkage mode

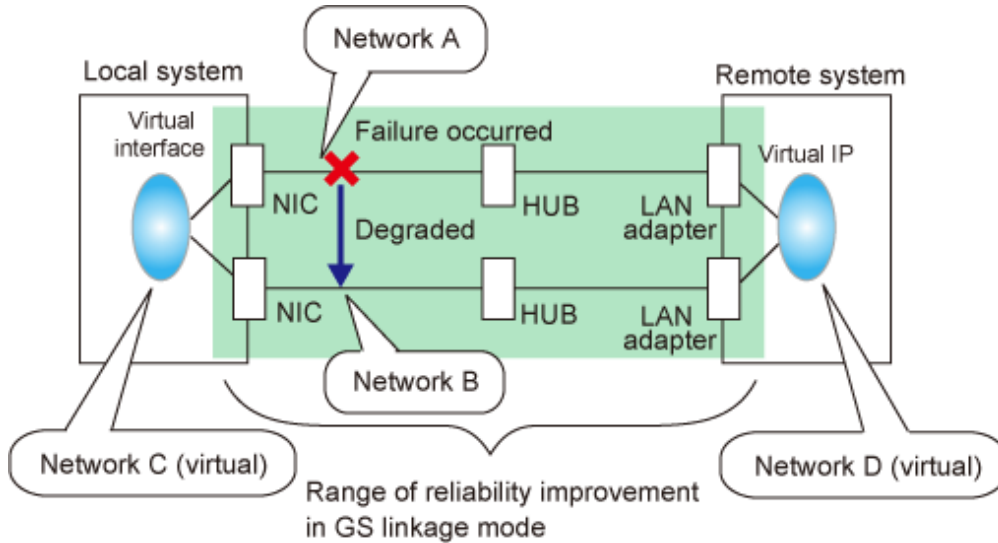
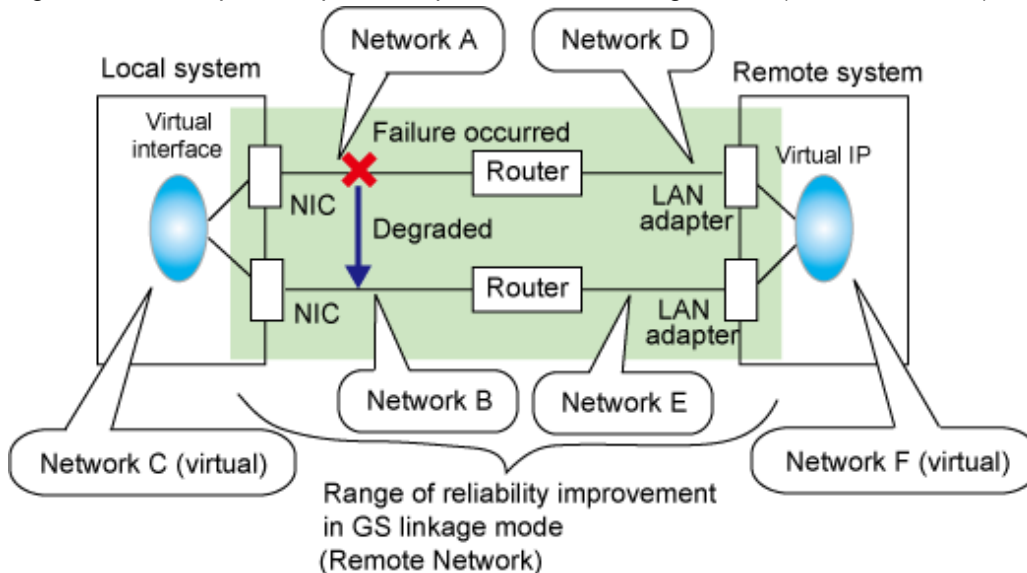


Figure 2.17 Example of duplicated operation in GS linkage mode (Remote network)



#### Connection type

If the GS 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.

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

#### System configuration

[Figure 2.18 System configuration in GS linkage mode](#) and [Figure 2.19 System configuration in GS linkage mode](#) show a system configuration of GS linkage mode.

Figure 2.18 System configuration in GS linkage mode

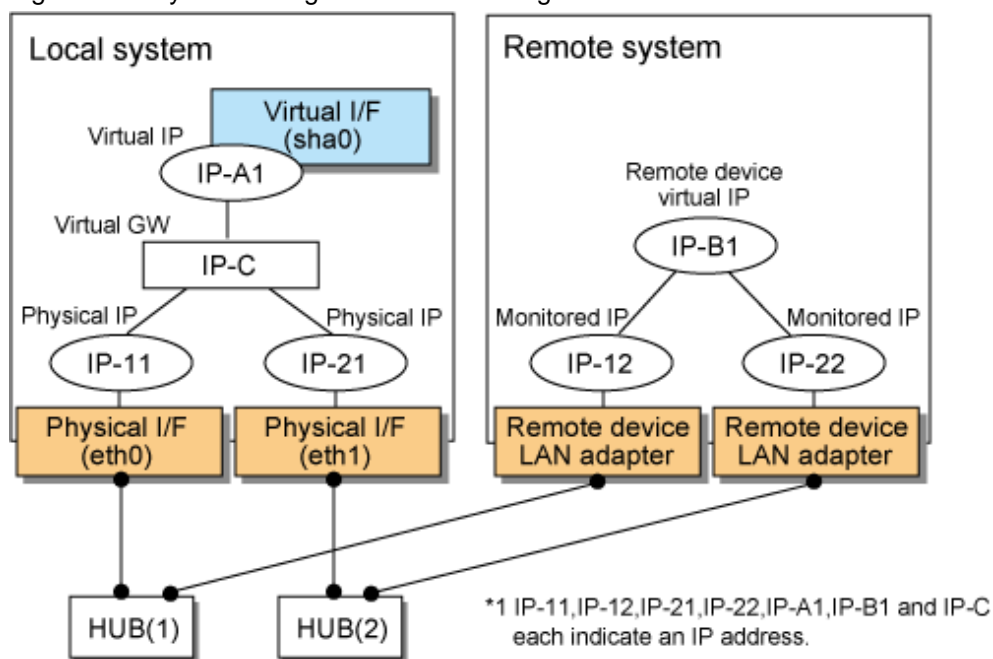
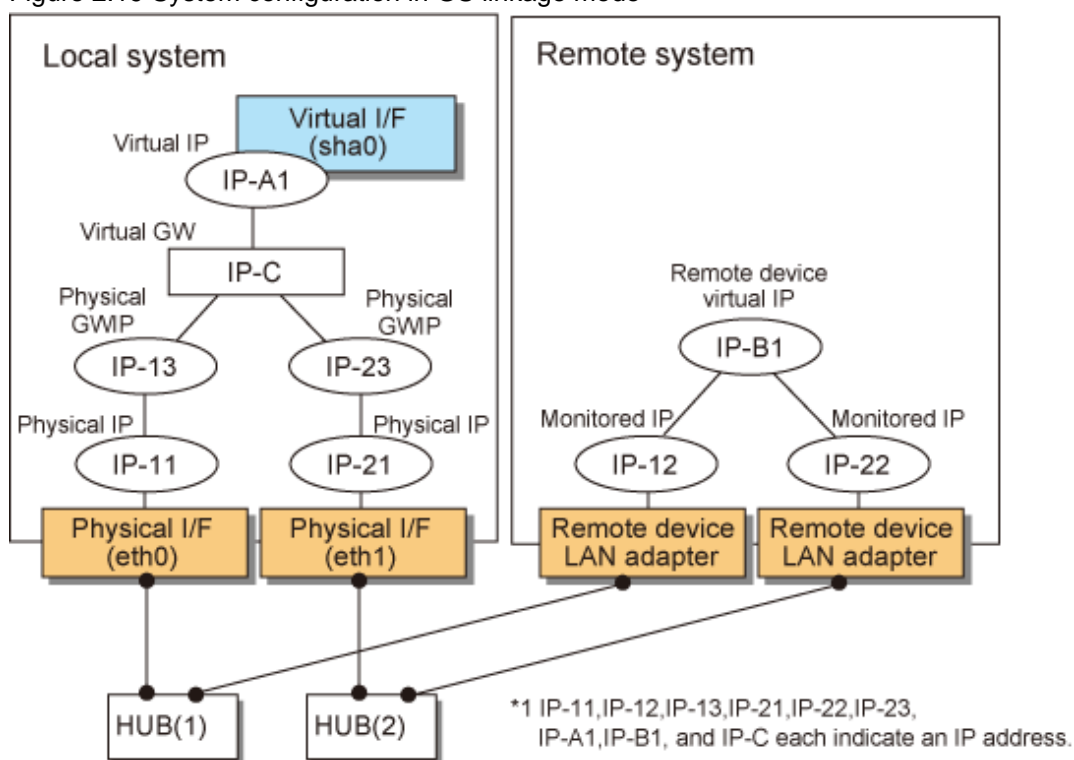


Figure 2.19 System configuration in GS linkage mode



The following explains each component and its meaning:

#### Physical interface

Indicates a physical interface (such as eth0 and eth1) 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. IPv6 addresses cannot be used. Note that the IP addresses to be attached to each physical interface must be different network addresses.

### 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. IPv6 addresses cannot be used.

### Virtual GW (Virtual Gateway)

Indicates a virtual gateway to be used for GS linkage mode. Only use the IPv4 address formats. IPv6 addresses cannot be used.

### Physical GW IP (Physical Gateway)

Indicates a cluster environment that connects to GS via a router, representing the physical IP address that will be the gateway for the GLS takeover virtual IP address. In a cluster configuration, this IP address is taken over along with the virtual IP address (takeover virtual IP address) between nodes, which means that you can statically specify the route for the GLS virtual IP address on the router even if the virtual IP address is taken over. In a cluster configuration, set the static route on the router so that the physical GWIP can act as the gateway for the GLS virtual IP address. In a single configuration, set the physical IP address as a gateway, rather than the physical GWIP, so you do not need to set the physical GWIP in a single configuration. The specifiable address format is IPv4. IPv6 addresses cannot be specified.

### 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. IPv6 addresses cannot be used.

### Remote device virtual IP

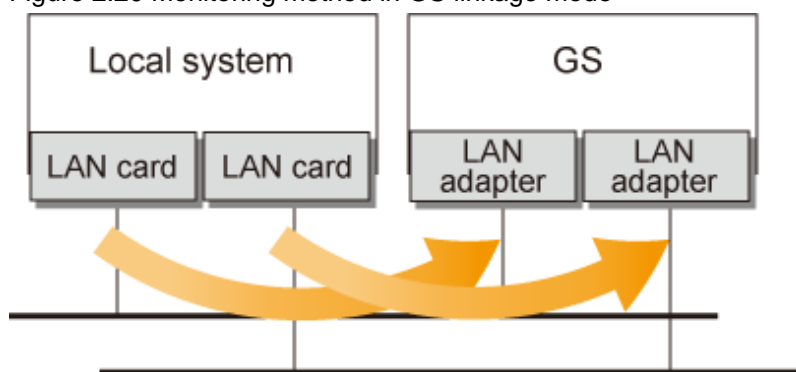
Indicates a virtual IP of the remote device with which communication should be carried out. IPv4 address can be used for a physical interface. IPv6 addresses cannot be used.

## 2.1.4.1 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 (For details, see "[2.6.1 Communication target monitoring](#)").

Figure 2.20 Monitoring method in GS linkage mode



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



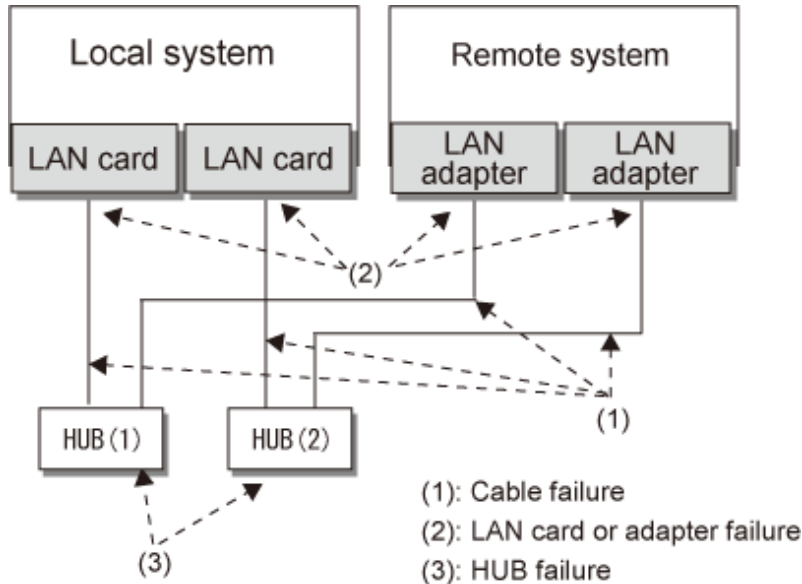
### Switching time

The switching time of a line is indicated by [monitoring interval (sec) X monitoring 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 2.21 Detectable failures in GS linkage mode



Because the failures (1) - (3) 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. Monitoring is automatically stopped when the virtual interface is inactivated. For cluster configuration, monitoring is started automatically when a GLS resource status changes to Online or Standby. Monitoring is stopped when all GLS resources change to Offline.

## 2.1.4.2 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.

## 2.1.4.3 Connectable remote host

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

- Global Server (GS)
- PRIMEQUEST
- PRIMERGY

## 2.1.4.4 Available applications

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.

### 2.1.4.5 Notes

- When using a physical interface, it is necessary to assign the IPv4 address.
- When using GS linkage mode (GS communication capability), the system must be configured as multi-homed host instead of a router.
- This mode cannot be applied for communication between Linux server and Solaris server.
- If GS is in the hot-standby configuration, the node that received the down notification by the TNOTIFY command from GS is recognized as the communication target.
- If GS is in the hot-standby configuration, GS must support the lookup of the location of virtual IP addresses.
- When you connect between GLS and GS via router, set the server with GS linkage mode to send the path for GS's virtual IP using RIPv1.

## 2.2 Interface structure

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	Virtual NIC mode	GS linkage mode
Configuring multiple virtual interfaces	A	A	A	A
Sharing physical interface	A	A	O	A
Configuring multiple logical virtual interfaces	A	O	A	A
Configuring single physical interface	A	A	A	A
Multiplex transfer route by Tagged VLAN interface	A	A	A	X

[Meaning of the symbols] A: Allowed, O: Replaced by other functions, X: Not allowed

### 2.2.1 Configuring multiple virtual interfaces

Multiple virtual interfaces can be defined in a single system. With this capability, the number of available transfer routes within a single system can be increased, which will be useful for a system requiring multiple networks, such as application gateway. With the multiple virtual interfaces, high network reliability can be ensured.

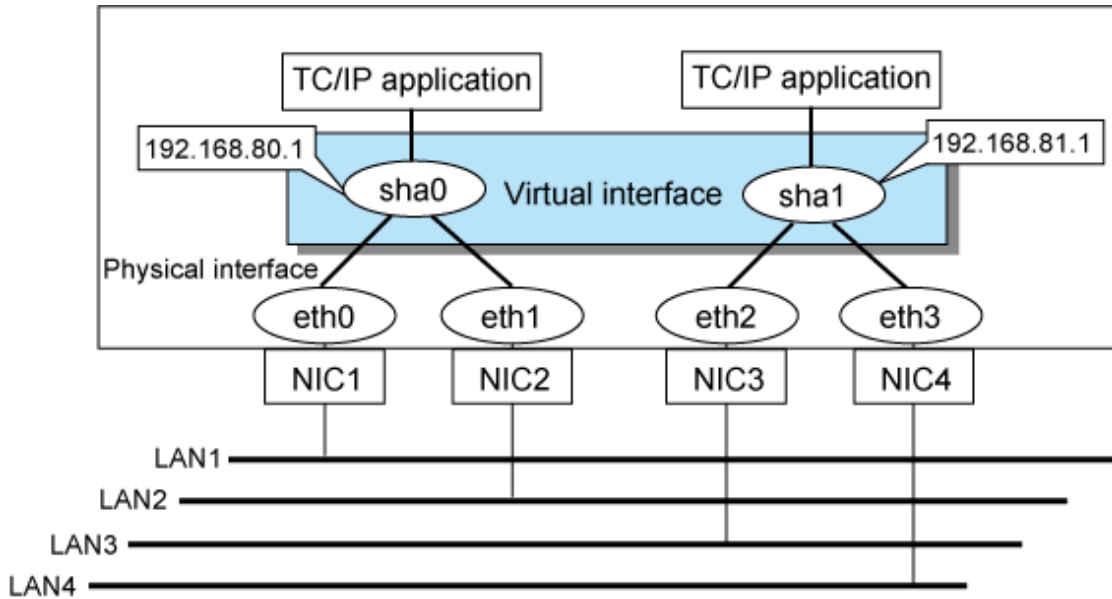


#### Note

The virtual IP address of different subnet must be assigned to the multiple virtual interfaces.

Figure 2.22 Two virtual interfaces being defined below shows an example of defining 2 virtual interfaces. A virtual IP address of different subnet must be assigned in sha0 and sha1.

Figure 2.22 Two virtual interfaces being defined



## 2.2.2 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 resources in Fast switching mode or GS linkage mode.
- Configuring multiple IP addresses on a single NIC in NIC switching mode and use different IP address for each application.

### 2.2.2.1 Using Fast switching mode

One portion or entire physical interfaces can be shared by the virtual interfaces which institute Fast switching mode. Though, it is not possible to share the physical interface and virtual interface of NIC switching mode and GS linkage mode.

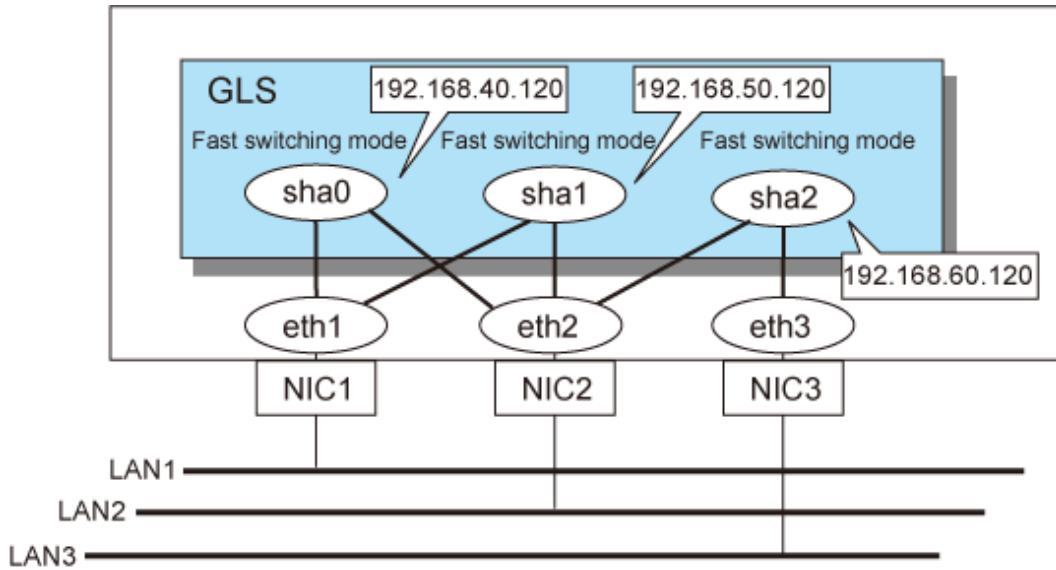


#### Note

- The virtual IP address of different subnet must be assigned to the multiple virtual interfaces.
- In Fast switching mode, you cannot share NICs between virtual interfaces for which IPv6 addresses are set. You can share NICs only between virtual interfaces for which IPv4 addresses are set, or between virtual interfaces for which IPv4 and IPv6 addresses are set.

Figure 2.23 Example of sharing physical interface (1) shows an example of three virtual interfaces, sha0, sha1, and sha2 (All in Fast switching mode) sharing three physical interfaces eth1, eth2, and eth3. Note that IP addresses with different subnets should be set for sha0, sha1, and sha2.

Figure 2.23 Example of sharing physical interface (1)



### 2.2.2.2 Using NIC switching mode

Within several virtual interfaces of NIC switching mode (logical IP takeover), if all the name of the physical interfaces and the value 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 linkage mode.

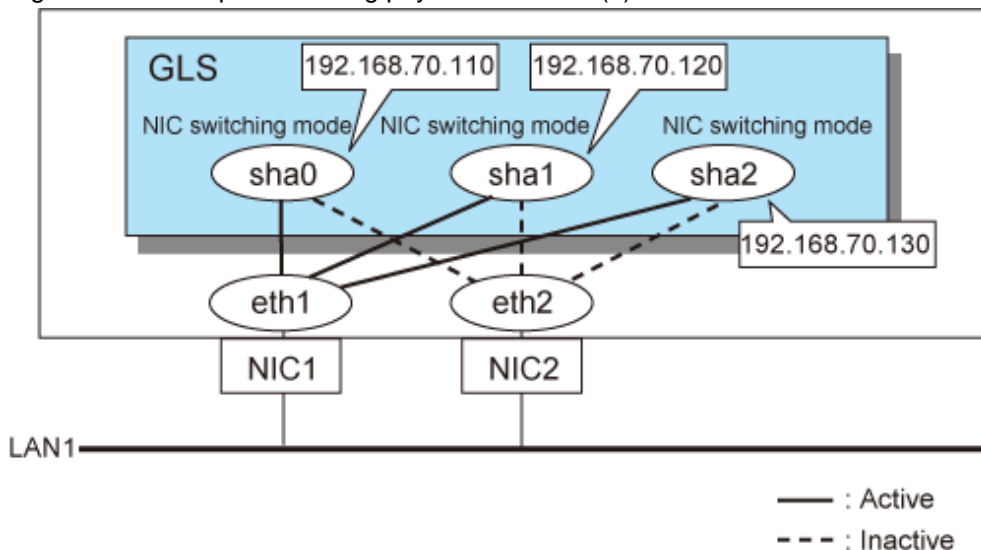


#### Note

The virtual IP address of same subnet must be assigned to the multiple virtual interfaces.

Figure 2.24 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 eth1, and eth2. Note that IP addresses with the same subnet should be set for sha0, sha1 and sha2.

Figure 2.24 Example of sharing physical interface (2)



### 2.2.2.3 Using GS linkage mode

Within several virtual interfaces of GS linkage mode, it is possible to share the physical interface. Sharing a portion of physical interface is not allowed. Nevertheless, sharing physical interface with the virtual interface is not possible for Fast switching mode and NIC switching mode.

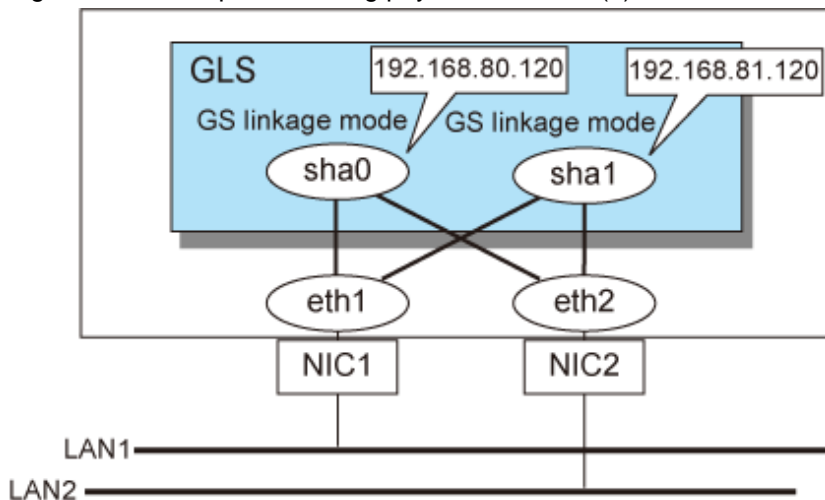


#### Note

The virtual IP address of different subnet must be assigned to the multiple virtual interfaces.

Figure 2.25 Example of sharing physical interface (3) shows an example of two virtual interfaces, sha0, sha1, and sha2 (All in GS linkage mode) sharing three physical interfaces eth1, and eth2. Note that IP addresses with different subnets should be set for sha0, sha1, and sha2.

Figure 2.25 Example of sharing physical interface (3)



### 2.2.2.4 Notices

In Fast switching mode, NIC sharing is not possible within the virtual interface that institutes IPv6 address. NIC sharing is possible between the virtual interfaces that are both configured with IPv4 address, or between the virtual interfaces that are configured with IPv6 address and IPv4 address.

## 2.2.3 Configuring multiple logical virtual interfaces

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

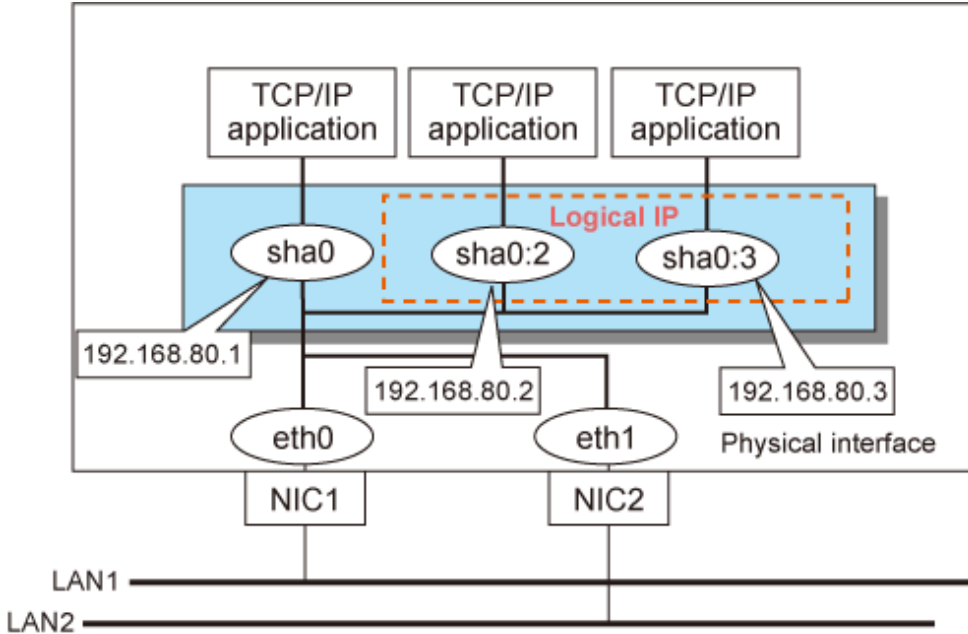


#### Note

The virtual IP address of same subnet must be assigned to the multiple virtual interfaces.

Figure 2.26 Logical virtual interfaces being defined shows an example of defining two IP addresses (logical virtual interface) on a single virtual interface sha0. Configure the IP address of the same subnet to sha0, sha0:2, sha0:3.

Figure 2.26 Logical virtual interfaces being defined

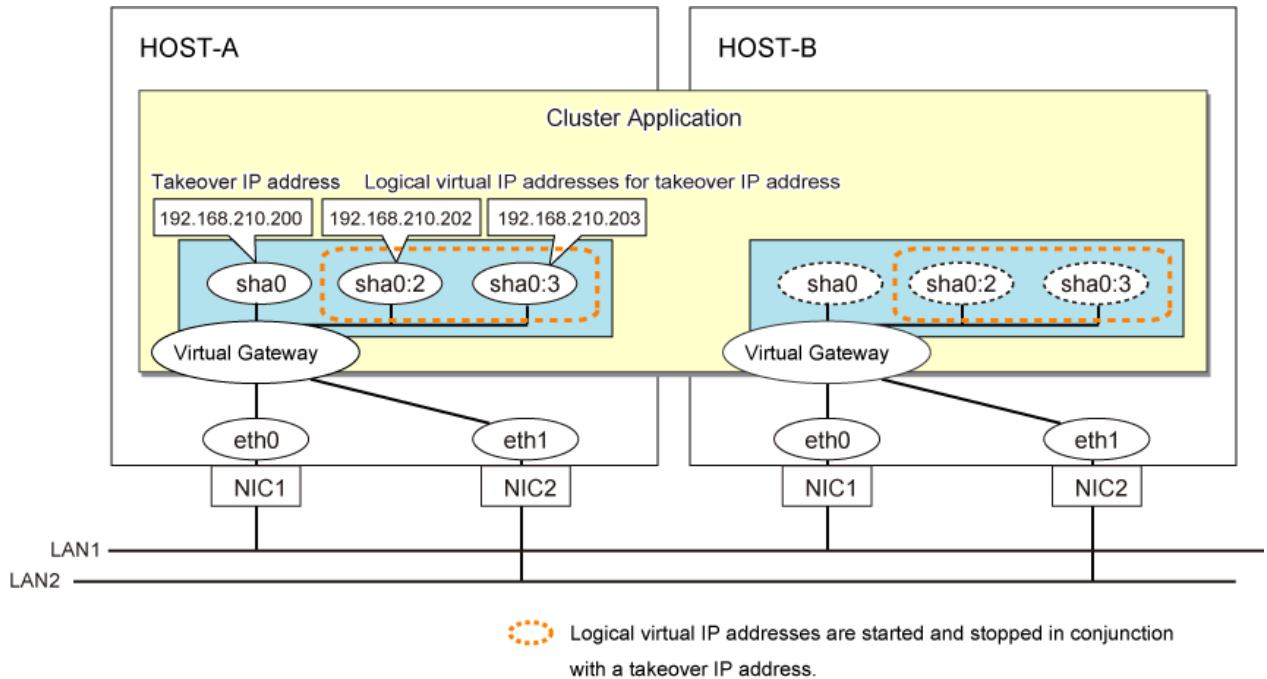


The total number of interfaces can be created as a logical virtual interface is 63 (from 2 to 64). The logical virtual interfaces greater than 65 will be used as takeover virtual interface upon Cluster configuration.

#### GS linkage mode in a cluster configuration

For GS linkage mode in a cluster configuration, you can take over a virtual IP address which belongs to the same network between clusters by using the logical virtual interface.

Figure 2.27 Logical virtual interfaces being defined (GS linkage mode in a cluster configuration)



#### Note

- This function is only available for Fast switching mode, Virtual NIC mode, and GS linkage mode.

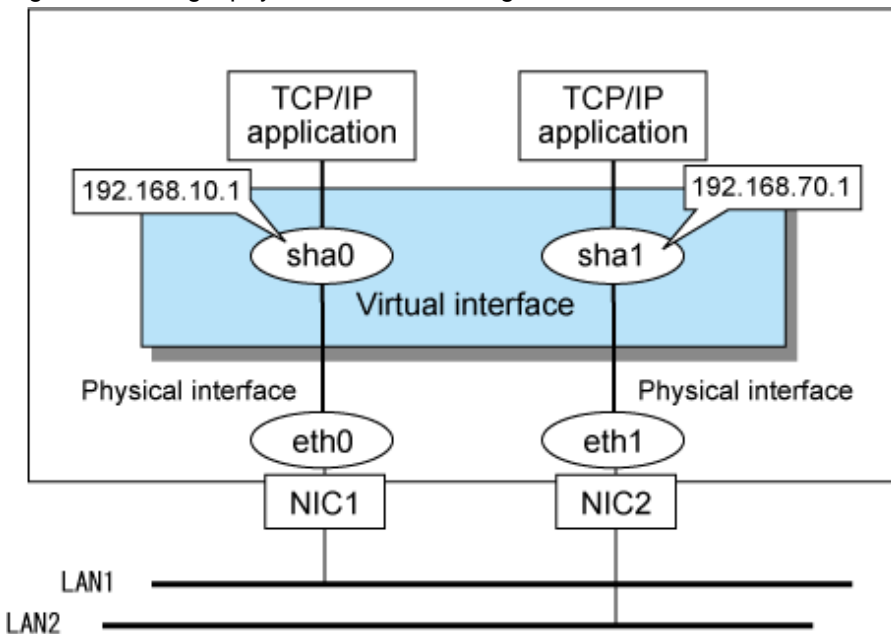
- For NIC switching mode, if using physical interface sharing function, it can process (a process of allocating multiple IP addresses to one physical interface) equally as this function.
- For Virtual NIC mode, create the definition file of the operating system (/etc/sysconfig/network-scripts/ifcfg-sha0:2) for setting, instead of using the GLS command. Do not set "DEVICETYPE=sha" for the definition file.

## 2.2.4 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.

Figure 2.28 Single physical interface configuration shows an example of single physical interface configuration.

Figure 2.28 Single physical interface configuration



### Note

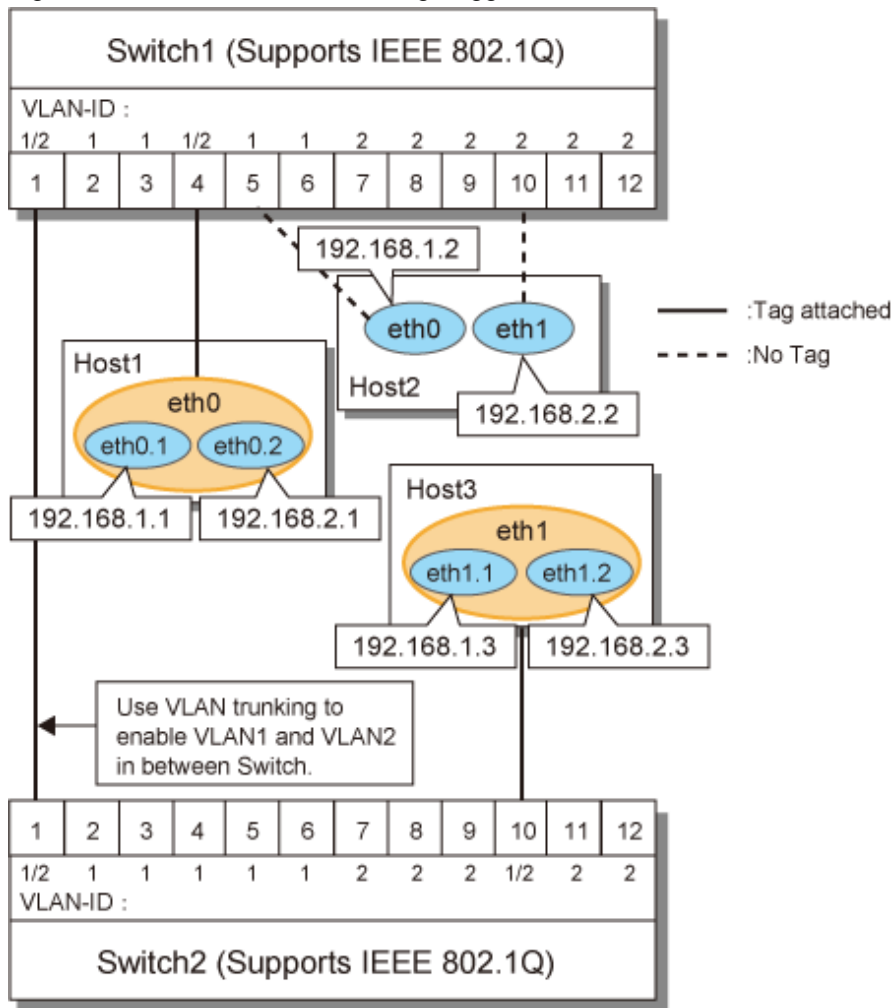
- This feature is capable for all switching modes.
- The selection criteria of a mode where a single physical interface is used on GLS relies on the mode where redundant line is used. Refer to the fault monitoring function requirements section on "[1.1.1 Functional comparison](#)" before selecting a single physical interface for either mode.

## 2.2.5 Configuring 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 switches/hubs that satisfy "IEEE 802.1Q" 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 2.29 Network structure using Tagged VLAN



In [Figure 2.29 Network structure using Tagged VLAN](#), VLAN1(VLAN-ID:1) and VLAN2(VLAN-ID:2) are created on both Switch 1 and Switch 2, and port 1 on both switches is used for VLAN Trunking.

A physical interface "eth0" on Host 1 has two VLAN interfaces "eth0.1" and "eth0.2", and is connected to port 4 on Switch 1 that belongs to both VLAN1 and VLAN2. Host 1 uses "eth0.1" and "eth0.2" to transmit tagged packets.

Similarly, a physical interface "eth1" on Host 3 has two VLAN interfaces "eth1.1" and "eth1.2", 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 packet communication.

Host 2 achieves data communications on both VLAN1 and VLAN2 by connecting a physical interface "eth0" to port 5 that belongs to VLAN1, and another physical interface "eth1" to port 10 that belongs to VLAN2.



#### Note

Ensure a switch/hub is configured to handle Tagged VLAN (IEEE 802.1Q).

### 2.2.5.1 Redundant Line Control function using Tagged VLAN interface

In Redundant Line Control Function, transfer paths can be multiplexed with tagged VLAN interfaces.



Figure 2.30 Using Tagged VLAN Interface architecture in NIC switching mode

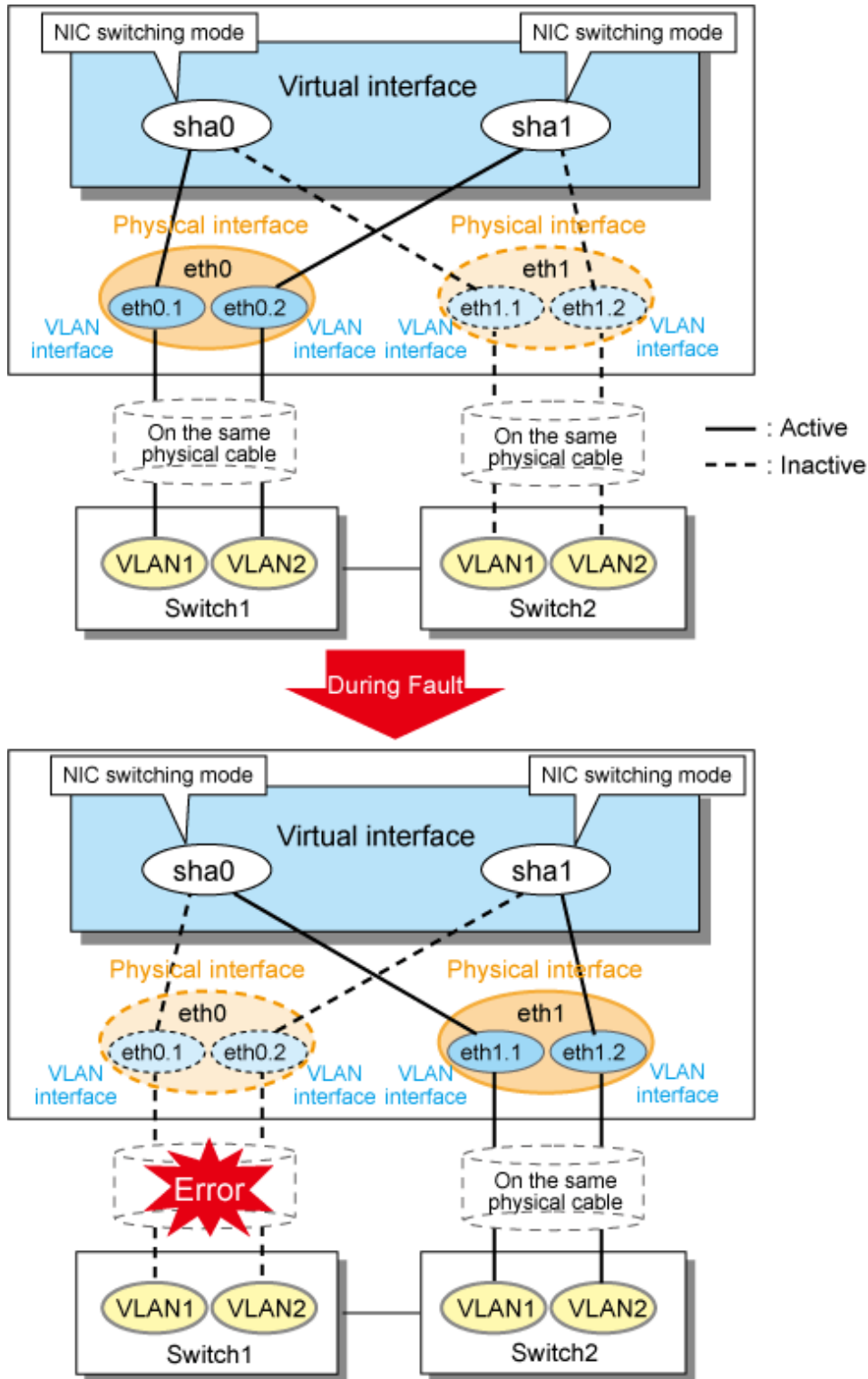
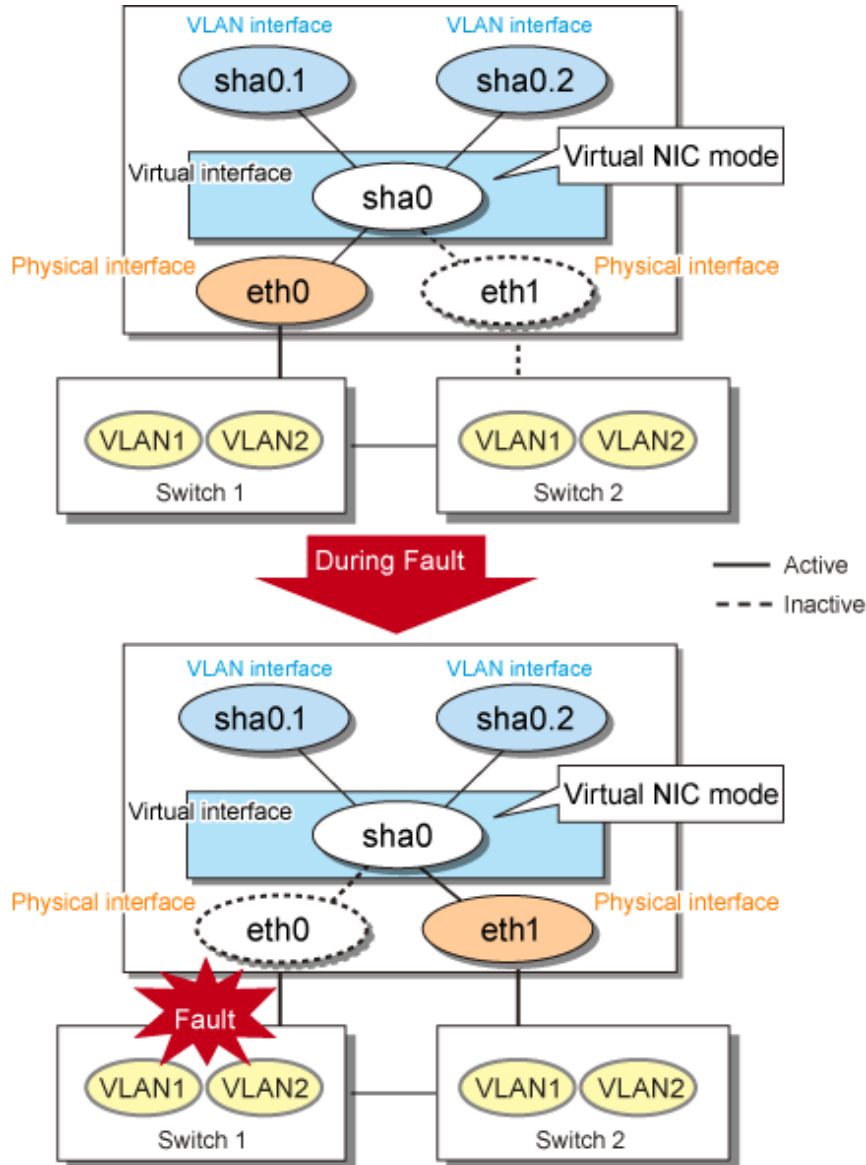


Figure 2.31 Using Tagged VLAN Interface architecture in Virtual NIC mode

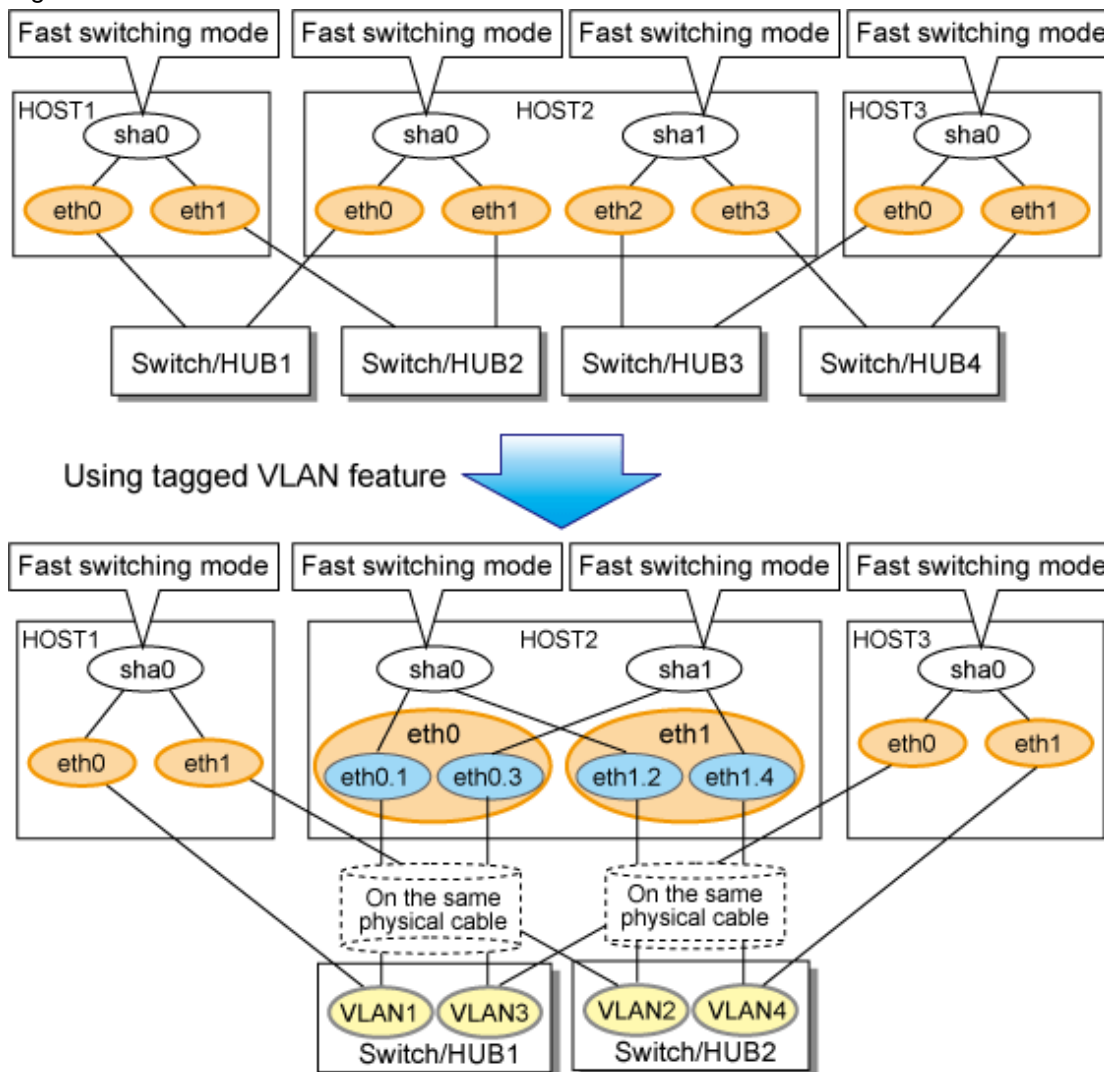


#### Point

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 2.32 When Switch/HUB and NIC come short



See

For details on using Tagged VLAN for other modes, refer to "3.6.5 Transfer route multiplexing with Tagged VLAN interface".

## 2.3 Monitoring function of Fast switching mode

In Fast switching mode, monitoring is performed using the following monitoring function.

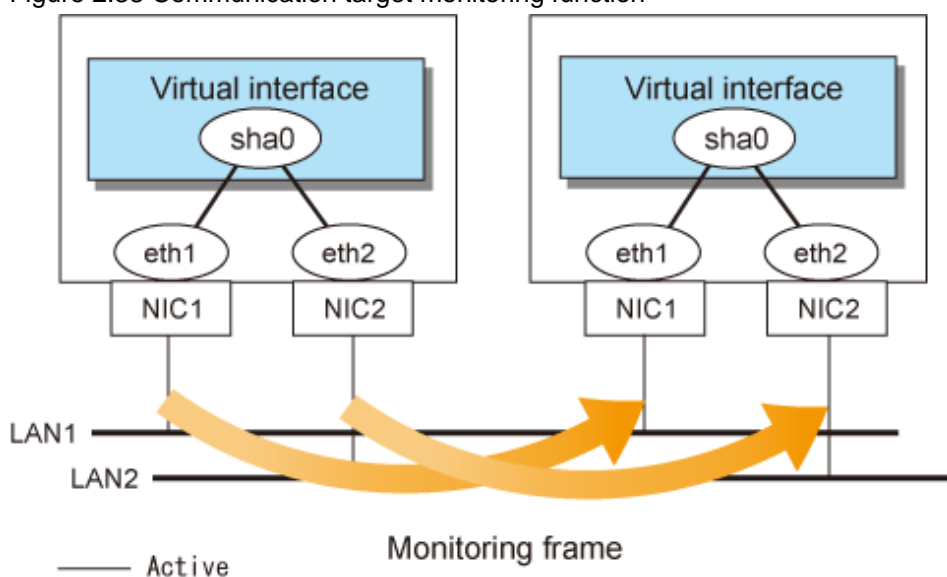
Table 2.2 Available option functions in each mode

Monitoring function	Setting	Function
Communication target monitoring	Not required	Performs monitoring by sending monitoring frames to communication targets. If an error is detected, the communication is switched to a normal NIC.

### 2.3.1 Communication target monitoring

In Fast switching mode, the network is monitored by sending and receiving monitoring frames periodically between the monitor and communication targets.

Figure 2.33 Communication target monitoring function



## 2.4 Monitoring function of NIC switching mode

In NIC switching mode, the following monitoring functions can be set.

Table 2.3 Available option functions in each mode

Monitoring function	Setting	Function
HUB monitoring function	Required	Monitors the network by issuing a ping command for HUBs. If an error is detected, a message appears indicating the error, and the communication is switched to a normal NIC.
HUB to HUB monitoring function	Optional	Enables HUB to HUB monitoring by using a ping command. If an error is detected, a message appears indicating the error. When the HUB to HUB monitoring recovers, a message appears indicating a successful recovery.
Standby patrol function	Optional	Monitors standby/active NICs by using monitoring frames. If an error is detected, a message appears indicating the error. When it is recovered, a message appears indicating a successful recovery.

### 2.4.1 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. Up to two HUBs can be registered per virtual interface. This function is available exclusively for NIC switching mode.

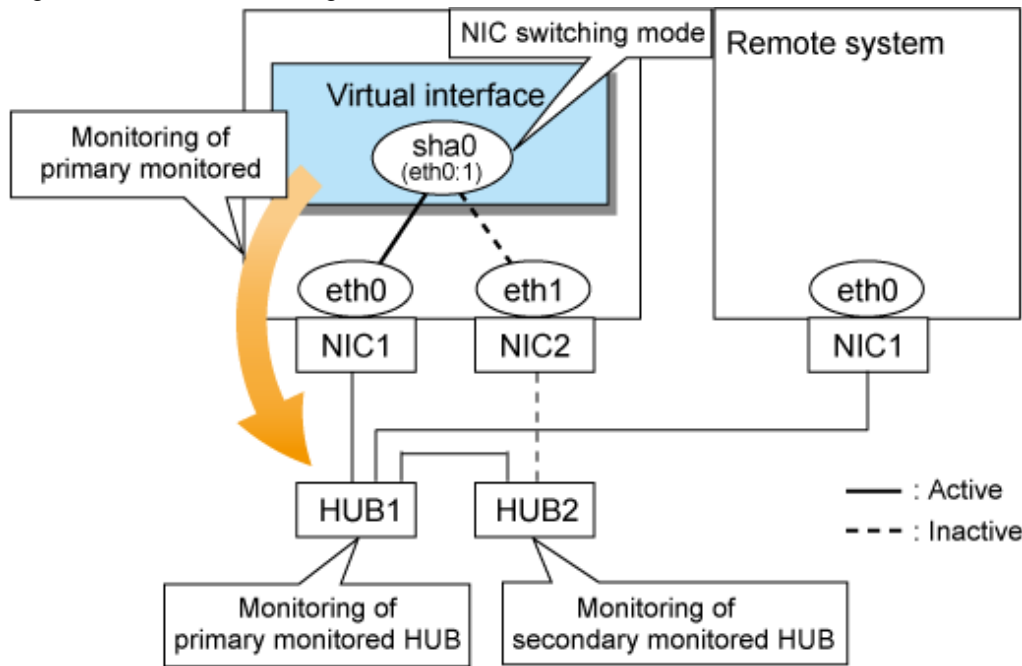
This function can also monitor a transfer path between two HUBs (this is called HUB-to-HUB monitoring function). HUB-to-HUB monitoring function detects a failure between two HUBs. This function can thus prevent a communication error from occurring due to NIC switching when a HUB-to-HUB failure occurs.

#### Information

If the standby patrol function is used, the HUB-to-HUB monitoring is not required because the standby patrol function is comprised with HUB-to-HUB monitoring function. (See section "2.4.2 Standby patrol function")

Figure 2.34 HUB monitoring function shows an outline of the HUB monitoring function

Figure 2.34 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.

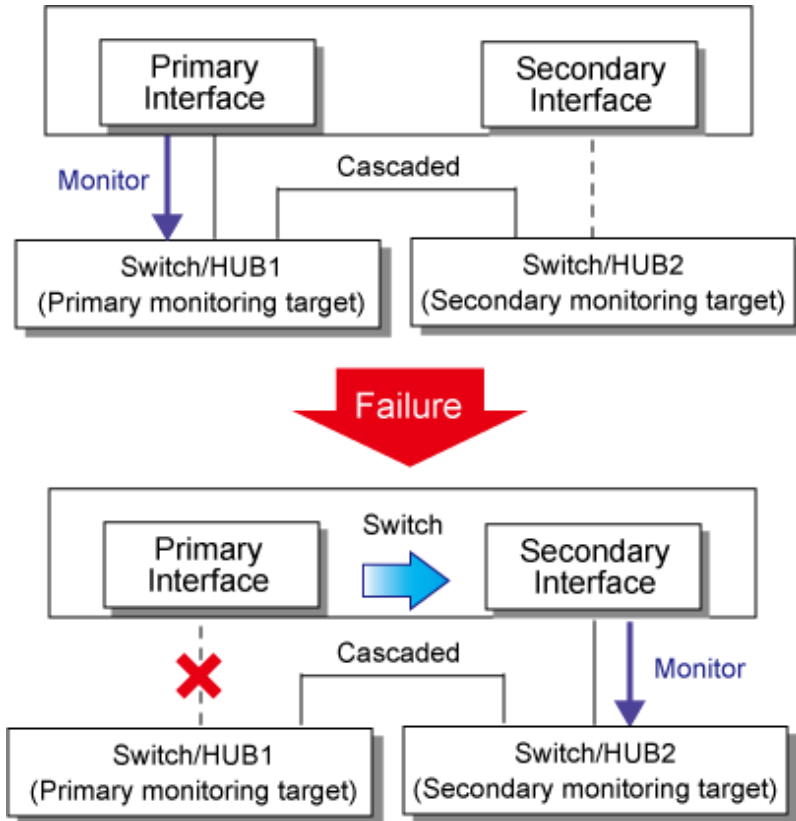
#### Note

- Refer to "7.7 hanetpoll Command" for configuration of HUB-to-HUB monitoring feature.
- It is not recommended to operate with a single HUB. It is possible to have only one configuration for a remote end when using a single HUB. However, it defeats the purpose of multiplexing transfer paths if the HUB breaks.

### 2.4.1.1 Not using HUB-to-HUB monitoring feature

If the operation starts without HUB-to-HUB monitoring function, the primary HUB (Switch/HUB1 in the [Figure 2.35 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 (Switch/HUB2 in the [Figure 2.35 HUB-to-HUB monitoring disabled](#)) is monitored using the ping command.

Figure 2.35 HUB-to-HUB monitoring disabled



#### 2.4.1.2 Using HUB-to-HUB monitoring feature

If the operation starts using the HUB-to-HUB monitoring function, the secondary HUB (Switch/HUB2 in the [Figure 2.36 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 2.36 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.

Also, when a failure is detected in the primary HUB after switching to the secondary interface with transfer path failure, a message (No. 873) will be output.

Figure 2.36 HUB-to-HUB monitoring enabled (failure on the secondary monitoring)

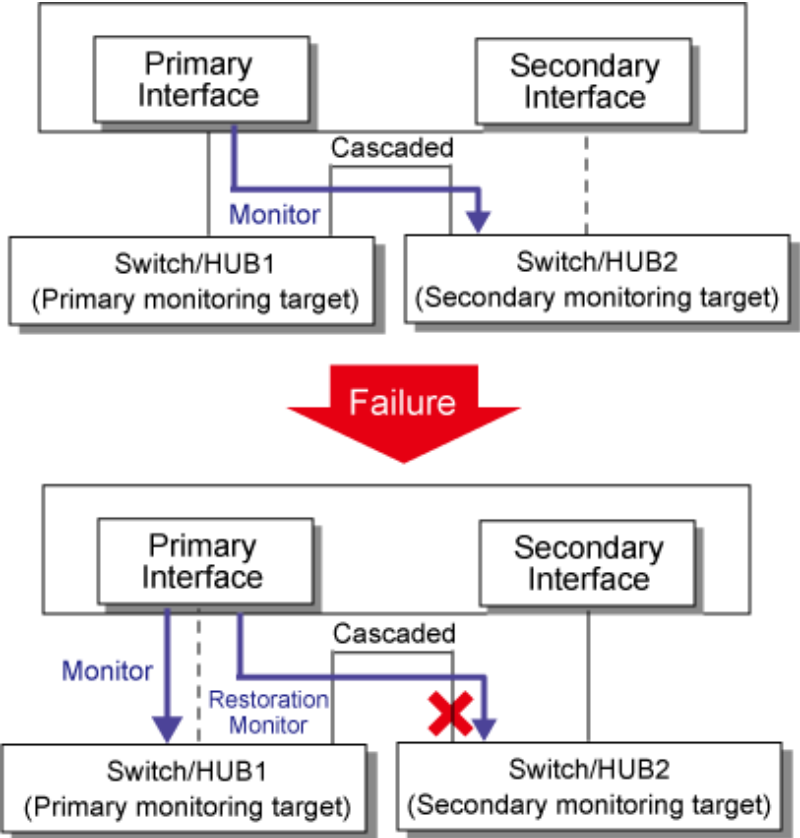
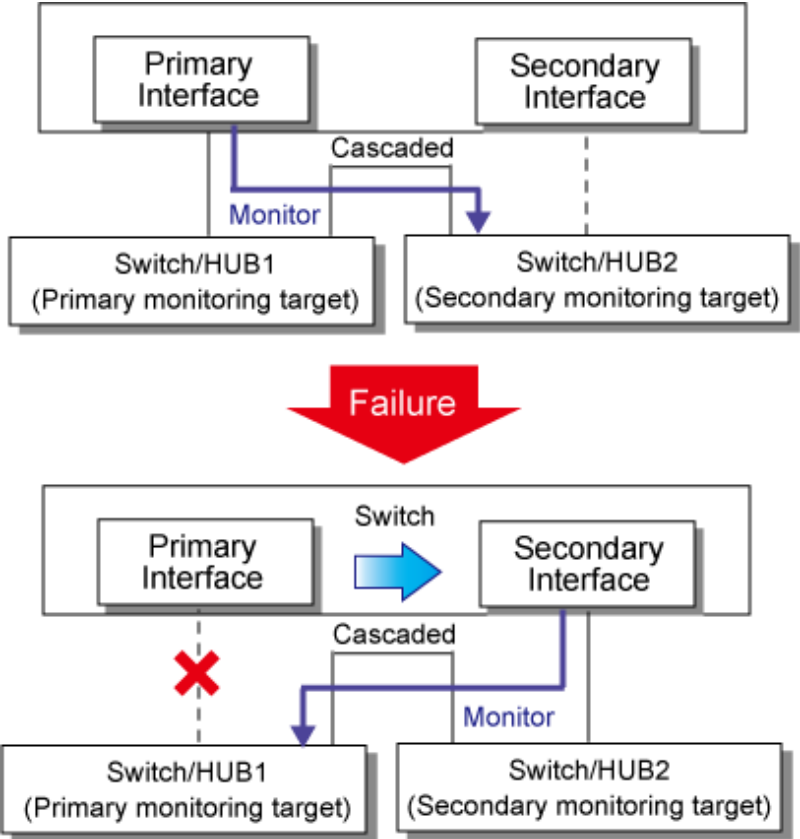


Figure 2.37 HUB-to-HUB monitoring enabled (failure on the primary monitoring)



## 2.4.2 Standby patrol function

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

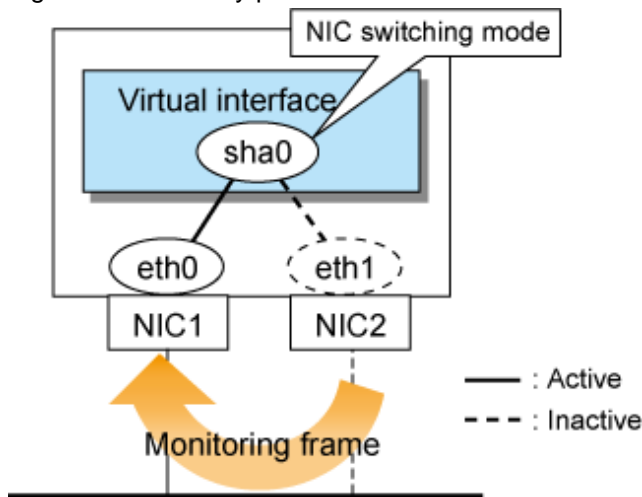
This brings the following effects:

- A message will be reported to an administrator when a failure occurs in standby interface. Therefore, even if a failure has already occurred in operating interface, an administrator is aware of the failure occurred in the standby interface so that switching can be prevented.
- It is possible to fail the interface back automatically, when the standby interface recovers after switching to previous operation. (Automatic fail-back feature.)
- When the transfer path monitoring feature stops due to a failure in every one of the transfer paths, standby patrol feature allows to recover transfer path monitoring feature 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 stpptl Command" for stopping standby patrol.

See "2.4.3 Automatic fail-back function" for an automatic fail-back function.

Figure 2.38 Standby patrol function



### Note

This feature is available exclusively for NIC switching mode. Fast switching mode does not have standby interface. Thus, this feature does not apply to the mode.

## 2.4.3 Automatic fail-back function

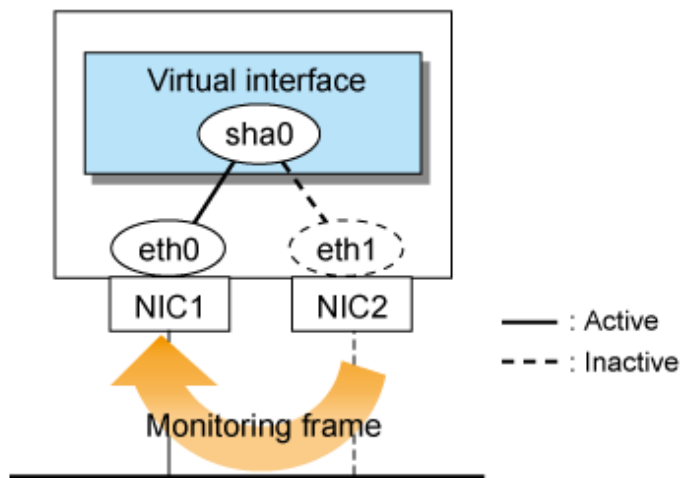
In NIC switching mode, "automatically perform fail-back immediately after recovering the faulted transfer path" or "perform fail-back when the transfer path currently used encounters a failure" can be defined by using a standby patrol function.

For information on the setup, [Figure 2.39 Automatic fail-back function](#) shows the outline of the automatic fail-back function.

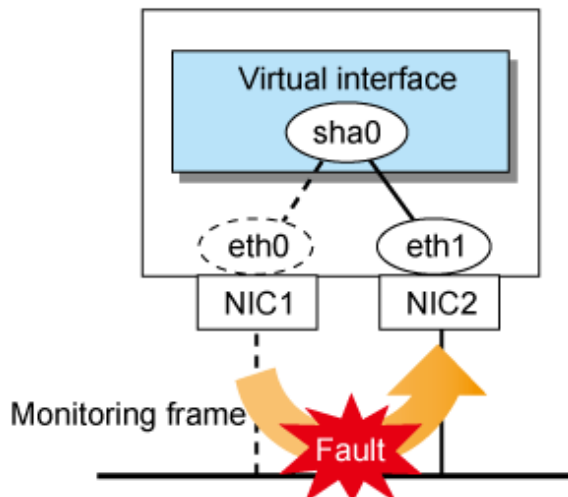


Figure 2.39 Automatic fail-back function

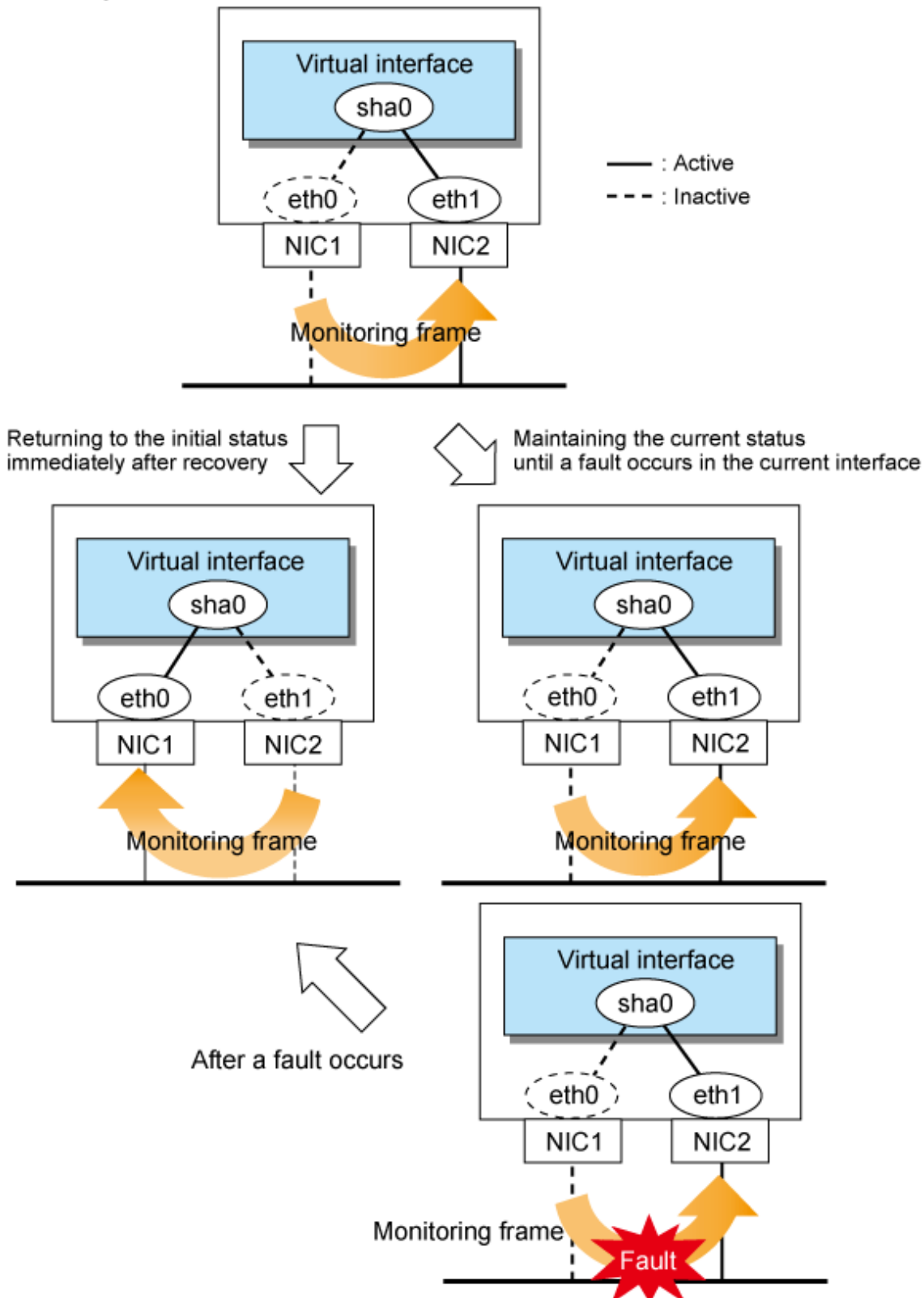
**Initial status**



**After a fault occurs**



## 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 ["4.5.2 Recovery procedure from line failure in NIC switching mode"](#).

## 2.5 Monitoring function of Virtual NIC mode

In Virtual NIC mode, monitoring is performed using the following monitoring functions.

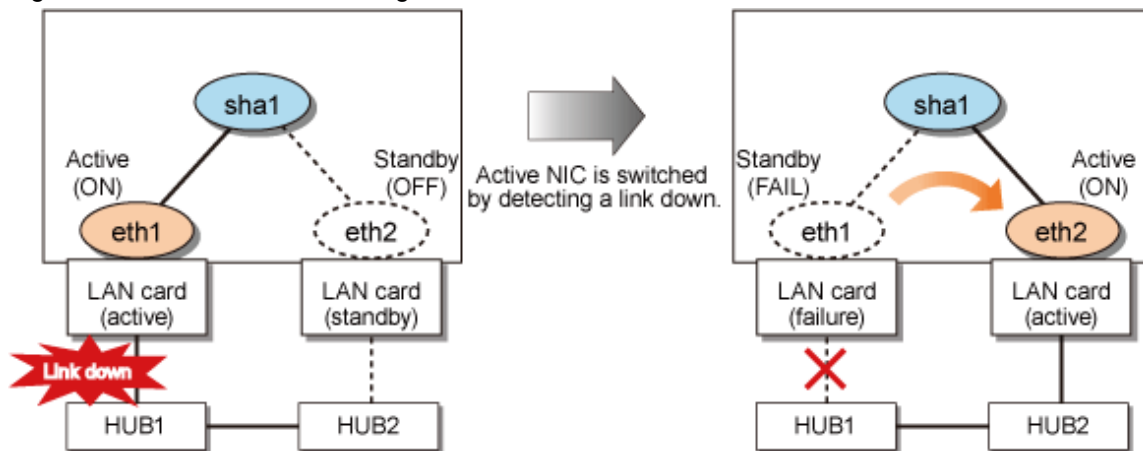
Table 2.4 Available option functions in each mode

Monitoring function	Setting	Function
Link status monitoring	Not required	Monitors the link status of a physical interface. If an error is detected, the communication is switched to a normal NIC.
Network monitoring	Optional	Monitors the status of the network to which a physical interface is connected. If an error is detected, the communication is switched to a normal NIC.

### 2.5.1 Link status monitoring function

In Virtual NIC mode, link statuses of physical interfaces are permanently monitored to detect a link down and a link up. If any link down has been detected in an interface on the active side, and if an interface on the standby side is available, a failover of the transfer path is performed immediately.

Figure 2.40 Link status monitoring function



Monitoring the link status is started on activation of a virtual interface and stops on deactivation of it. You cannot stop monitoring while a virtual interface is activated.



## Point

- Immediately after activating a virtual interface, the system waits for 5 seconds until the links of the bundled physical NICs are established. Therefore, a failover is suspended by 5 seconds after detecting an NIC failure.
- Even if the physical interface is deactivated while the virtual interface is being activated, it is determined that a link is now down.

### 2.5.2 Network monitoring function

In Virtual NIC mode, two methods in the table below are available to monitor the network status to which a physical interface is connected.

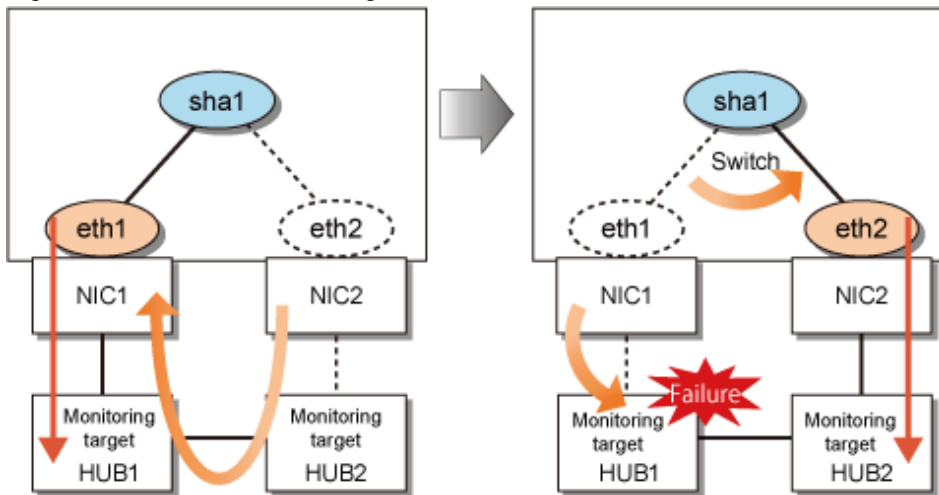
Monitoring type	Monitoring method
HUB monitoring	A ping command is sent periodically to the switch/HUB to which the NIC is connected to check whether the device responds normally.
Standby patrol	An Ethernet frame for monitoring is sent periodically from the standby NIC to the active NIC to check the status of the transfer path between the standby and the active NICs.

The network monitoring function is available by any of the following combination. It is not possible to use this function with only HUB monitoring.

- HUB monitoring and standby patrol
- Only standby patrol
- Nothing

The network monitoring function combines two different types of monitoring inhibit unnecessary switching of transfer paths. For example, if only HUB monitoring detects an error while the standby patrol is normal, this means that the both active NICs and the standby NICs are normal, so the failover of transfer paths is inhibited. Failovers are performed only when both monitoring functions detect an error.

Figure 2.41 Network monitoring function



### Point

- When a link down occurs due to an NIC malfunction, a failover is performed immediately by link status monitoring.
- If automatic fail-back is enabled, after any failover, operation will switch back to the original NIC as soon as the standby patrol detects that the network has recovered.
- After the route is switched to the standby side due to failure detection in case that a communication route failure is also detected in the standby side, switch back to the original NIC automatically.

## 2.6 Monitoring function of GS linkage mode

In GS linkage mode, the following function can be set.

Table 2.5 A monitoring function in GS linkage mode

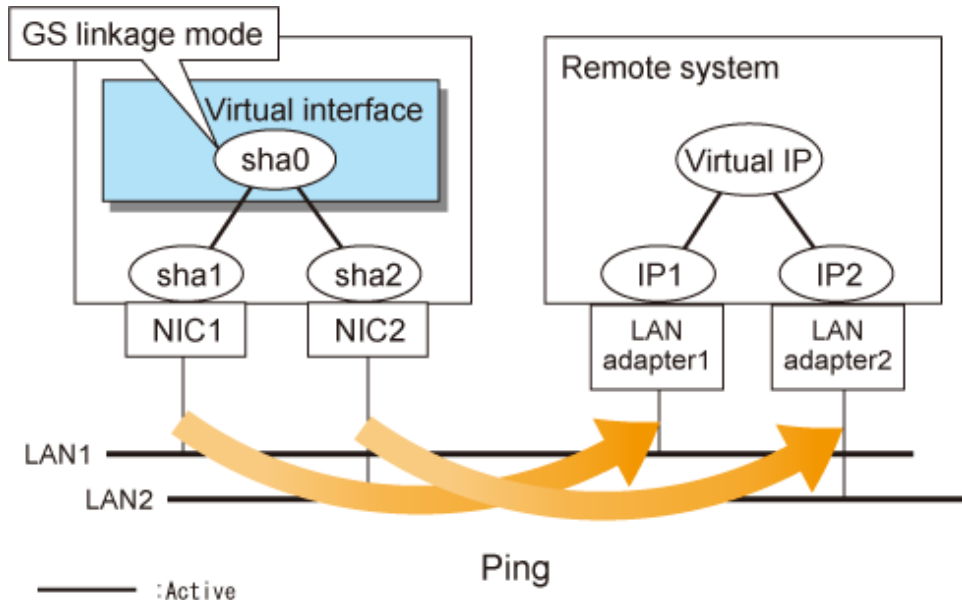
Monitoring function	Setting	function
Communication target monitoring function	Required	Monitors the network by issuing a ping command to the real IP of the communication target. If an error is detected, the communication will be switched to a normal NIC.

## 2.6.1 Communication target monitoring

In GS linkage mode, the ping command is issued against the IP address of the actual interface of the remote system at regular interval. If a transfer path failure is detected or a failure notification is received from the remote system, the route is switched and a reporting message will be output. Then, communication is continued using other transfer path.

In addition, ping monitoring is performed at regular intervals for the path where an error was detected. If the path recovery is detected or is notified by the remote system, the recovered path will be re-enabled after a message is sent out.

Figure 2.42 Communication target monitoring function



See

Set the interval and frequency for ping monitoring to detect errors by using the -s or -c options of the hanetobserv command. Set the interval for ping monitoring to detect path recovery by using the -b option of the hanetobserv command. Also set a ping monitoring destination by using the -t option of the hanetobserv command. For details, see "7.15 hanetobserv Command"

## 2.7 Other monitoring functions

Table 2.6 Functions available for each mode

Function	Mode			
	Fast switching mode	NIC switching mode	Virtual NIC mode	GS linkage mode
Interface status monitoring feature	A	A	X	A
Self-checking function	A	A	A	A

[Meaning of the symbols] A: Allowed, X: Not allowed

### 2.7.1 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 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 2.7 Recoverable interfaces using interface status monitoring feature

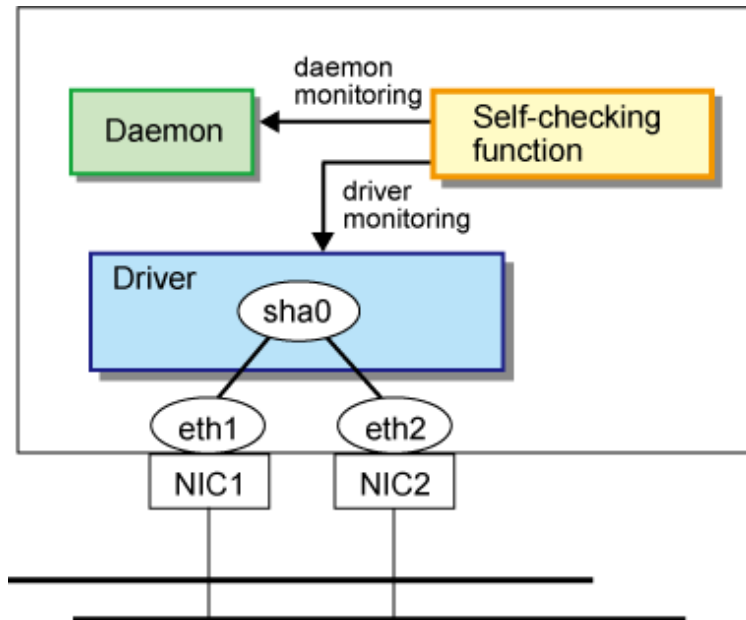
Mode	Single System			Cluster System		
	Virtual I/F (logical I/F)	Logical virtual I/F	Physical I/F	Virtual I/F (logical I/F)	Logical virtual I/F	Physical I/F
Fast switching	N	N	N	A	A	N
NIC switching	A	-	A	A	-	A
Virtual NIC mode	N	N	N	N	N	N
GS linkage	N	-	N	A	A	N

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

## 2.7.2 Self-checking function

GLS achieves the high reliability of the transfer route by using the control daemon and virtual driver. By enabling this function, states are monitored periodically, and users are notified if an error occurs, which provides higher availability.

Figure 2.43 Self-checking function



### Note

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

## 2.8 Linkage functions

Each mode supports the features shown in the [Table 2.8 Functions available for each mode](#).

Table 2.8 Functions available for each mode

Function	Mode			
	Fast switching mode	NIC switching mode	Virtual NIC mode	GS linkage mode
Cluster fail-over when entire transfer routes fails	A	A	A	A

Function	Mode			
	Fast switching mode	NIC switching mode	Virtual NIC mode	GS linkage mode
User command execution function	X	A	X	A

[Meaning of the symbols] A: Allowed, X: Not allowed

## 2.8.1 Cluster fail-over when entire transfer routes fails

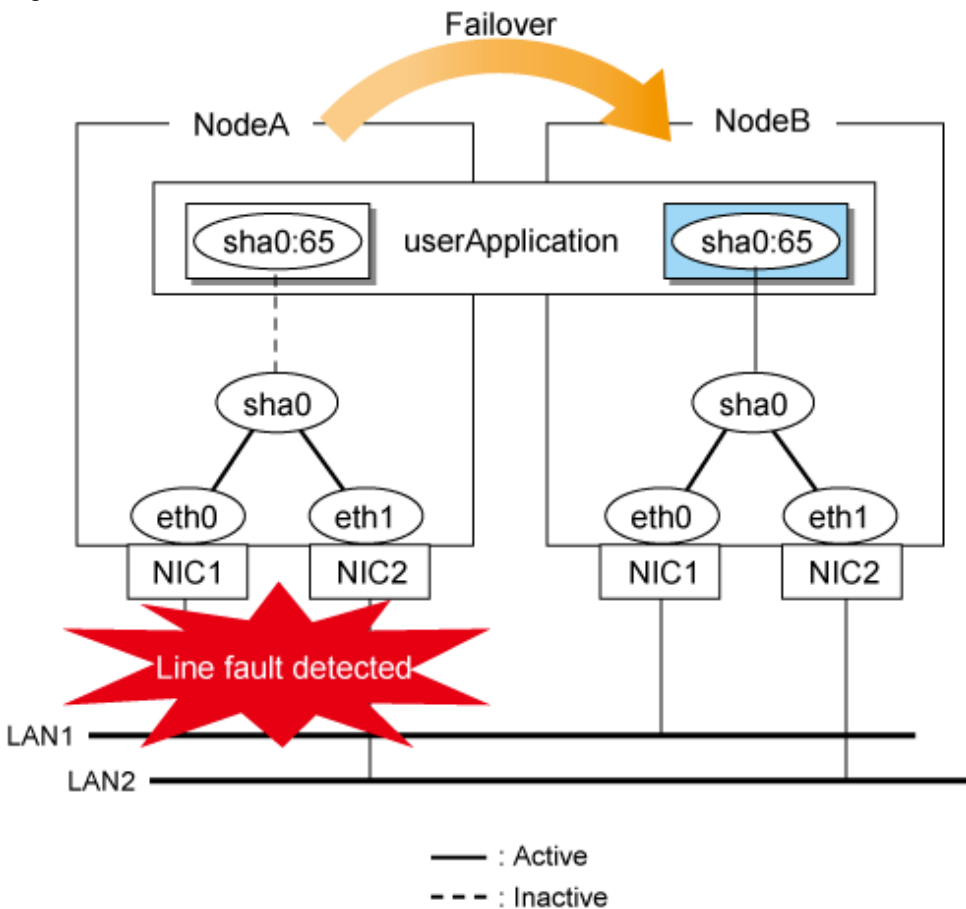
While operating a cluster, if every single transfer route fails for a particular virtual interface, a cluster can switchover to the other cluster. With this capability, the system can be recovered, without administrator's interference, by performing switchover within the cluster when detecting failures 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, Virtual NIC mode, and GS linkage mode. This function is automatically configured when the cluster definition is defined.

Figure 2.44 Cluster failover due to line fault shows an example of fail-over to node B when communication is disabled via both eth0 and eth1 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, Virtual NIC mode, and GS linkage mode as well.

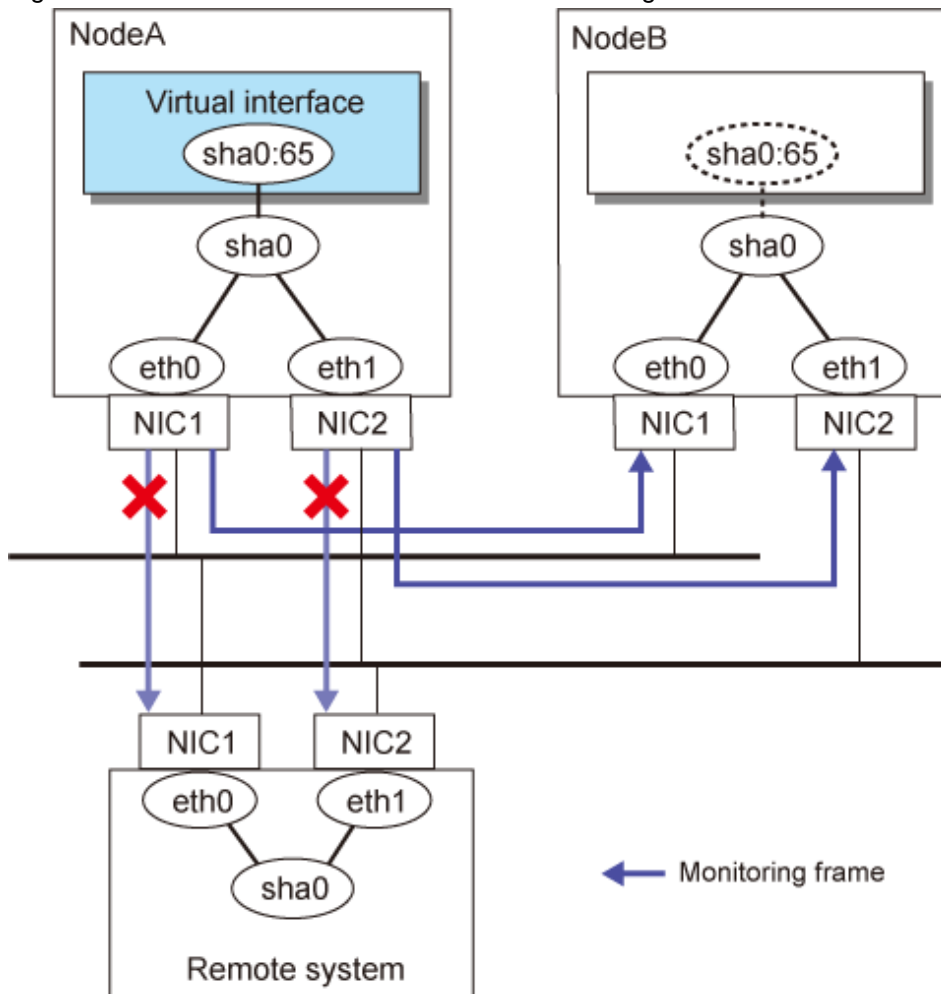
Figure 2.44 Cluster failover due to line fault



### 2.8.1.1 Cluster fail-over of Fast switching mode

In Fast switching mode, GLS determines that an error has occurred on a node when communication is cut off from another node on the same network (via dedicated monitoring frame) in Fast switching mode.

Figure 2.45 Error detection on a node in Fast switching mode



#### Note

When multiple virtual machines are created on one server to set up a cluster configuration, and Fast switching mode is used, an error will not occur to the cluster resources, even if a failure occurs to a switch which exists outside of the server. This is because a configuration is for successful monitoring at any time in the virtual switch in which multiple virtual machines are connected.

#### Information

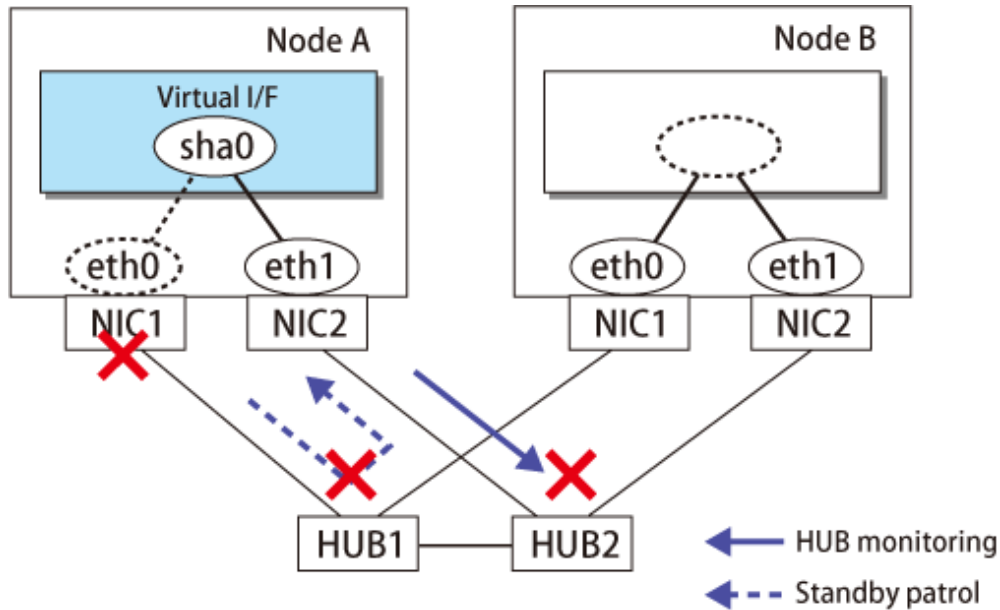
In Fast switching mode, the system is set as a monitoring destination when it is added to the virtual interface bundles' networks.

### 2.8.1.2 Cluster fail-over of NIC switching mode

In NIC switching mode, GLS determines that an error has occurred if HUB monitoring (by ping) fails a second time during standby patrol after the first HUB monitoring (by ping) failure and after NIC switching is performed.



Figure 2.46 Error detection on a node in NIC switching mode



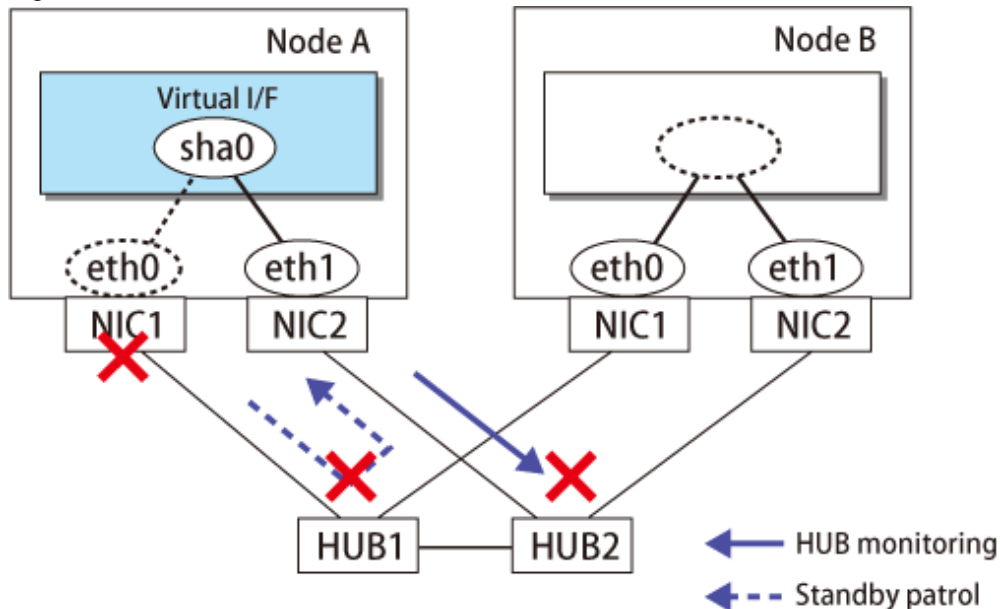
### Information

HUB monitoring is performed for the IP address that is set by the -p option of the hanetpoll command. For details, see "[7.1 hanetconfig Command](#)" and "[7.7 hanetpoll Command](#)".

## 2.8.1.3 Cluster fail-over of Virtual NIC mode

In Virtual NIC mode, GLS determines that an error has occurred on a node if NIC is not recovered and monitoring error is detected also on a switched node after detection of a monitoring error on an active NIC and NIC switching.

Figure 2.47 Error detection on a node in Virtual NIC mode



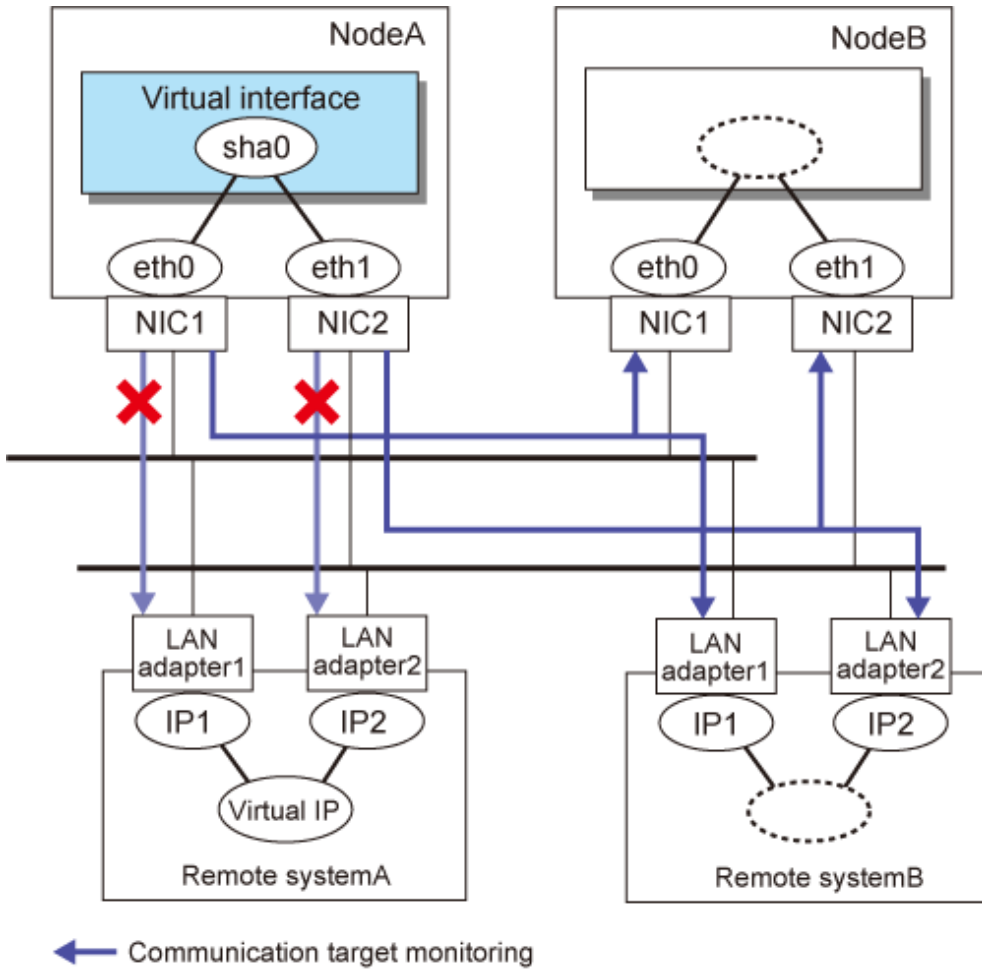
## Information

In network monitoring, HUB monitoring is performed for the IP address that is set by the `-i` option of the `hanetpathmon` command. In addition, setting up the standby patrol is not required. For details, see "[7.1 hanetconfig Command](#)" and "[7.12 hanetpathmon Command](#)".

### 2.8.1.4 Cluster fail-over of GS linkage mode

In GS linkage mode, GLS determines that an error has occurred when every remote host monitoring (by ping) for the remote node and other nodes comprising the local cluster failed.

Figure 2.48 Error detection on a node in GS linkage mode



## Information

Remote host monitoring is performed for the IP address that is set by the `-t` option of the `hanetobserv` command. For details, see "[7.15 hanetobserv Command](#)".

### 2.8.2 User command execution function

A user-defined command can be executed.

## See

For information on the setup, see Section "[3.12.2 Setting user command execution function](#)".



## Note

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

Timing to run is as follows:

### NIC switching mode

- **Running a user-specified 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 monitoring a transfer route 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 and to set the specified routing information.

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

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

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

Run a user-specified command when detected an error in monitoring a transfer route by standby patrol or recovery. Use this to notify a system administrator or an application of detecting an error or recovery. When set 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 2.49 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (Continued.) shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a logical IP address takeover function).

Figure 2.49 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]

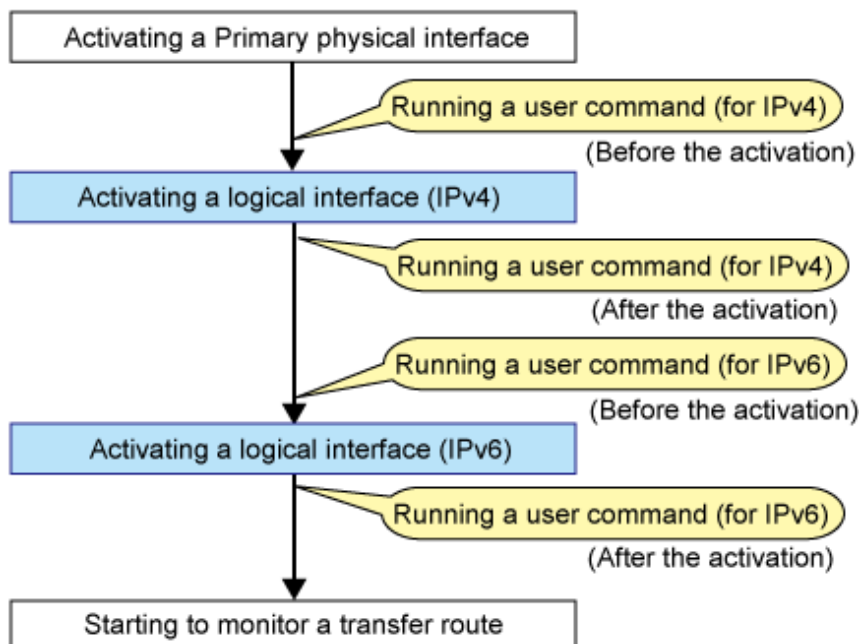


Figure 2.50 Timing of running a user command when activating or deactivating an IP address (a logical IP address takeover function) (End.)

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

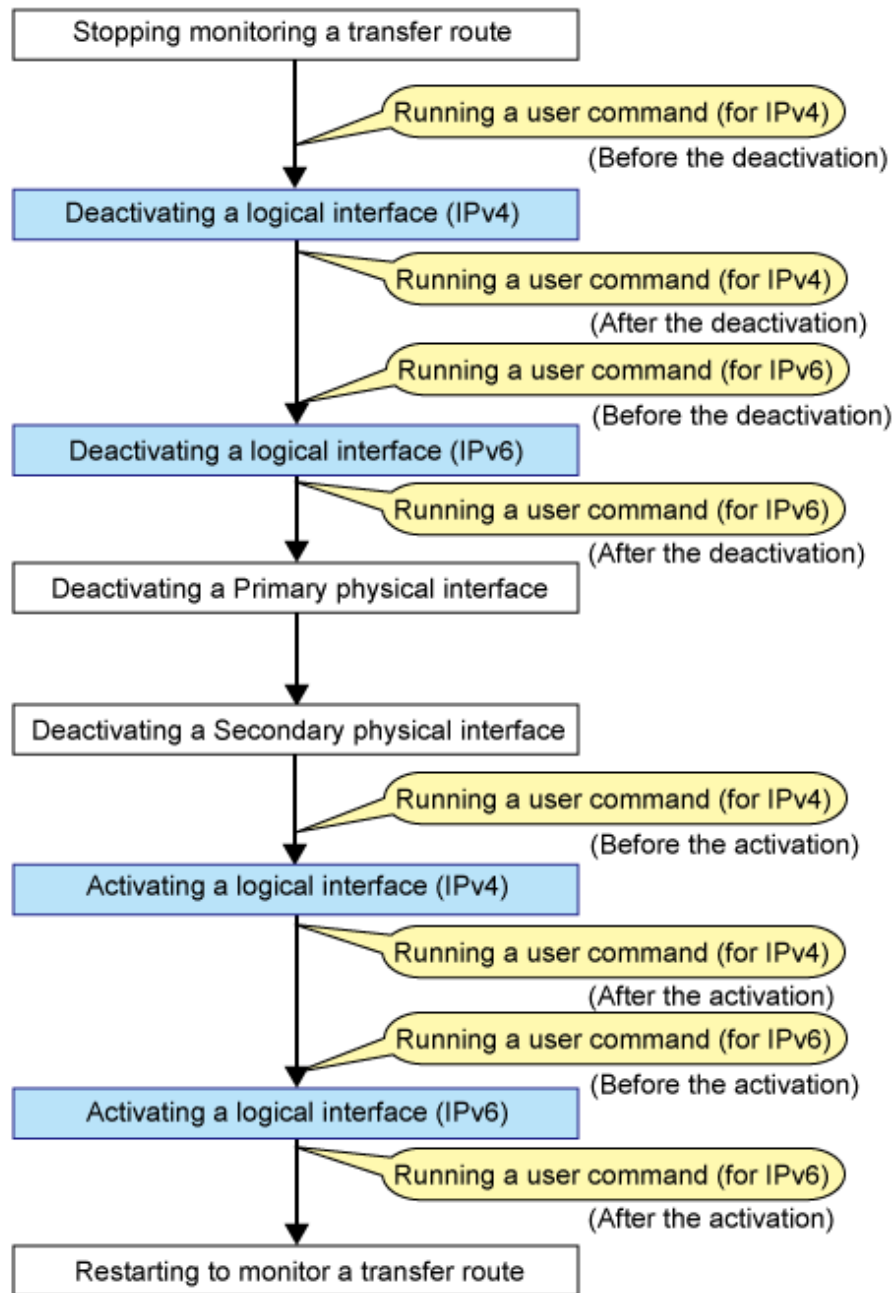
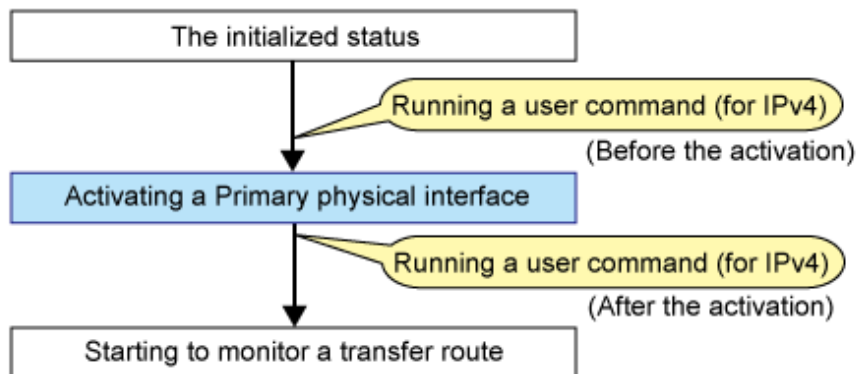


Figure 2.51 Timing of running a user command when activating or deactivating an IP address (a physical IP address takeover function) shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (a physical IP address takeover function).

Figure 2.51 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]

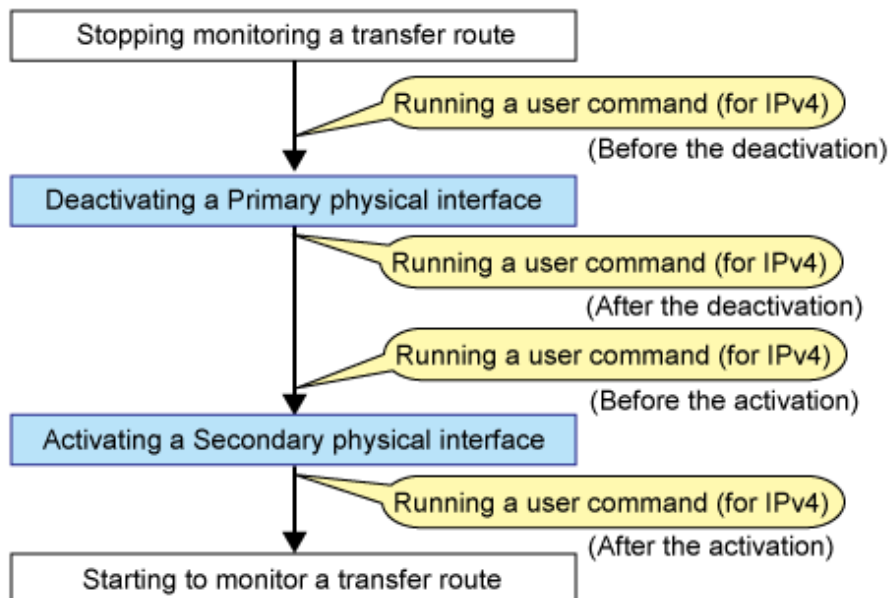
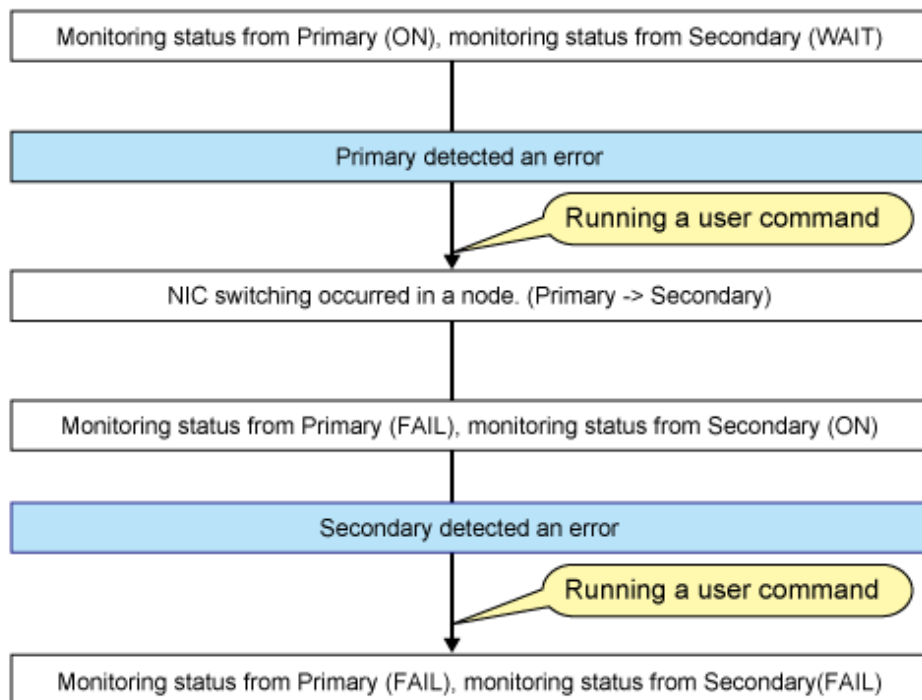


Figure 2.52 Timing of running a user command when detected an error in a transfer route shows timing to run a user command when detected an error in a transfer route in NIC switching mode

Figure 2.52 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]

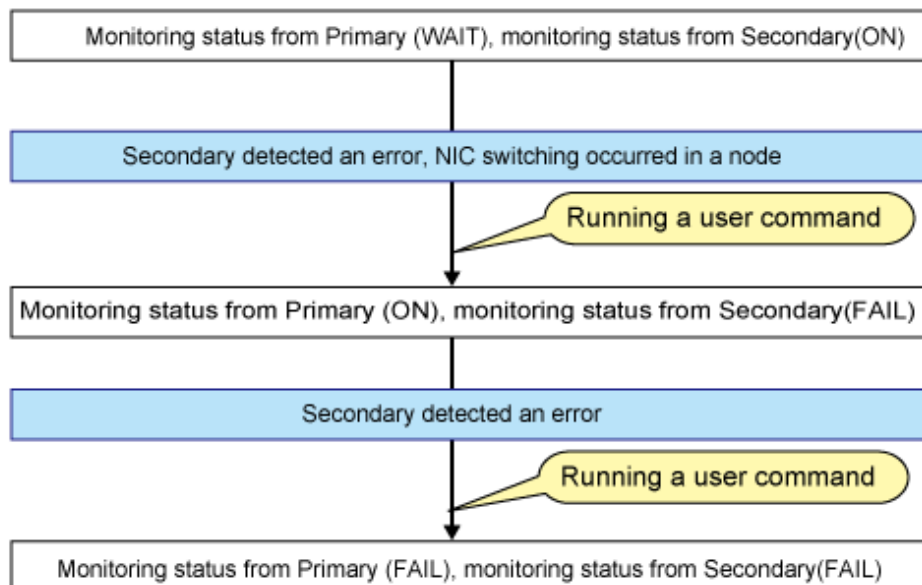
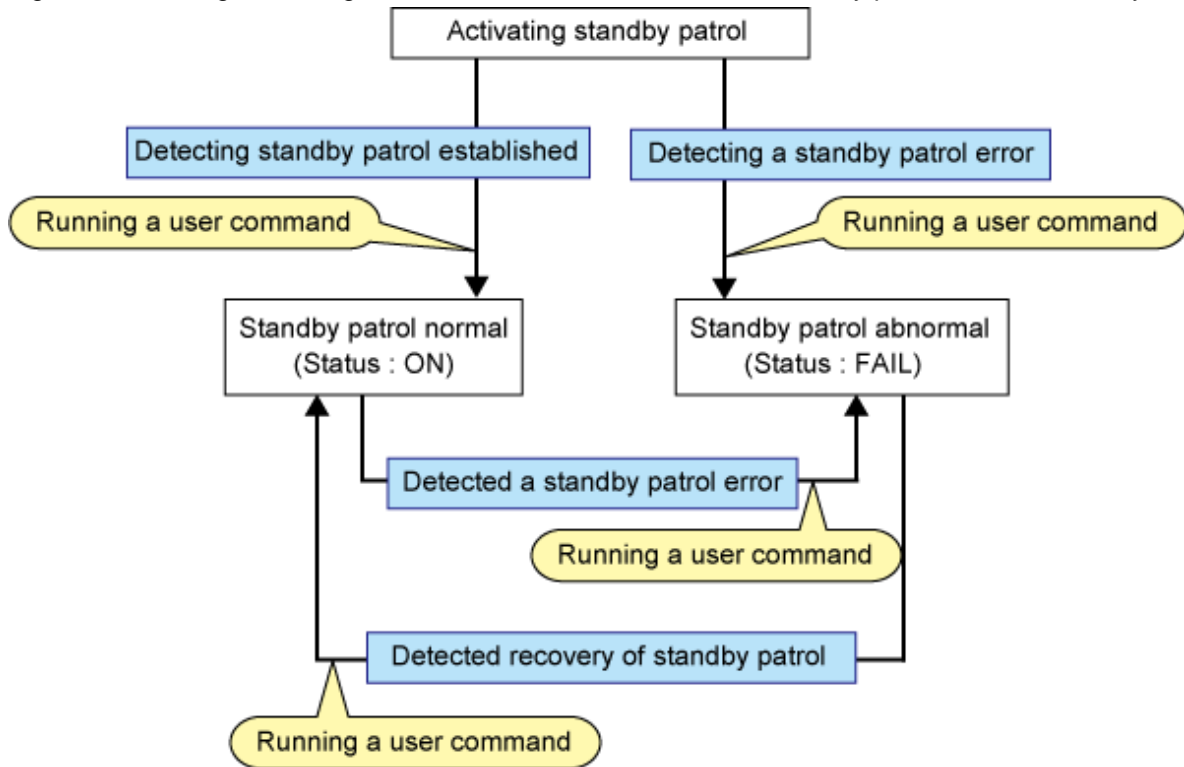


Figure 2.53 Timing of running a user command when detected a standby patrol error or recovery shows timing to run a user command when detected a standby patrol error or recovery in NIC switching mode.

Figure 2.53 Timing of running a user command when detected a standby patrol error or recovery



## GS linkage mode

### - Executing the user command when changing the remote hot-standby system

If a hot-standby system is changed on GS (if you receive a message from GS saying the virtual IP address has been activated.), execute the user-specified command.

This command is used to inform the system administrator or applications that an error occurred.

### - Executing the user command when an error is detected in remote host monitoring

If the monitoring for all physical IP addresses that the virtual IP address on GS bundles is stopped for a specified period of time (default is about 180 seconds), execute the user-specified command.

This command is used to inform the system administrator or applications that an error occurred.

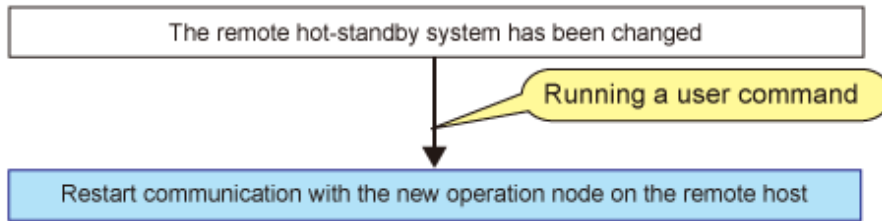
### - Executing the user command when changing nodes on the local system

If a node is changed on the local cluster system, and the takeover virtual IP address is deactivated, execute the user-specified command.

This command is used to inform the system administrator or applications that an error occurred.

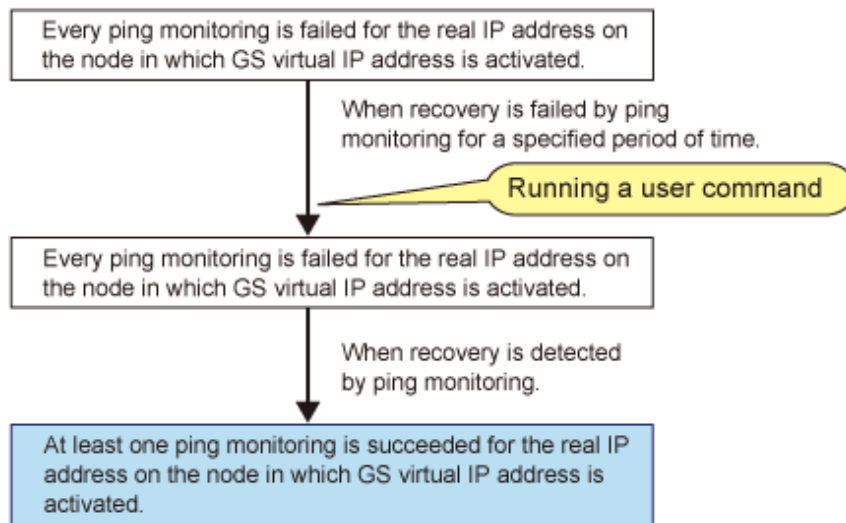
The following shows the timing for executing the user command in GS linkage mode.

Figure 2.54 Timing for executing the user command in GS linkage mode  
[When changing the remote hot-standby system]



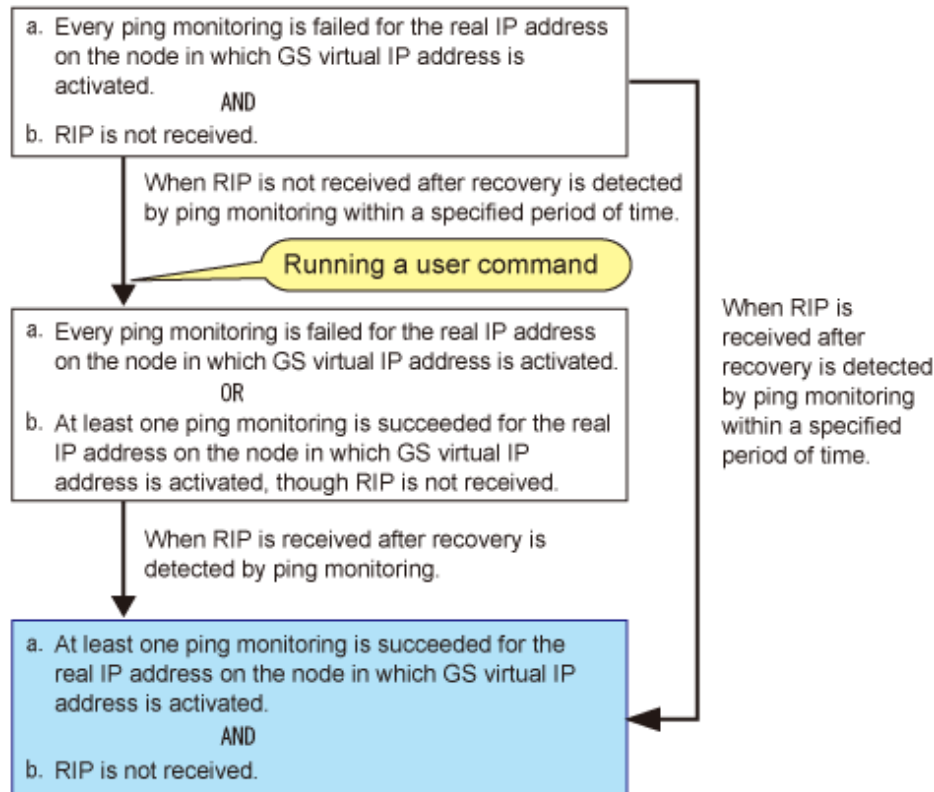
[When an error is detected in remote host monitoring]

- When connecting to GS in the same network

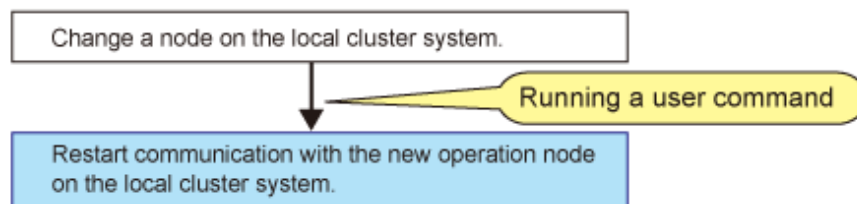




- When connecting to GS in the different network



[When a node is changed on the local cluster system]



## Self-checking function

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.

## 2.9 Maintenance function

The optional functions shown in "Table 2.9 Available option functions in each mode" can be used for each mode.

Table 2.9 Available option functions in each mode

Function	Mode			
	Fast switching mode	NIC switching mode	Virtual NIC mode	GS linkage mode
Dynamically adding/deleting/switching physical interface	A	A	A	A
Active maintenance of NIC (PCI card)	A	A	A	A

[Meaning of the symbols] A: Allowed

## 2.9.1 Dynamically adding/deleting/switching physical interface

---

In Fast switching mode, Virtual NIC mode, and GS linkage mode, 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 2.55 Dynamic adding/deleting function of physical interfaces used](#) shows the outline of workings when executed a command to add/delete the physical interface dynamically.

There are following two modes in a command to add/delete the physical interface dynamically.

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. It is not possible to delete permanently when a virtual interface of Fast switching mode is registered to the cluster resource.



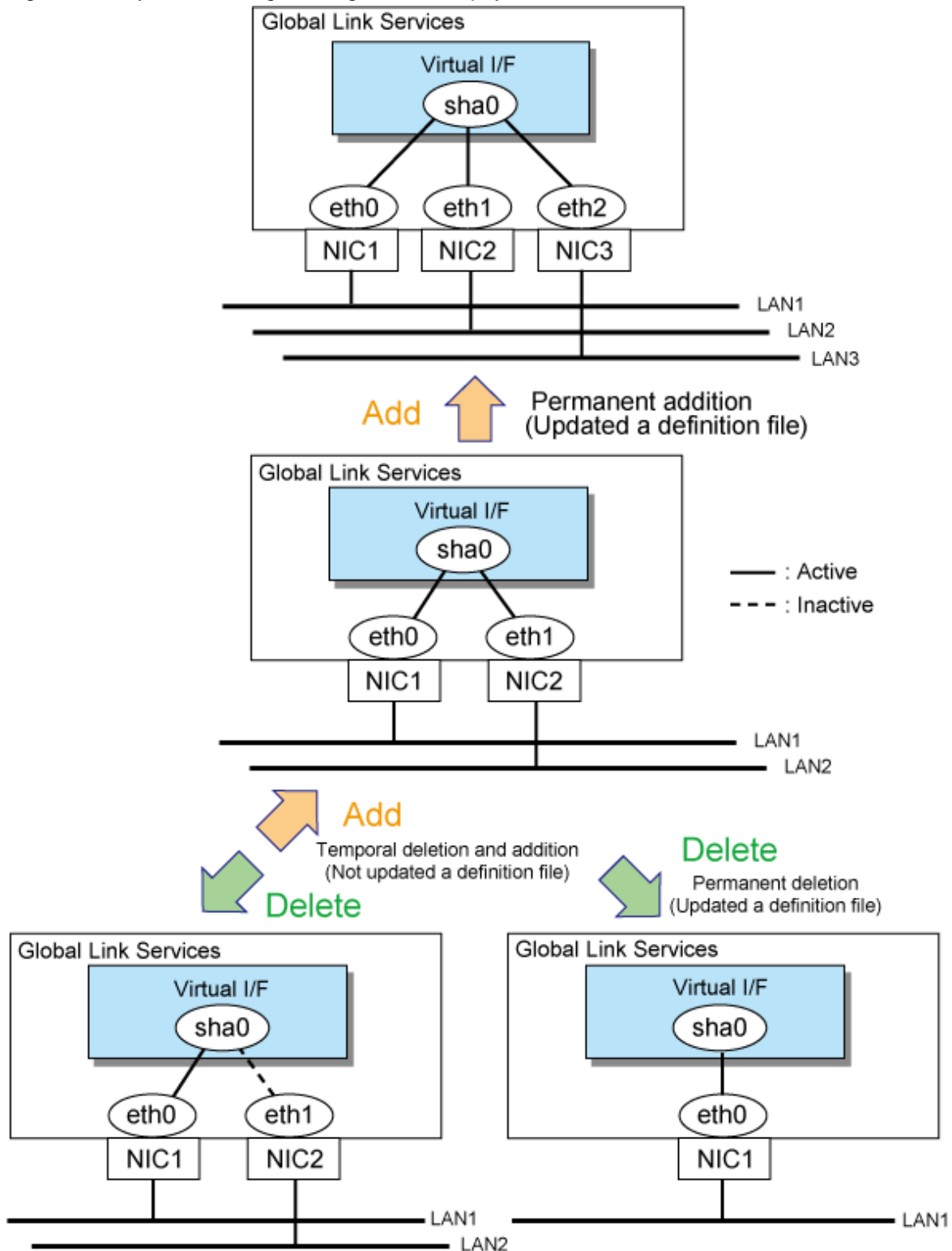
### Note

.....

In GS linkage mode, only temporary dynamic addition/deletion is possible.

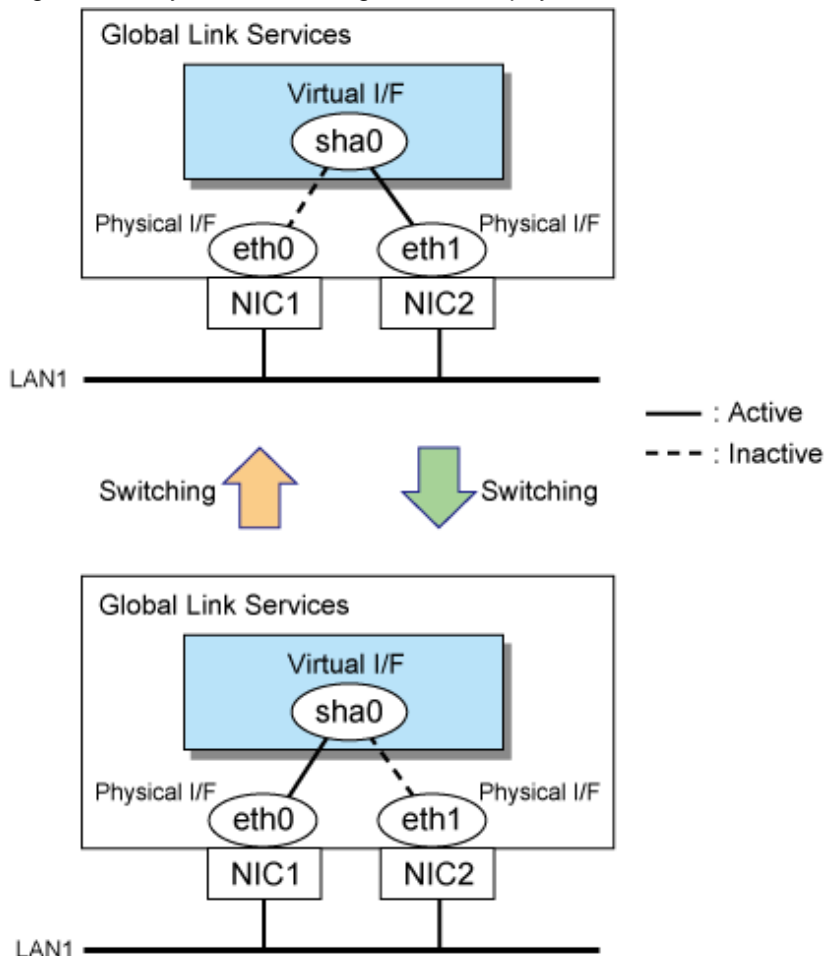
.....

Figure 2.55 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 2.56 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 2.56 Dynamic switching function of physical interfaces used



## 2.9.2 Active maintenance of NIC (PCI card)

Active maintenance of NIC enables NIC removal and replacement without disrupting ongoing operation.



### Note

When the main unit is PRIMEQUEST, it is possible to active maintenance. When the main unit is PRIMERGY, it is not possible to active maintenance.



### See

When you use this function, please refer to the following manual.

- PRIMEQUEST 1000 Series  
PRIMEQUEST 1000 Series Administration Manual
- PRIMEQUEST 2000 Series  
PRIMEQUEST 2000 Series Administration Manual

For information on how to perform active maintenance of the redundant line control function, see "[6.3 NIC maintenance \(for RHEL5\)](#)" or "[6.4 NIC maintenance \(for RHEL6\)](#)".

## 2.10 Notes

---

### 2.10.1 General

---

#### Notes on setting a configuration:

- The minimum and maximum number of virtual and logical virtual interface can be defined is 1 to 64 in total.
- The number of physical interfaces can be used for redundancy on a single virtual interface is within 1 to 8 for Fast switching mode and GS 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.

#### Notes on the operation:

- Do not operate physical interfaces that a virtual interface bundles with an ifconfig command.
- On the system that makes the transfer route redundant by the Redundant line control function, the user must not execute the /etc/init.d/network script.
- The following messages may be output to the console and system log during system startup. This does not disrupt ongoing operation.
  - For RHEL6

```
kernel: sha: module license 'Proprietary' taints kernel.
kernel: Disabling lock debugging due to kernel taint
```
  - For RHEL5

```
kernel: sha: module license 'Proprietary' taints kernel.
```

#### Notes on upper applications:

- When using TCP in a working application, 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 as a timer. When TCP connection is disconnected by the reason such as not possible 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 a working application uses the UDP. It is necessary to execute a recovery process such as sending the data by the application itself.
- When using NTP as an upper 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. In addition, when using NTP on GLS, a NTP daemon has to be defined to be able to communicate using a logical IP address.

### 2.10.2 Duplicated operation by Fast switching mode

---

- To use all host names and IP addresses used in a Redundant line Control Function, they must be defined in /etc/hosts files of the local system
- The length of MTU cannot be modified.
- Multicast IP addresses cannot be used.
- An IPv6 over IPv4 tunneling interface (sitX) is not supported.
- If a user individually activates or deactivates virtual interfaces registered in the cluster, the interface status monitoring feature restores them to their original state on the operation.
- It is not possible to use DHCP (a server function and a client function) as the upper application.

- 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 subnetwork 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 stop using VLAN or 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.

### 2.10.3 Duplicated operation via NIC switching mode

---

- To use all host names and IP addresses used in a Redundant line Control Function, they must be defined in /etc/hosts files of the local system.
- When modifying the length of MTU for an interface, set the same value for the configuration file (ifcfg-ethX) of the primary interface and the secondary interface. The changed value is valid after a system reboot.

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
(...)
MTU=9000

# cat /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
(...)
MTU=9000
```

- Multicast IP addresses cannot be used.
- An IPv6 over IPv4 tunneling interface (sitX) is not supported.
- If a user individually activates or deactivates physical interfaces bundled by the virtual interface, the interface status monitoring feature restores them to their original state on the operation.
- It is not possible to use DHCP (a server function and a client function) as the upper application.
- 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").
- In NIC switching mode, it is necessary to use a hub that can be assigned an IP address in order for the hub to be monitored. If a hub cannot be assigned an IP address, an IP address of a device connected to the hub can be monitored. However, it should be noted that if the device whose IP address is monitored fails, the failure is regarded as a transfer route failure.
- When the system is RHEL, if you are using IPv6 virtual interface, you must set "NETWORKING\_IPV6=yes" in the /etc/sysconfig/network file. By defining this configuration, the system loads ipv6 module during the system startup.
- When using an IPv6 virtual interface, an radvd daemon is occasionally reactivated not to delay configuring an IPv6 address automatically. A message "radvd[XXXX]: resuming normal operation" is output from the radvd daemon following this, but this is not an error.
- Do not configure the server running NIC switching mode as an IPv6 router.

### 2.10.4 Duplicated operation via Virtual NIC mode

---

- By virtual interfaces in Virtual NIC mode, activation and deactivation are performed in conjunction with the network service of the operating system. Therefore, virtual interfaces keep active state by the "resethanet" command even when restarting GLS.

- In Virtual NIC mode, define the settings of IP addresses in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) same as for usual NICs. As in other communication modes, it is not required to set IP addresses by using the hanetconfig command.
- Do not set tagged VLAN interfaces for physical interfaces used in Virtual NIC mode. If tagged VLAN interfaces are set, activation of virtual interfaces fails.
- In Virtual NIC mode, the interface setting file of a virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX) is created and deleted at the following timing:
  - For creation: when a virtual interface is set by using the "hanetconfig create" command.
  - For deletion: when a virtual interface is deleted by using the "hanetconfig delete" command.
- The interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) of the virtual interface is prepared as a symbolic link of the GLS configuration file (/etc/opt/FJSVhanet/config/ifcfg-shaX) when the virtual interface is set up. If you delete the symbolic link by mistake, re-create a symbolic link by using the "ln(1)" command.
- When the libvirtd service is started by starting RHEL6, NIC (for example: 10G NIC) which supports LRO (large-receive-offload) function may link down temporally. In this case, GLS detects a link down of NIC and an error message may be output to the system log. To prevent a link down, perform one of the following actions:
  - Set "1" to "net.ipv4.ip\_forward = "in the /etc/sysctl.conf file.
  - Disable the libvirtd service. (when the virtual machine function is not used.)

For details, refer to "Linux documentation".

- When modifying the length of MTU for an interface, set the same value for the configuration file (ifcfg-ethX) of the primary interface and the secondary interface, and for the virtual interface configuration file (ifcfg-shaX). The changed value is valid after a system reboot.

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
(...)
MTU=9000

# cat /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
(...)
MTU=9000

# cat /etc/sysconfig/network-scripts/ifcfg-sha0
DEVICE=sha0
(...)
MTU=9000
```

- The interface created by SR-IOV cannot be used.
- Do not enable the LLDP(Link Layer Discovery Protocol) function of the physical interface.

## 2.10.5 Duplicated operation via GS linkage mode

- To use all host names and IP addresses used in a Redundant line Control Function , they must be defined in /etc/hosts files of the local system
- The length of MTU cannot be modified.
- Multicast IP addresses cannot be used.
- An IPv6 over IPv4 tunneling interface (sitX) is not supported.
- If a user individually activates or deactivates virtual interfaces registered in the cluster, the interface status monitoring feature restores them to their original state on the operation.
- It is not possible to use DHCP (a server function and a client function) as the upper application.

- If you use GS linkage mode, be sure to set up the remote host monitoring function. For information on how to do this, see "[7.15 hanetobserv Command](#)".
- If you use GS linkage mode, be sure to set up the virtual gateway. For information on how to do this, see "[7.14 hanetgw Command](#)".
- GS linkage mode is not available for communications between a Linux server and a Solaris server.
- Do not set the same virtual IP address on GS for the communication target, if you set multiple GLS's takeover virtual IP addresses within the same cluster. You can do this between different clusters.
- Set a different network address from the virtual IP address of the communication target GS for a virtual IP address in GS linkage mode.
- Set the virtual IP addresses used in GS linkage mode to have different network addresses.
- When communicating between GLS and GS via router, make sure that the router neighboring GLS is RIPv1 and the path to GS's virtual IP address is broadcast.
- When using the remote network communication (communication via router) in GS linkage mode, set the same netmask for the virtual IP addresses of GS and GLS, and physical IP addresses.
- When using the neighboring communication (communication without router) in GS linkage mode, setting the same netmask for the virtual IP addresses of GS and GLS, and physical IP addresses is recommended. Use the different netmask for each IP address only under the following conditions:
  - Length of the netmask of all the physical IPs is consistent.
  - Length of the netmask of the virtual IP is consistent between the host and the server, and longer than the length of the physical IP.
- In GS linkage mode, the tagged VLAN function is not available.
- If GS is in the hot-standby configuration, the node that received the down notification by the TNOTIFY command from GS is recognized as the communication target.
- If the TNOTIFY command is executed to GLS from GS, GLS returns the processing result 80.
- When using the logical virtual IP address of GS linkage mode as a source, it is necessary to fix the logical virtual IP address to be the source on the application side with the bind function.
- The interface created by SR-IOV cannot be used.
- In a cluster configuration, in order to prevent a failover when all the GSs of communication targets stopped, the information of operation node and standby nodes and neighboring switches needs to be created as the monitoring destination information of the remote host. For information on the creation, see "[7.15 hanetobserv Command](#)".



## Chapter 3 Environment configuration

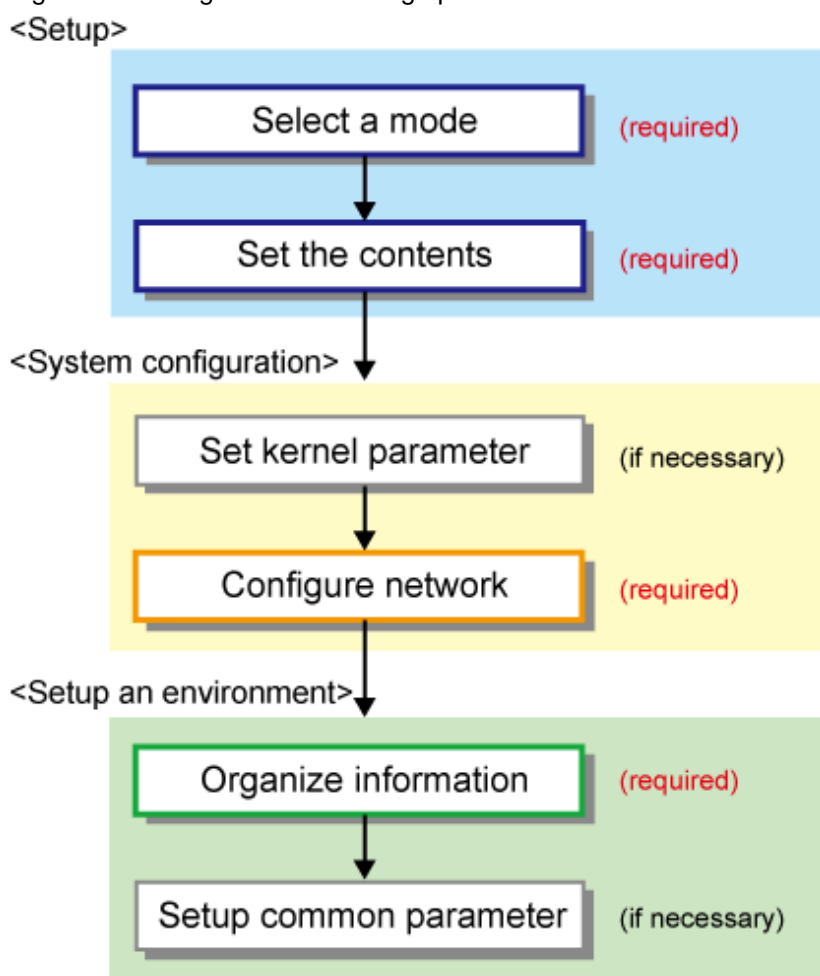
This chapter discusses how to set up and configure GLS.

### 3.1 Setup

Select a GLS mode and prepare 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 uses Fast switching mode. 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. Select this mode in most cases.

Mode	Selecting mode
Virtual NIC mode	Select this mode in the following cases: - A Linux server is placed on a network where a hot-standby router, a network load balancer, or servers and other various network devices from other manufacturers are used.  - Multicast communication or IPv6 is used.  - Communication of a guest OS is duplicated on the host OS when the virtual machine function is used.
GS linkage mode	Select this mode if a transfer route is multiplexed between GS, PRIMEQUEST, or PRIMERGY.

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

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 [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 following 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/radvd.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 set by using "hanetmask" command. However, this configuration is not necessary if using IPv6 address.

### <Physical interface information>

Setup the following 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. eth1, eth2 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. To setup this component, create "/etc/sysconfig/network-scripts/ifcfg-ethX" file and then assign the IP address in the file.

#### 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/sysconfig/network-scripts/ifcfg-ethX" 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
	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 virtual interfaces)		

Description of each component is as follows:

### <Virtual interface information>

Setup the following 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 by using "hanetmask" command. When using IPv6 address, it is not required to configure this value.

#### <Physical interface information>

Setup the following 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.eth1, eth2 etc)

##### 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. In order to specify an IP address for the physical interface, create "/etc/sysconfig/network-scripts/ifcfg-ethX" file and then assign an IP address in the file.

#### <Standby patrol information>

When using Standby patrol function, setup the following. 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.

#### <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 the 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 Virtual NIC mode

[Table 3.4 Configuration information of Virtual NIC mode](#) shows the information required to configure Virtual NIC mode.

Table 3.4 Configuration information of Virtual NIC mode

Components			
Virtual interface information (1)	Virtual interface name		
	Virtual IP address (or host name)		
	Subnet mask		
	Physical interface information (1)	Physical interface name	
	Physical interface information (2)	Physical interface name	
	Monitored remote system information	Primary Monitored remote system IP address or host name	
		Secondary Monitored remote system IP address or host name	
(Repeat for the number of virtual interfaces)			

Description of each component is as follows:

#### <Virtual interface information>

Set up the following 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. The interface setting file of the virtual interface is created when the virtual interface is set by the "hanetconfig create" command.

##### Virtual IP address or host name

Specify an IP address or host name allocated to the virtual interface. This value is defined in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) of the virtual interface "shaX".

##### Subnet mask

When setting virtual IP address, specify the value of a sub network mask used for the virtual IP address. This value is defined in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) of the virtual interface "shaX".

In addition, when setting a cluster takeover IP address with the hanethvrsc command, specify the subnet mask also with the hanetmask command.

#### <Physical interface information>

Set up the following 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.eth1, eth2 etc)

#### <Monitored remote system information>

Set up the following to activate HUB monitoring of the network monitoring function. Note that HUB monitoring is not performed when this information is 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 "hanetpathmon target" command.

##### 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 "hanetpathmon target" command. This step can be omitted. In such case, the same value as primary remote end IP address or host name is applied.

### 3.1.2.4 GS linkage mode

Table 3.5 Configuration information of GS linkage mode shows the information required to configure GS linkage mode.

Table 3.5 Configuration information of GS linkage mode

Components				
Virtual interface information	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	Remote node name			
	Virtual IP information	Virtual IP address		
		Remote host physical IP address information	IP address or host name (1)	
			Router IP address or host name (1)	
			IP address or host name (2)	
			Router IP address or host name (2)	
			(Repeat for the number of IP addresses)	
	(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 following 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. This configuration can be omitted if not allocating a subnet. Set a subnet mask by using "hanetmask" command. When applying subnet mask, apply the same mask value to the whole virtual and physical IP.

#### <Physical interface information>

Setup the following 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. This configuration can be omitted if not allocating a subnet. Set a subnet mask by using "hanetmask" command. 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 creates the "/etc/sysconfig/network-scripts/route-virtual interface name" file and sets the information for the virtual gateway static route in the file. In addition, specify the IP address of the virtual gateway with the -g option of the hanetgw create command.

#### <Remote node information>

Configure the following for the number of host nodes.

##### Remote node 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 following 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.

##### Router IP address or host name

When you use remote network communication with GS via router, specify the IP address or host name of the local system's router in the 'router IP address + remote physical IP address' format according to the remote physical IP address information. The host name and IP address need to be defined in the /etc/hosts file as well. You do not need to set this item if you do not use remote network communication.

### 3.1.2.5 Configuration of individual mode

[Table 3.6 Configuration of redundancy mode](#) shows description of common parameters for each mode. These values apply to the whole system. However, these values cannot convert to unit of the virtual interface or redundancy mode. This configuration is not necessary when using the default value.

Table 3.6 Configuration of redundancy mode

Contents	Fast switching mode	NIC switching mode	Virtual NIC mode	GS linkage mode	Default
Transfer path monitoring interval	A	N	N	N	5 sec
The number of constant monitoring prior to outputting message	A	N	N	N	0 time
The number of constant monitoring prior to switching cluster	A	N	N	N	5 sec
Switching cluster immediately after starting	A	N	N	N	none
Outputting message (monitoring the physical interface)	A	N	N	N	none
Standby patrol monitoring period	N	A	N	N	15 sec
The number of constant standby monitoring prior to outputting message	N	A	N	N	3 times
Monitoring period	N	A	A	A	5 sec (Virtual NIC mode: 3 sec)
The number of monitoring	N	A	A	A	5 times
Recovery monitoring period	N	N	N	A	5 sec
Cluster switching	N	A	A	A	Yes
Link up waiting period	N	A	A	A	60 sec (Virtual NIC mode: 45 sec )
Link status monitoring function	N	A	A	N	No (Virtual NIC mode: Automatically activated)
Hostname resolution function	A	A	N	A	No
Automatic start of monitoring	N	N	A	N	Yes
The number of recovery monitoring	N	N	A	A	Virtual NIC mode: 2 times GS linkage mode: 0 times
Automatic fail-back	N	N	A	N	No
Self-checking function	A	A	A	A	No

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

The following 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). This feature is specified 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 mode.

#### 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 mode.

#### 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 execution 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 execution 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 execution 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 execution 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.

#### 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). For Virtual NIC mode, 3 (seconds) is set.

This configuration is specified by the following commands:

- NIC switching mode

Specify the value by using the "hanetpoll on" command with the "-s" option.

- Virtual NIC mode

Specify the value by using the "hanetpathmon param" command with the "-s" option.

- GS linkage mode

Specify the value by using the "hanetobserv param" command with the "-s" option.

This feature is available for NIC Switching mode, Virtual NIC mode, or GS 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 by the following commands:

- NIC switching mode

Specify the value by using the "hanetpoll on" command with the "-c" option.

- Virtual NIC mode

Specify the value by using the "hanetpathmon param" command with the "-c" option.

- GS linkage mode

Specify the value by using the "hanetobserv param" command with the "-c" option.

This feature is available for NIC switching mode, Virtual NIC mode, or GS linkage mode.

## Recovery monitoring period

Specify the monitoring period when a failure is detected by communication host monitoring for GS linkage mode. The values which can be specified are from 1 to 300. The default value is 5 (seconds). This configuration is assigned via "hanetobserv param" command with -b option. This feature is available for GS 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 the following commands:

- NIC switching mode

Specify the value by using the "hanetpoll on" command with the "-f" option.

- Virtual NIC mode

Specify the value by using the "hanetpathmon param" command with the "-f" option.

- GS linkage mode

Specify the value by using the "hanetobserv param" command with the "-f" option.

This feature is available for NIC switching mode, Virtual NIC mode, or GS linkage mode only when operating as a cluster.

## Link up waiting period

Specify the time period (in seconds) until the HUB to 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). For Virtual NIC mode, it is set to 45 (seconds). If the value is less than the product of monitoring period and monitoring times (monitoring period X 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 the following commands:

- NIC switching mode

Specify the value by using the "hanetpoll on" command with the "-p" option.

- Virtual NIC mode

Specify the value by using the "hanetpathmon param" command with the "-p" option.

- GS linkage mode

Specify the value by using the "hanetobserv param" command with the "-p" option.

This feature is available for NIC switching mode, Virtual NIC mode, or GS linkage mode.

## Link status monitoring function

Specify whether to monitor the link state of the NICs in the virtual interface bundles.

- NIC switching mode

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. Specify this monitoring with the -l option of the hanetpoll on command.

- Virtual NIC mode

The link status is automatically monitored.

This feature is available for NIC switching mode or Virtual NIC mode.

#### Hostname resolution function

If you enable this function when the host name, not the IP address, is specified for setting GLS, you can assign the IP address of GLS to NICs based on the host file (/etc/hosts) without depending on the OS setting (/etc/nsswitch.conf). This function is enabled in Fast switching mode, NIC switching mode, or GS linkage mode.

#### Automatic start of monitoring

Specify whether to start the network monitoring function in conjunction with startup of the virtual interface in Virtual NIC mode.

yes: Starts the network monitoring function in conjunction with startup of the virtual interface.

no: Does not start the network monitoring function in conjunction with startup of the virtual interface.

The default value is "yes". Specify the value using "hanetpathmon param" command with - a option. This value is effective in Virtual NIC mode.

#### The number of recovery monitoring

- Virtual NIC mode

Specify the number of success counts to go back to the normal monitoring after recovery of a monitoring target is detected in the recovery monitoring by the standby patrol of the network monitoring function. The values which can be specified are from 1 to 300. The default value is 2 (times). (The monitoring target is considered as recovered if the standby patrol succeeds twice.) Specify the value using "hanetpathmon param" command with - r option.

- GS linkage mode

Specify the number of retry counts to go back to the normal monitoring after recovery of a monitoring target is detected in the recovery monitoring for the real IP of the communication target. The values which can be specified are from 0 to 300. The default value is 0 (times). (The monitoring target is considered as recovered if the ping monitoring succeeds once and no retry occurs.)

Specify the value using "hanetobserv param" command with - r option.

This feature is available for Virtual NIC mode or GS linkage mode.

#### Automatic fail-back

Specify whether to perform the automatic fail-back when recovery of transfer paths between active NICs and standby NICs is detected by using the standby patrol function in Virtual NIC mode.

yes: Performs the automatic fail-back.

no: Does not perform the automatic fail-back.

The default value is "no". Specify the value using "hanetpathmon param" command with - q option. This value is effective in Virtual NIC mode.

#### Self-checking function

If this function is enabled, the operational state of the GLS is monitored periodically. This function is available for the Fast switching mode, NIC switching mode, Virtual NIC mode, or GS linkage mode.

### 3.1.2.6 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 linkage mode

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

Configuration item	Upper limit
Maximum number of virtual IP addresses (Note 1)	128
Maximum number of physical IP addresses	64
Maximum number of nodes in which a single virtual IP address can be transferred (Note 2)	4

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



See

For information on how to set the upper limit, refer to "7.15 hanetobserv Command".

For details on setting of monitoring in a cluster configuration, refer to "3.10.1 Monitoring the remote host".

Note 2) Node can be expanded to 16 by editing the configuration file as follows.

/etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
# Each entry is of the form:
#
# <param> <value>
#
observ_msg      0
observ_polling_timeout 180
max_node_num    4      <- changed
```



Note

Executing the resethanet -s command or restarting the operating system is required to reflect the change.

## 3.2 System Setup

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

## 3.2.1 Setup kernel parameters

The following system resources are required for redundant line control function. If the values are insufficient for the entire system, modify the kernel parameters to expand the system resources.

For modifying the kernel parameter, refer to the Linux, sysctl(8), or proc(5) manual.

Table 3.7 Required system resource

System resource	Required value	file
maximum size of shared memory segment (byte)	6144 or more	/proc/sys/kernel/shmmax
amount of shared memory segment	2	/proc/sys/kernel/shmmni
semaphore identification value	1	/proc/sys/kernel/sem
semaphore identification value in the system	1	/proc/sys/kernel/sem

## 3.2.2 Network configuration

### 3.2.2.1 Setup common to modes

#### (1) Physical interface settings

Set up physical interfaces. The physical interface settings vary depending on redundant network methods and operating system.

See the following [Table 3.8 Physical interface settings](#).

Table 3.8 Physical interface settings

Redundant network methods		Operating system	
		RHEL5/RHEL6	
		Tagged VLAN disabled	Tagged VLAN enabled
Fast switching mode (IPv4)		<a href="#">Setup 1</a>	<a href="#">Setup 3</a>
Fast switching mode (IPv6)		<a href="#">Setup 2</a>	<a href="#">Setup 4</a>
Fast switching mode (Dual)		<a href="#">Setup 1</a>	<a href="#">Setup 3</a>
NIC switching mode (IPv4)	Primary interface	<a href="#">Setup 1</a>	<a href="#">Setup 3</a>
	Secondary interface	<a href="#">Setup 2</a>	<a href="#">Setup 4</a>
NIC switching mode (IPv6)	Primary interface	<a href="#">Setup 2</a>	<a href="#">Setup 4</a>
	Secondary interface	<a href="#">Setup 2</a>	<a href="#">Setup 4</a>
NIC switching mode (Dual)	Primary interface	<a href="#">Setup 1</a>	<a href="#">Setup 3</a>
	Secondary interface	<a href="#">Setup 2</a>	<a href="#">Setup 4</a>
Virtual NIC mode		<a href="#">Setup 5</a>	<a href="#">Setup 5</a>
GS linkage mode		<a href="#">Setup 1</a>	Not supported



#### Note

When a operating system is RHEL5 or RHEL6, to specify "HWADDR=XX:XX:XX:XX:XX:XX" for the GLS physical interface settings (the "/etc/sysconfig/network-scripts/ifcfg-ethX" file), add "HOTPLUG=no" to the settings. When the system is RHEL5, edit /etc/udev/rules.d/60-net.rules file, /etc/hotplug/net.agent file or /etc/udev/rules.d/31-network.rules file to invalidate the network hotplug function of the interface (sha\*,eth\*.\*).

## Information

If "HOTPLUG=no" is set when the operating system is RHEL5 or RHEL6, it will not disable the PCI Hot Plug. Active maintenance of NIC (PCI cards) can be performed for the physical interface where "HOTPLUG=no" is set.

### Setup 1

**/etc/sysconfig/network-scripts/ifcfg-ethX**

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

### Setup 2

**/etc/sysconfig/network-scripts/ifcfg-ethX**

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

### Setup 3

**/etc/sysconfig/network-scripts/ifcfg-ethX**

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

**/etc/sysconfig/network-scripts/ifcfg-ethX.Y**

```
DEVICE=ethX.Y
BOOTPROTO=static
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
```

## Information

If you want to use the NIC switching mode to share the same physical connection between two virtual interfaces, one bundles physical interfaces and the other bundles tagged VLAN interfaces, you need to set up ifcfg-ethX the same as Setup 1 using the same IP address (IPADDR=) and other values. For example, if sha0 bundles eth0 and eth1, and sha1 bundles eth0.2 and eth1.2, configure ifcfg-eth0 according to ifcfg-ethX in Setup 1, not according to that shown in Setup 3.

#### Setup 4

**/etc/sysconfig/network-scripts/ifcfg-ethX**

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

**/etc/sysconfig/network-scripts/ifcfg-ethX.Y**

```
DEVICE=ethX.Y
BOOTPROTO=static
ONBOOT=yes
```

#### Setup 5

**/etc/sysconfig/network-scripts/ifcfg-ethX**

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

## (2) Verification of the physical interface

Verify if the physical interface is inserted into the system using ifconfig command.

Also, if the physical interface is UP, check whether it is marked as "RUNNING". If "RUNNING" is not displayed, the links might be down on the interface. Check the cable switch and HUB speed settings. Use the "ethtool" command to check the link state.

```
# ifconfig -a
eth0      Link encap:Ethernet  HWaddr xx:xx:xx:xx:xx:xx
          inet addr:192.168.70.2  Bcast:192.168.70.255  Mask:255.255.255.0
          inet6 addr: fe80::xxx:xxxx:xxxx:xxxx/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2140 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:22 txqueuelen:1000
          RX bytes:278285 (271.7 KiB)  TX bytes:273656 (267.2 KiB)
          Base address:0xec80 Memory:d2fc0000-d2fe0000
eth1      Link encap:Ethernet  HWaddr 0xx:xx:xx:xx:xx:xx
          inet addr:192.168.71.2  Bcast:192.168.71.255  Mask:255.255.255.0
          inet6 addr: fe80::xxx:xxxx:xxxx:xxxx/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:278492 (271.9 KiB)  TX bytes:273666 (267.2 KiB)
          Base address:0xecc0 Memory:d2fe0000-d3000000
```

In the above example, it is possible to use eth0 and eth1. For details regarding ifconfig command, refer to the Linux manual.

## Information

When using Tagged VLAN, ensure that the NIC supports tagged VLAN functionality (IEEE 802.1Q). In addition, in a Redundant Line Control function, the effective range of VLAN-ID which can be specified is from 1 to 4094.

### (3) Checking the name service

When using name services such as DNS or NIS, define keywords such as hosts 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.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Legal entries are:
#
#      nisplus or nis+      Use NIS+ (NIS version 3)
#      nis or yp            Use NIS (NIS version 2), also called YP
#      dns                 Use DNS (Domain Name Service)
#      files               Use the local files
#      db                 Use the local database (.db) files
#      compat             Use NIS on compat mode
#      hesiod              Use Hesiod for user lookups
#      [NOTFOUND=return]   Stop searching if not found so far
#
# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis
#
passwd:     files
shadow:     files
group:      files
#
#hosts:     db files nisplus nis dns
hosts:      files dns
.....
```

## Information

If the host name rather than the IP address is used in setting GLS, enable the hostname resolution function (set by hanetparam -h), which allows you to change the host name to the IP address using only the /etc/hosts file without depending on the /etc/nsswitch.conf file setting.



## (4) IPv6 RA daemon configuration

GLS supports radvd(router advertisement daemon for IPv6) for RA (router advertisement) daemon. To use IPv6(dual) on Fast switching mode, you must start RA daemon on the host running GLS in order to transmit RA from virtual interfaces. Other than this purpose, RA daemon is not necessary. The following describes configuration procedure.

### radvd configuration

1. Define the configuration in /etc/radvd.conf.

When transmitting network information (network fec0:1::, prefix length 64) from sha0 with RA(router advertisement), define the configuration description as shown below.

In addition, the difference in the version of radvd needs to define the following kernel parameters (net.ipv6.conf.all.forwarding=1) in /etc/sysctl.conf.

For details on radvd configuration, refer to radvd manual.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from
sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

2. Configure radvd to startup during system startup (when run level is 2, 3, or 5).

```
# chkconfig --level 235 radvd on
```

3. Verify radvd is configured to startup on run level 2, 3, 5.

```
# chkconfig --list radvd
radvd          0:off  1:off  2:on   3:on   4:off  5:on
6:off
```

## (5) Route configuration

Route configuration of IPv4 or IPv6 is described below.

### Default gateway configuration

Define the default gateway address (GATEWAY) in the "/etc/sysconfig/network" file.

/etc/sysconfig/network

```
GATEWAY=192.168.1.254
```

For IPv6 and NIC switching mode, configure the setting by using the user command execution function instead of the network configuration file for the operating system. In the configuration file of the user command execution function, define the operating system command assigning the route of IPv6 to be executed after activation of the IP address. For details, refer to the Linux manual (ip(6), route(8) and so on).

## Information

- The default gateway device (GATEWAYDEV) can not be configured for a physical interface bound with NIC switching mode.
- When defining the default gateway (GATEWAY) in the "/etc/sysconfig/network-scripts/ifcfg-ethX" file in the NIC switching mode, add the same configuration of GATEWAY in the configuration files of all NICs bound by GLS. Note that if different configurations of GATEWAY are defined in the "/etc/sysconfig/network" file and the "/etc/sysconfig/network-scripts/ifcfg-ethX" file, the configuration in the "/etc/sysconfig/network-scripts/ifcfg-ethX" file has a priority.

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

Name          Hostname          Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0          192.168.1.10        e                      eth1,eth2

# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
(omitted)
GATEWAY=192.168.1.254

# cat /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
(omitted)
GATEWAY=192.168.1.254
```

- If you do not use the "/etc/sysconfig/network" file in the environment where Virtual NIC mode is used, configure the route in the "/etc/sysconfig/network-scripts/ifcfg-shaX" file. You do not need to configure it in the "/etc/sysconfig/network-scripts/ifcfg-ethX" file in the same way as NIC switching mode. For details, see "[3.3.3 Virtual NIC mode](#)".

### Static route configuration

To configure a static route on a routing table, define the configuration on the "/etc/sysconfig/network-scripts/route-Interface name" file.

- NIC switching mode

Apply the same setting for both physical interfaces (route-ethX, route-ethY) bundled by NIC switching mode.

/etc/sysconfig/network-scripts/route-ethX

```
GATEWAY0=192.168.40.10
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0
```

/etc/sysconfig/network-scripts/route-ethY

```
GATEWAY0=192.168.40.10
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0
```

- Virtual NIC mode and GS linkage mode

Configure it for the virtual interface (route-shaX).

/etc/sysconfig/network-scripts/route-shaX

```
GATEWAY0=192.168.40.10
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0
```



## Information

When activating the interface on the standby side where the static route was set on startup of the operating system, the message of "RTNETLINK answers:" may be output. This is because the IP address is not set to the setting file (ifcfg-ethY) of the interface on the standby side. Ignore this message.

- Virtual interface mode and GS linkage mode

Apply the setting to virtual interfaces (route-shaX).

/etc/sysconfig/network-scripts/route-shaX

```
GATEWAY0=192.168.40.10
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0
```

## (6) IPv6 module configuration

Supporting IPv6(dual) on GLS Fast switching mode or NIC switching mode, or performing the IPv6 communication on Virtual NIC mode, it is required to load IPv6 module on Linux. See the following for configuring IPv6 module.

### Loading ipv6 module

1. Configure /etc/sysconfig/network to use IPv6. Ignore the tunneling configuration, since GLS does not support tunneling feature.

```
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

In the environment with RHEL5 or earlier, when the setting which disables IPv6 is defined in /etc/modprobe.conf, delete the setting or comment it out.

```
# alias net-pf-10 off
# alias ipv6 off
# options ipv6 disable=1
```

2. Reboot the system.

```
# /sbin/shutdown -r now
```

3. Verify IPv6 module is loaded.

```
# lsmod | grep ipv6
ipv6                662756    10
```

## (7) Tagged VLAN configuration

To use tagged VLAN interfaces in Fast switching mode, NIC switching mode, or Virtual NIC mode, set up the tagged VLANs as follows:

### Loading tagged VLAN module

1. Configure /etc/sysconfig/network to use tagged VLAN.

```
VLAN=yes
```

2. Reboot the system.

```
# /sbin/shutdown -r now
```

3. Verify tagged VLAN module is loaded.

```
# lsmod | grep 8021q
8021q                18760      1
```

## (8) Network hotplug configuration

To use GLS in RHEL5, edit the following file to deactivate the hotplug function for the virtual interface (sha). You do not need to edit the file below in RHEL6.

/etc/udev/rules.d/60-net.rules

```
SUBSYSTEM=="net", ENV{INTERFACE}=="sha*", GOTO="skipqls"
ACTION=="add", SUBSYSTEM=="net", IMPORT{program}="/lib/udev/
rename_device"
SUBSYSTEM=="net", RUN+="/etc/sysconfig/network-scripts/net.hotplug"
LABEL="skipqls"
```



When PTF of RHEL is applied, the "/etc/udev/rules.d/60-net.rules" file may return to the content before it is edited. Edit the file after application.

### 3.2.2.2 System setup in Fast switching mode

#### Common settings between IPv4 and IPv6

- To create backup of the physical interface settings (the "/etc/sysconfig/network-scripts/ifcfg-ethX" or "/etc/sysconfig/network/ifcfg-ethX" file), the file name must begin with names other than "ifcfg-".  
(e.g. bak\_ifcfg-ethX)  
If the file name begins with "ifcfg-", OS might recognize the interface as an interface to be activated during system startup.

#### When using an IPv4 address

- Define the IPv4 address (virtual IP address, physical IP address, logical virtual interface, takeover virtual IP address) and a host name in /etc/hosts file. These host names must be specified in the /etc/hosts file even if no host names but IP addresses are directly specified in environment definitions.
- Before defining a virtual interface, the physical interface you are going to apply must be in active state and be sure the IPv4 address is assigned. (When the system is RHEL, in the file /etc/sysconfig/network-scripts/ifcfg-ethX, define "ONBOOT=yes" and "IPADDR=X.X.X.X" then reboot the system.)

#### When using an IPv6 address

- Define the IPv6 address (logical virtual interface, takeover virtual IP address) and a host name in /etc/hosts file.
- Before defining a virtual interface, the physical interface you are going to apply must be in active state and be sure the IPv6 link-local address is assigned. (When the system is RHEL, in the file /etc/sysconfig/network-scripts/ifcfg-ethX, define "ONBOOT=yes" and in the /etc/sysconfig/network file, define "NETWORKING\_IPV6=yes" then reboot the system.)
- You must start the radvd daemon on 2 or more servers running as Fast switching mode in order to set the stateless address auto-configuration. Note that when starting up radvd on multiple servers, synchronize the prefix data of the virtual interfaces defined in /etc/radvd.conf between the servers. An example of setting a /etc/radvd.conf file when using a Linux server as an IPv6 router is shown below. In addition, depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on this topic, see the manual of radvd.conf(5) and radvd(8).

/etc/radvd.conf

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from
sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

- When setting stateless address auto-configuration against the physical interface (ethX) using Fast switching mode, start up radvd on either of the servers or provide IPv6 router on the same network. Additionally, stateless address auto-configuration on the physical interface (ethX) does not apply on the server that has kernel configuration (net.ipv6.conf.all.forwarding=1) for starting up radvd. In such case, after starting radvd, use sysctl command to reconfigure the kernel parameter. For details, refer to sysctl(8) manual.

```
# sysctl -w net.ipv6.conf.all.forwarding=0
```

### 3.2.2.3 System setup in NIC switching mode

#### Common settings between IPv4 and IPv6

- To create backup of the physical interface settings (the "/etc/sysconfig/network-scripts/ifcfg-ethX" or "/etc/sysconfig/network/ifcfg-ethX" file), the file name must begin with names other than "ifcfg-".  
(e.g. bak\_ifcfg-ethX)  
If the file name begins with "ifcfg-", OS might recognize the interface as an interface to be activated during system startup.

#### When using an IPv4 address

- Define the IPv4 address (virtual IP address, physical IP address, monitored IP addresses to be specified in monitoring destination information) and a host name in /etc/hosts file. These host names must be specified in the /etc/hosts file even if no host names but IP addresses are directly specified in environment definitions.
- Before booting an OS, the primary interface (physical interface) you are going to apply must in active state and make sure IPv4 address is assigned. (When the system is RHEL, in the file /etc/sysconfig/network-scripts/ifcfg-ethX, define "ONBOOT=yes" and in the /etc/sysconfig/network file, define "NETWORKING\_IPV6=yes".)  
Also, make sure the secondary interface (physical interface) is in inactive state.
- 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 a configuration file for routing daemon.

#### When using an IPv6 address

- Define the IPv6 address (takeover virtual IP address, monitored IP addresses to be specified in monitoring destination information) and a host name in /etc/hosts file.
- For communication using IPv6, use the virtual IP address defined for GLS. When using the IPv6 address assigned by stateless address auto-configuration, it will be changed according to the change of the link-local address assigned for the active NIC around the time of NIC switching.
- Before booting an OS, the primary interface (physical interface) you are going to apply must in active state and be sure IPv6 address is assigned. (When the system is RHEL, in the file /etc/sysconfig/network-scripts/ifcfg-ethX, define "ONBOOT=yes" and in the file /etc/sysconfig/network, set "NETWORKING\_IPV6=yes")  
Also, make sure the secondary interface (physical interface) is in inactive state.
- Do not set the server running NIC switching mode as an IPv6 router.

- When using IPv6 virtual interfaces in the environment where stateless address auto-configuration by an IPv6 router is not set, assign the link-local address of monitored HUB to the monitored IP.

### 3.2.2.4 System setup in Virtual NIC mode

Edit the setting (/etc/sysconfig/network-scripts/ifcfg-ethX file) for the physical interface of the GLS bundles as follows:

Table 3.9 Configuration of physical interface

Item	Value (Example)	Description
DEVICE	ethX	Specify the device name. Set to "ethX".
BOOTPROTO	static	Specify the protocol when getting the IP address. Set to "static" or "none".
HWADDR	XX:XX:XX:XX:XX:XX	Specify the MAC address of the device.
HOTPLUG	no	Specify use of hotplug. Set to "no". Set to "no".
ONBOOT	yes	Select whether to start the physical interface on startup of the operating system. Set to "yes".
DEVICETYPE	hanet	Specify the type of the device. Set to "hanet".
MTU	9000	Specify the length of MTU.  When specifying the length of MTU, set the same value for the configuration file (ifcfg-ethX) of the primary interface and the secondary interface, and for the virtual interface configuration file (ifcfg-shaX).

An example is shown below.

- Example of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=AA:AA:AA:AA:AA:AA
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

To create backup of the physical interface settings (the "/etc/sysconfig/network-scripts/ifcfg-ethX" file), the file name must begin with names other than "ifcfg-".

(e.g. bak\_ifcfg-ethX)

If the file name begins with "ifcfg-", OS might recognize the interface as an interface to be activated during system startup.



#### Point

- For the physical interfaces bundled by GLS, do not specify "TYPE=Ethernet". Otherwise, GLS will not work properly.
- IPADDR and other addresses are not required, so do not make any settings.
- Specify the HWADDR and "ONBOOT=yes" to avoid renaming the device on startup of the operating system.
- Set HWADDR to the unique MAC address of the NIC.
- For the ifcfg-ethX configuration of the physical interfaces bundled in the GLS virtual interface, add the item "DEVICETYPE=hanet".

### 3.2.2.5 System setup in GS linkage mode

- If you use "HWADDR=XX:XX:XX:XX:XX:XX" in the setting (the /etc/sysconfig/network-scripts/ifcfg-ethX file) for the physical interface of the GLS bundles, add the "HOTPLUG=no" setting.
- To create backup of the physical interface settings (the "/etc/sysconfig/network-scripts/ifcfg-ethX" or "/etc/sysconfig/network/ifcfg-ethX" file), the file name must begin with names other than "ifcfg-".

(e.g. bak\_ifcfg-ethX)

If the file name begins with "ifcfg-", OS might recognize the interface as an interface to be activated during system startup.

- Define the IPv4 address (virtual IP address, physical IP address, logical virtual interface, takeover virtual IP address) and a host name in /etc/hosts file. These host names must be specified in the /etc/hosts file even if no host names but IP addresses are directly specified in environment definitions.
- Before defining a virtual interface, the physical interface you are going to apply must be in active state and be sure the IPv4 address is assigned. (When the system is RHEL, in the file /etc/sysconfig/network-scripts/ifcfg-ethX, define "ONBOOT=yes" and "IPADDR=X.X.X.X" then reboot the system.)
- Be sure to define the virtual gateway in the /etc/sysconfig/network-scripts/route-shaX file to set the static route information.
- You do not need to configure the routing daemon for the network setting when using this method.

### 3.2.3 Setting up the system log

---

Operation history of the interface up/down in NIC switching mode can be output as a system log message. Since this message is output at the INFO level, the following setting is needed:

[Setting file]

- For RHEL5  
/etc/syslog.conf
- For RHEL6  
/etc/rsyslog.conf

[Settings]

When enabling message output, add "\*.info" information to the setting file.

In this setting, messages are output to the system log.

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none    /var/log/
messages

# The authpriv file has restricted access.
authpriv.*                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                    /var/log/
maillog
```

When disabling message output, delete "\*.info" information from the setting file.

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
mail.none;authpriv.none;cron.none    /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                /var/log/secure

# Log all the mail messages in one place.
```

mail.* maillog	/var/log/
-------------------	-----------

#### [Setting notification]

After changing the setting file of the system log, obtain the super-user rights and then restart the system log daemon as shown below:

- For RHEL5

```
# /etc/init.d/syslog restart
```

- For RHEL6

```
# /etc/init.d/rsyslog restart
```

#### [Others]

For details about how to set the system log, see the system online manuals. Because line monitor error messages 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.  
INFO: 91080: link up detected: the physical interface link is up.  
WARNING: 91180: link down detected: the physical interface link is down.  
INFO: 91280: link up detected: the virtual interface link is up.  
INFO: 91480: the physical interface of the virtual interface was switched.

## 3.3 Additional system setup

This section describes additional setup procedure for setting up the system. Note that if there is an active virtual interface, perform the change distribution procedures such as a system reboot according to "[3.4 Changing system setup](#)" after adding a setting.



### 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 to add 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. Setup a subnet mask to a virtual IP address using the "hanetmask create" command. For information, see "[7.5 hanetmask Command](#)".
2. 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 "[7.1 hanetconfig Command](#)".



### 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 subnet mask to a virtual IP address using the "hanetmask create" command. For information, see "[7.5 hanetmask Command](#)".
2. Set up a virtual interface using the "hanetconfig create" command. For information, see "[7.1 hanetconfig Command](#)".
3. Set up the standby patrol function using the "hanetconfig create" command (only if the standby patrol function is used). For information, see "[7.1 hanetconfig Command](#)".
4. Set up the HUB monitoring function using the "hanetpoll create" command. For information, see "[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 a 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 a HUB monitoring function with "hanetpoll copy" command. See "[7.7 hanetpoll Command](#)" for the detail.



#### Note

- When setting the definition information of NIC switching mode, if virtual interfaces of the other NIC switching modes are already working, already working, it is necessary to stop them once to make the added information valid. Therefore, deactivate GLS temporarily using "stphanet" command and then execute "strhanet" command to restart it. In cluster operation, reactivate a userApplication of NIC switching mode.
- In NIC switching mode, physical interfaces are activated or deactivated when switching over the transfer path. However, these logs might not be recorded according to the state of the definition. Please refer to "[3.2.3 Setting up the system log](#)" for the method of recording these logs.
- In the cluster environment other than physical IP takeover II, ensure to specify the same IP address configured in "/etc/sysconfig/network-scripts/ifcfg-ethX" when specifying physical IP address by "hanetconfig" command using '-i' or '-e' option. If you specify different physical IP address, it disturbs communication using physical interface because this IP address will overwrite the physical IP address specified with "hanetconfig" command when activating the virtual interface. Do not set any value to IPADDR (IP address) in ifcfg-ethX in the cluster environment with physical IP takeover II.
- 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 "[F.3.3 Switching takes place in NIC switching mode regardless of failure at the monitoring end](#)".
- It only has to set only one standby patrol function at the composition to which two or more virtual interfaces bundle the same physical interface when tagged VLAN interface is used.
- When tagged VLAN interface is used, it is not possible to compose like sharing only one from among the bundled physical interface.

### 3.3.3 Virtual NIC mode

---

The following shows the procedure to add configuration information.

1. Set up a virtual interface using the "hanetconfig create" command. For information, see "[7.1 hanetconfig Command](#)".
2. Edit the interface setting file of the virtual interface to set the IP address or netmask.

The interface setting file of the virtual interface is created when the virtual interface is set by the "hanetconfig create" command.

3. Setup the monitoring destination information by using the "hanetpathmon target" command. For details, see "[7.12 hanetpathmon Command](#)".

#### Configuration of virtual interface

Edit the setting (/etc/sysconfig/network-scripts/ifcfg-shaX file) for a virtual interface as follows:

Item	Value (Example)	Description
DEVICE	shaX	Specify the device name. Set to "ethX".
IPADDR	192.168.1.1	Specify the IP address.
NETMASK	255.255.255.0	Specify the subnet mask.
PREFIX	24	Set either NETMASK or PREFIX.
NETWORK	192.168.1.0	Specify the network address. Omit this step if PREFIX is specified.
BROADCAST	192.168.1.255	Specify the broadcast address. Omit this step if PREFIX is specified.
BOOTPROTO	static	Specify the protocol when getting the IP address. Set to "static" or "none".
ONBOOT	yes	Select whether to start the virtual interface on startup of the operating system. Set to "yes". When the virtual interface is registered as cluster resource, it is started regardless of the value during the system startup.
DEVICETYPE	sha	Specify the type of the device. Set to "sha".
HOTPLUG	no	Specify use of hotplug. Set to "no".
GATEWAY	192.168.2.1	Specify the IP address when setting the default gateway.
IPV6INIT	yes	Specify "yes" when assigning the IPv6 address.
IPV6ADDR	fec0:1::1/64	Specify the IPv6 address.
IPV6_DEFAULTGW	fec0:1::2	Specify the IPv6 address when setting the default gateway of IPv6.
BRIDGE	br0	Specify the name of the virtual bridge which is to be connected to the virtual interface.
MTU	9000	Specify the length of MTU. When specifying the length of MTU, set the same value for the configuration file (ifcfg-ethX) of the primary interface and the secondary interface, and for the virtual interface configuration file (ifcfg-shaX).
SHAMACADDR	XX:XX:XX:XX:XX:XX	Specify the MAC address.  - If specifying the MAC address The specified address is set.  - If specifying "auto" A local address is automatically created.

Example of /etc/sysconfig/network-scripts/ifcfg-sha0

[For IPv4]

```
DEVICE=sha0
IPADDR=192.168.1.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

[For IPv6]

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fec0:1::1/64
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

[For DualStack]

```
DEVICE=sha0
IPADDR=192.168.1.1
NETMASK=255.255.255.0
IPV6INIT=yes
IPV6ADDR=fec0:1::1/64
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

[When using a local address created automatically and IPv4 for the MAC address]

```
DEVICE=sha0
IPADDR=192.168.1.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
SHAMACADDR=auto
```

When creating a tagged VLAN interface (shaX.Y) of which VLAN-ID is Y on a virtual interface (shaX), edit the setting file (/etc/sysconfig/network-scripts/ifcfg-shaX.Y) for a tagged VLAN interface as follows. The effective range of VLAN-ID which can be specified is from 1 to 4094.

/etc/sysconfig/network-scripts/ifcfg-eth0.2

[For IPv4]

```
DEVICE=sha0.2
IPADDR=192.168.100.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

[For IPv6]

```
DEVICE=sha0.2
IPV6INIT=yes
IPV6ADDR=fec0:100::1/64
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

[For DualStack]

```
DEVICE=sha0.2
IPADDR=192.168.100.1
NETMASK=255.255.255.0
```

```
IPV6INIT=yes
IPV6ADDR=fec0:100::1/64
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

## Note

- In Virtual NIC mode, you cannot share physical interfaces with other virtual interfaces.
- Just as for the standard interface of the operating system, define IP address and netmask settings in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) in Virtual NIC mode. Subnet mask settings by the hanetmask command are only necessary when the cluster takeover IP address is set by the hanethvrsc command.
- For implementing tagged VLAN communication in Virtual NIC mode, generate a tagged VLAN interface on the virtual interface. The procedure for generation is the same as for the standard tagged VLAN interface of the operating system.
- Do not delete a file or change a file name for the interface setting file of the virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX). If you change or delete a file name, the interface setting file is omitted from the backup target when you back up configuration files by the "hanetbackup" command.
- Directly edit the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) for a virtual interface and the setting file (/etc/sysconfig/network-scripts/ifcfg-shaX.Y) for a tagged VLAN interface by using an editor such as vi. You cannot make any settings by using the network configuration function provided by GUI or other interfaces of the operating system.
- When using the virtual NIC mode on a guest OS in VMware, specify the MAC address or "auto" to SHAMACADDR.
- Set [Accept] for [Promiscuous Mode] under [Security] for each virtual switch in VMware.
- When using the virtual NIC mode on a VMware guest OS, a tagged VLAN interface is not usable. For a tagged VLAN connection, set the VLAN ID for a port group of VMware.
- Specifying with SHAMACADDR is applied only to the virtual interface. Not applied to the physical interface.
- Do not use MACADDR that is a standard configuration item of the operating system.
- SHAMACADDR cannot be used for the configuration file for a tagged VLAN interface (ifcfg-shaX.Y).
- In Virtual NIC mode, the bonding interface (bondX) can be bundled. To do so, pay attention to the following points:
  - Specify the MAC address or "auto" to SHAMACADDR.
  - A link down may not be detected depending on the bonding specification. Make sure to set the monitoring target IP.
  - When using mode=4(802.3ad), set its switch so that untagged LACPDU can be transmitted.
  - A tagged VLAN interface is not available.
  - ARP monitoring for bonding is not available.
- When configuring the logical virtual interface (shaX:Y), do not set "DEVICETYPE=sha" for the configuration file (ifcfg-shaX:Y).

## 3.3.4 GS linkage mode

The following shows the procedure to add configuration information.

1. Setup a subnet mask to a virtual IP address using the "hanetmask create" command. For information, see "[7.5 hanetmask Command](#)".
2. Create a virtual interface using "hanetconfig create" command. For information, see "[7.1 hanetconfig Command](#)".
3. Configure the remote host monitoring information by using the hanetobserv create command. For details, see "[7.15 hanetobserv Command](#)". To change the monitoring interval and monitoring count for the remote host, use the hanetobserv param command.
4. Configure the virtual gateway information by using the hanetgw create command. For details, see "[7.14 hanetgw Command](#)".

### 3.3.5 Setting parameter for individual mode

See the following procedure for using a value different from the default value indicated in section ["3.1.2.5 Configuration of individual mode"](#).

1. Use "hanetparam" command and "hanetpoll on" command for setting up the common 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/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 ["7.20 resethanet Command"](#).

### 3.4.1 Fast switching mode

This section describes how to change the settings for Fast switching mode. After changing the settings, you need to reflect the changes in the operations following some procedures. Note that the distribution procedures vary depending on the command used for changing the settings, and whether the settings were changed in a single system configuration (no cluster is used), or in a cluster configuration.

#### Distribution procedure

hanetconfig command	Single	Cluster
IP address to be assigned for the virtual interface (-i)	1	2
Virtual Interface (-n) (newly added)	1	2
Physical interface (-t)	1	2

hanethvrsc command	Single	Cluster
Takeover virtual ip address (-i)	-	2

hanetmask command	Single	Cluster
Subnet mask (-m)	1	1

hanetparam command	Single	Cluster
Transfer path monitoring interval (-w)	3	3
The number of constant monitoring prior to outputting message (-m)	3	3
The number of constant monitoring prior to switching cluster (-l)	-	2

hanetparam command	Single	Cluster
Switching cluster immediately after starting (-c)	-	2
Outputting message (-s)	3	3
Hostname resolution (-h)	3	3

Network configuration of OS	Single	Cluster
Network configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX, /etc/sysconfig/network), hosts file(/etc/hosts) etc.	4	4

#### Procedure 1

Perform one of the following procedures after changing settings.

- Deactivate and then activate the target virtual interface.
- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 2

Perform one of the following procedures after changing settings.

- Reboot the system.
- Execute the "resethanet -s" command.

#### Procedure 3

Changed settings are immediately reflected in operations after executing the command to change settings. No distribution procedure is required.

#### Procedure 4

If you modified the network configuration file for the operating system, you must reboot the system instead of manually restarting the network service (/etc/init.d/network restart, service network restart).

### Changing Procedure

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

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

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 ["7.1 hanetconfig Command"](#) or ["7.5 hanetmask 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
- Subnet mask to a virtual interface or a logical virtual interface

- Monitoring function information

Use the "hanetparam" command to change the following information. For information, see ["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

### [Example 1]

The following shows the procedure for changing the virtual IP address of a virtual interface in operation.

1. Check the setting.

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

Name	Hostname	Mode	Physical	ipaddr	Interface List
sha0	192.168.100.10	t			eth1,eth2
sha1	192.168.101.10	t			eth1,eth2

2. Deactivate the target interface. To change the virtual IP address for sha0, deactivate the virtual interface of sha0.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
```

3. Change the monitoring destination.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.100.11
```

4. Distribute the changes. Because the "IP address of a virtual/physical interface" was changed in the single configuration, perform the "deactivate and then activate the target virtual interface" procedure or "reboot the system" procedure, or "execute the resethanet -s command" procedure according to Procedure 1. The following is an execution example in which the "deactivate and then activate the target virtual interface" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 3.4.2 NIC switching mode

This section describes how to change the settings for NIC switching mode. After changing the settings, you need to reflect the changes in the operations following some procedures. Note that the change distribution procedures vary depending on the command used for changing the settings, and whether the settings were changed in a single system configuration (no cluster is used), or in a cluster configuration.

### Distribution Procedure

hanetconfig command	Single	Cluster
IP address to be assigned for the virtual or physical interface (-i, -e)	1	2
Virtual interface (-n)	1	2
Physical interface (-t)	1	2
Name of the virtual interface monitored by the standby patrol (-t)	1	2

hanetmask command	Single	Cluster
Subnet mask (-m)	5	5

hanetparam command	Single	Cluster
Standby patrol monitoring period (-m)	4	4
The number of constant standby monitoring (-p)	4	4
Hostname resolution (-h)	4	4

hanetpoll command	Single	Cluster
a monitor-to ip address (-p)	1	2
Setting of HUB-to-HUB monitoring function (-b)	1	2
Monitoring period (-s)	3	3
The number of monitoring (-c)	3	3
Cluster switching (-f)	-	3
Link up waiting period (-p)	3	3
Link status monitoring (-l)	3	3

Network configuration of OS	Single	Cluster
Network configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX, /etc/sysconfig/network), hosts file(/etc/hosts) etc.	6	6

### Procedure 1

Perform one of the following procedures after changing settings.

- Deactivate and then activate all the virtual interfaces in NIC switching mode.
- Reboot the system
- Execute the resethanet -s command.

### Procedure 2

Perform one of the following procedures after changing settings.

- Reboot the system.
- Execute the resethanet -s command.

### Procedure 3

Perform one of the following procedures after changing settings.

- Deactivate and then activate monitoring.



- Deactivate and then activate all the virtual interfaces.
- Reboot the system
- Execute the resethanet -s command.

#### Procedure 4

Changed settings are immediately reflected in the operations after executing the command to change settings. No distribution procedure is required.

#### Procedure 5

Perform one of the following procedures after changing settings.

- Deactivate and then activate the target virtual interface.
- Deactivate and then activate all the virtual interfaces.
- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 6

If you modified the network configuration file for the operating system, you must reboot the system instead of manually restarting the network service (/etc/init.d/network restart, service network restart).

### Changing Procedure

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 common parameter. (For changing monitoring period, the number of monitoring times, recovery monitoring period, cluster switching and link up period, apply changes with "hanetpoll on" command.)  
See "[7.7 hanetpoll Command](#)" for the detail.
4. Deactivate temporarily all virtual interfaces set in NIC switching mode using a "stphanet" command, then reactivate them using a "strhanet" command. See "[7.2 strhanet Command](#)" and "[7.3 stphanet Command](#)" for the detail.
5. Starts a function to monitor HUB using a "hanetpoll on" command.  
(For changing monitoring period, the number of monitoring times, recovery monitoring period, cluster switching and link up period, apply changes with "hanetpoll on" command)  
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 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. 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
- Subnet mask to a virtual interface, a logical virtual interface or a physical interface

- Standby patrol information

Use the "hanetconfig" command to change the following information. For information, see "7.1 hanetconfig Command".

- Interface names to be bundled by a virtual interface

- Information of monitored remote system and common parameters

Use the "hanetpoll" command to change the following information. For information, see "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
- Recovery monitoring period
- Link status monitoring
- Cluster switching
- Link up waiting time

Use the "hanetparam" command to change the following information. For information, see "7.6 hanetparam Command".

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



## Note

- In the cluster environment other than physical IP takeover II, ensure to specify the same IP address configured in "/etc/sysconfig/network-scripts/ifcfg-ethX" when specifying physical IP address by "hanetconfig" command using '-i' or '-e' option. If you specify different physical IP address, it disturbs communication using physical interface because this IP address will overwrite the physical IP address specified with "hanetconfig" command when activating the virtual interface. Do not set any value to IPADDR (IP address) in ifcfg-ethX in the cluster environment with physical IP takeover II.
- 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.

## [Example 1]

The following shows the procedure for changing the monitoring destination of a virtual interface in single system operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol / Virtual NIC]
Name      Hostname      Mode Physical ipaddr      Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.10.100 d    192.168.10.10 eth1,eth2
sha1      192.168.10.101 d    192.168.10.10 eth1,eth2
# /opt/FJSVhanet/usr/sbin/hanetpoll print
```

```

Polling Status      = ON
interval(idle) = 5( 60) sec
time               = 5 times
repair_time       = 5 sec
link detection     = NO
FAILOVER Status    = YES
Name      HUB Poll Hostname
+-----+-----+-----+-----+
sha0      OFF   192.168.10.250,192.168.10.251
sha1      OFF   192.168.10.250,192.168.10.251

```

## 2. Stop HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

## 3. Deactivate the target interface. To change the monitoring destinations of sha0 and sha1, deactivate the virtual interfaces of sha0 and sha1.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
# /opt/FJSVhanet/usr/sbin/stphanet -n sha1
```

## 4. Change the monitoring destination.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha0 -p
192.168.10.150,192.168.10.251
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha1 -p
192.168.10.150,192.168.10.251
```

## 5. Distribute the changes. Because the "IP address of the HUB monitoring destination" was changed in a single system configuration, perform the "deactivate and then activate all the virtual interfaces in NIC switching mode" procedure or "reboot the system" procedure, or "execute the resethanet -s command" procedure according to Procedure 1. The following is an execution example in which the "deactivate and then activate all the virtual interfaces in NIC switching mode" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/stphanet
# /opt/FJSVhanet/usr/sbin/strhanet
```

## 6. Restart the stopped HUB monitoring. Note that if you performed a reboot or executed the resethanet command, you do not need to perform the following procedure because the monitoring is restarted automatically when GLS reboots.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```



## Point

You need to specify the same monitoring destinations for the monitoring destinations of all virtual interfaces sharing the same NIC. Therefore, change all the monitoring destinations at once when changing them.

## [Example 2]

The following shows the procedure for changing the virtual IP address of a virtual interface in cluster operation.

### 1. Check the setting

```

# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol / Virtual NIC]
Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+-----+
sha0      192.168.10.100    d   192.168.10.10   eth1,eth2
sha1      -                 p   -               sha0

```

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4      takeover-ipv6      logical ip address list
+-----+-----+-----+-----+
sha0:65     192.168.10.100      -                  -
```

2. Stop the cluster operation and delete the setting for GLs resources from cluster applications.

3. Stop HUB monitoring and the standby patrol.

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

4. Delete the setting for the takeover virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n sha0:65
```

5. Change the virtual IP address.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.10.101
```

6. Set the takeover virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

7. Create the GLs resource setting on cluster applications.

8. Distribute the changes. Because the "IP address of a virtual/physical interface" was changed in a cluster configuration, perform a "reboot the system" procedure or "execute the resethanet -s command" procedure according to Procedure 2. The following is an execution example in which the system is rebooted.

```
# /sbin/shutdown -r now
```

### [Example 3]

The following shows the procedure for changing the monitoring destination of a virtual interface in cluster operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
[IPv4,Patrol / Virtual NIC]
Name      Hostname      Mode Physical ipaddr      Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.10.100      d   192.168.10.10      eth1,eth2
sha1      -                  p   -                  sha0

# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = ON
interval(idle) =    5( 60) sec
time                =    5 times
repair_time         =    5 sec
link detection      = NO
FAILOVER Status     = YES
Name      HUB Poll Hostname
+-----+-----+-----+-----+
sha0      OFF   192.168.10.250,192.168.10.251
```

2. Stop the cluster operation.

3. Stop HUB monitoring and the standby patrol.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
# /opt/FJSVhanet/usr/sbin/stpptl -n sha1
```

4. Change the monitoring destination.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha0 -p
192.168.10.150,192.168.10.251
```

5. Distribute the changes. Because the "IP address of the HUB monitoring destination" was changed in a cluster configuration, perform a "reboot the system" procedure, or "execute the resethanet -s command" procedure according to Procedure 2. The following is an execution example in which the system is rebooted.

```
# /sbin/shutdown -r now
```

#### [Example 4]

The following shows the procedure for changing the HUB monitoring interval during single system or cluster operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = ON
interval(idle)     = 5( 60) sec
time               = 5 times
repair_time        = 5 sec
link detection      = NO
FAILOVER Status     = YES
Name      HUB Poll Hostname
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
s sha0      OFF    192.168.10.250,192.168.10.251
```

2. Change the monitoring interval.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on -s 3
```

3. To change the monitoring interval, perform a "deactivate and then activate monitoring" procedure or "deactivate and then activate all the virtual interfaces" procedure or "reboot the system" procedure, or "execute the resethanet -s command" procedure. The following is an execution example in which the "deactivate and then activate monitoring" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 3.4.3 Virtual NIC mode

This section describes how to change the settings for Virtual NIC mode. After changing the settings, you need to reflect the changes in the operations following some procedures. Note that the change distribution procedures vary depending on the command used for changing the settings, and whether the settings were changed in a single system configuration (no cluster is used), or in a cluster configuration.

#### Distribution Procedure

Network configuration file of virtual interface	Single	Cluster
/etc/sysconfig/network-scripts/ifcfg-shaX	1	1

hanetpathmon command	Single	Cluster
Monitored IP (target -p)	2	3
Monitored IP VLAN (target -v)	2	3

hanetpathmon command	Single	Cluster
Automatic start of monitoring (param -a)	2	3
Monitoring period (param -s)	2	3
The number of monitoring (param -c)	2	3
The number of recovery monitoring (param -r)	2	3
Link up waiting period (param -p)	2	3
Automatic fail-back (param -q)	2	3
Failover (param -f)	None	3

hanethvrsc command	Single	Cluster
Takeover virtual IP address (-i)	None	4

hanetparam command	Single	Cluster
Link down detection timer (-q)	4	4
Link up detection timer (-r)	4	4
Link status monitoring standby timer (-g)	4	4

Network configuration file of OS	Single	Cluster
Network configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX, /etc/sysconfig/network, /etc/hosts) etc.	5	5

#### Procedure 1

Perform one of the following procedures after changing settings.

- Activate the target virtual interface.
- Reboot the system

#### Procedure 2

Perform one of the following procedures after changing settings.

- Enable the monitoring (activating).
- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 3

Perform one of the following procedures after changing settings.

- Enable the monitoring (activating).
- Reboot the system

#### Procedure 4

Changed settings are immediately reflected in the operations after changing settings. No distribution procedure is required.

#### Procedure 5

If you modified the network configuration file for the operating system, you must reboot the system instead of manually restarting the network service (/etc/init.d/network restart, service network restart).

## Changing Procedure

The following shows the procedure for changing configuration information. Changes become effective by performing distribution procedures.

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

The following shows the procedure for changing information of network monitoring. Changes become effective by performing distribution procedures.

1. Stop network monitoring with the hanetpathmon off command.
2. Change the monitoring target with the hanetpathmon target command.  
Change the following monitoring parameters with the hanetpathmon param command:

- Automatic start of monitoring
- Monitoring period
- The number of monitoring
- The number of recovery monitoring
- Link up waiting period
- Automatic fail-back
- Cluster switching

3. Start network monitoring with the hanetpathmon on command.

For details, see "[7.12 hanetpathmon Command](#)".

The following shows the procedure for changing link status monitoring parameters. Changes become effective by performing distribution procedures.

1. Change the following link status monitoring parameters with the hanetparam command:
  - Link down detection timer
  - Link up detection timer
  - Link status monitoring standby timer

For details, see "[7.6 hanetparam Command](#)".

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

- Configuration definition information

You can change the information such as IP addresses and a subnet mask by editing the network setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) of the virtual interface. For details, see "[3.3.3 Virtual NIC mode](#)".

- Network monitoring information

The following information can be changed with the hanetpathmon command. For details, see "[7.12 hanetpathmon Command](#)".

- Monitored IP (primary monitored remote system IP address and secondary monitored remote system IP address)
- Monitored IP VLAN (primary monitored remote system IP address and secondary monitored remote system IP address)
- Automatic start of monitoring
- Monitoring period
- The number of monitoring
- The number of recovery monitoring

- Link up waiting period
- Automatic fail-back
- Cluster switching (failover)
- Information of link status monitoring parameter

The following information can be changed with the hanetparam command. For details, see "[7.6 hanetparam Command](#)".

- Link down detection timer
- Link up detection timer
- Link status monitoring standby timer

## Note

If a virtual bridge is connected to a virtual interface of the Virtual NIC mode, the virtual interface cannot be deactivated. Deactivate it after disconnecting the virtual interface from the virtual bridge.

### [Example 1]

The following shows the procedure for changing the monitoring target and monitoring period of network monitoring during single system or cluster operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target
[Target List]
Name      VID  Target
+-----+-----+-----+
sha0      -   192.168.10.250,192.168.10.251

# /opt/FJSVhanet/usr/sbin/hanetpathmon param
[Parameter List]
Name      Monitoring Parameter
+-----+-----+-----+
sha0      auto_startup      =    yes
          interval        =     3 sec
          times            =     5 times
          repair_times     =     2 times
          idle             =    45 sec
          Auto fail-back   =     no
          FAILOVER Status  =     yes
```

2. Stop network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon off
```

3. Change the monitoring target and monitoring period.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p
192.168.10.150,192.168.10.251
# /opt/FJSVhanet/usr/sbin/hanetpathmon param -n sha0 -s 5
```

4. Check the changed setting.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target
[Target List]
Name      VID  Target
+-----+-----+-----+
```



```

sha0      -      192.168.10.150,192.168.10.251

# /opt/FJSVhanet/usr/sbin/hanetpathmon param
[Parameter List]
Name      Monitoring Parameter
+-----+-----+-----+-----+
sha0      auto_startup      =      yes
          interval          =      5 sec
          times              =      5 times
          repair_times       =      2 times
          idle               =      45 sec
          Auto fail-back     =      no
          FAILOVER Status    =      yes

```

5. Distribute the changes. Perform the "enable the monitoring (activating)" procedure, "reboot the system" procedure, or "execute the resethanet -s command (in the single configuration)" procedure according to Procedure 2 or 3. The following is an execution example in which the "enable the monitoring (activating)" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon on
```

## [Example 2]

The following shows the procedure for changing the virtual IP address for a virtual interface in single system operation.

1. Check the virtual interface.

```

# /sbin/ifconfig sha0
sha0      Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
          inet addr:192.168.80.10  Bcast:192.168.80.255  Mask:255.255.255.0
          inet6 addr: fe80::XXXX:XXXX:XXXX:XXXX/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:372 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1314 errors:0 dropped:11 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30500 (29.7 KiB)  TX bytes:124151 (121.2 KiB)

```

2. Check the status of the virtual interface.

```

# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
sha0      Active    v    OFF  eth1(ON),eth2(OFF)
[IPv6]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+

```

3. Deactivate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
```

4. Check the status of the virtual interface.

```

# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
sha0      Inactive    v    OFF  eth1(OFF),eth2(OFF)
[IPv6]

```

Name	Status	Mode	CL	Device
+-----+-----+-----+-----+-----+				

5. Edit the network setting file of the virtual interface to change the IP address.

Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

6. Distribute the changes. Because the "network setting file of the virtual interface" was changed, perform the "activate the target virtual interface" procedure or "reboot the system" procedure according to Procedure 1. The following is an execution example in which the "activate the target virtual interface" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

7. Check the status of virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status    Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active    v    OFF  eth1(ON),eth2(OFF)
[IPv6]
Name      Status    Mode CL  Device
+-----+-----+-----+-----+-----+
```

8. Check the virtual interface.

```
# /sbin/ifconfig sha0
sha0      Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
          inet addr:192.168.80.1  Bcast:192.168.80.255  Mask:255.255.255.0
          inet6 addr: fe80::XXXX:XXXX:XXXX:XXXX/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:7 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:4505 (4.3 KiB)
```

### [Example 3]

The following shows the procedure for changing the virtual interface connected to the virtual bridge during the operation process in a virtual machine environment.

1. Check the virtual interface connected to the virtual bridge.

```
# /usr/sbin/brctl show
bridge name      bridge id                STP enabled    interfaces
br0              8000.*****             no             sha0
```

2. Check the status of the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status    Mode CL  Device
```

```
+-----+-----+-----+-----+
sha0      Active    v    OFF  eth1(ON),eth2(OFF)
sha1      Active    v    OFF  eth3(ON),eth4(OFF)
[IPv6]
Name      Status    Mode CL  Device
+-----+-----+-----+-----+
```

3. Disconnect the virtual interface from the virtual bridge.

```
# /usr/sbin/brctl delif br0 sha0
```

4. Check the status of the virtual bridge.

```
# /usr/sbin/brctl show
bridge name      bridge id                STP enabled    interfaces
br0              8000.000000000000        no
```

5. Deactivate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
# /opt/FJSVhanet/usr/sbin/stphanet -n sha1
```

6. Check the status of the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status    Mode CL  Device
+-----+-----+-----+-----+
sha0      Inactive  v    OFF  eth1(OFF),eth2(OFF)
sha1      Inactive  v    OFF  eth3(OFF),eth4(OFF)
[IPv6]
Name      Status    Mode CL  Device
+-----+-----+-----+-----+
```

7. Edit the network setting file of the virtual interface.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

Delete "BRIDGE=br0" and add "IPADDR", "NETMASK", and similar statements related to the IP address.

[Before modification]

```
DEVICE=sha0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
BRIDGE=br0
```

[After modification]

```
DEVICE=sha0
IPADDR=192.168.80.10
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha1

Delete "IPADDR", "NETMASK", and similar statements related to the IP address and add "BRIDGE=br0".

[Before modification]

```
DEVICE=sha1
IPADDR=192.168.81.10
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

[After modification]

```
DEVICE=sha1
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
BRIDGE=br0
```

8. Distribute the changes. Because the "network setting file of the virtual interface" was changed, perform the "activate the target virtual interface" procedure or "reboot the system" procedure according to Procedure 1. The following is an execution example in which the "activate the target virtual interface" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0
# /opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

Changed virtual interface is connected to the virtual interface by activating the virtual interface.

9. Check the status of the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active  v    OFF  eth1(ON),eth2(OFF)
sha1      Active  v    OFF  eth3(ON),eth4(OFF)
[IPv6]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
```

10. Check the virtual interface connected to the virtual bridge.

```
# /usr/sbin/brctl show
bridge name      bridge id                STP enabled    interfaces
br0              8000.*****             no             sha1
```

#### [Example 4]

The following shows the procedure for changing the takeover virtual IP for the virtual interface in cluster operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4    takeover-ipv6    vlan-id/logical ip address list
+-----+-----+-----+-----+-----+
sha0:65     192.168.20.102  -                -
```

2. Stop the cluster operation. Also delete the setting for GLs resources from cluster applications.
3. Delete the virtual interface once, and then reconfigure it.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n sha0:65
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.10.101
```

4. Check the setting after reconfiguring.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4      takeover-ipv6      vlan-id/logical ip address list
+-----+-----+-----+-----+
sha0:65     192.168.10.101      -                  -
```

5. Distribute the changes. Because the "takeover IP address" was changed, no distribution procedure is required according to Procedure 4.
6. Create the GLs resource setting on cluster applications.
7. Start the cluster operation.

### [Example 5]

The following shows the procedure for changing the virtual IP address for a virtual interface in cluster operation.

1. Stop the cluster operation.
2. Check the virtual interface.

```
# /sbin/ifconfig sha0
sha0      Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
          inet addr:192.168.20.20  Bcast:192.168.80.255  Mask:255.255.255.0
          inet6 addr: fe80::XXXX:XXXX:XXXX:XXXX/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:372 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1314 errors:0 dropped:11 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30500 (29.7 KiB)  TX bytes:124151 (121.2 KiB)
```

3. Check the status of the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
sha0      Active    v    ON   eth1(ON),eth2(OFF)
[IPv6]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
```

4. Deactivate the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
```

5. Edit the network setting file of the virtual interface to change the IP address.

Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.20.10
NETMASK=255.255.255.0
BOOTPROTO=static
```

```
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

6. Distribute the changes. Because the "network setting file of the virtual interface" was changed, perform the "activate the target virtual interface" procedure or "reboot the system" procedure according to Procedure 1. The following is an execution example in which the "activate the target virtual interface" procedure is used.

```
# /opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

7. Check the status of the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
sha0      Active    v    ON   eth1(ON),eth2(OFF)
[IPv6]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
```

8. Check the virtual interface.

```
# /sbin/ifconfig sha0
sha0      Link encap:Ethernet  HWaddr XX:XX:XX:XX:XX:XX
          inet addr:192.168.20.10  Bcast:192.168.80.255  Mask:255.255.255.0
          inet6 addr: fe80::XXXX:XXXX:XXXX:XXXX/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:7 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:4505 (4.3 KiB)
```

9. Start the cluster operation.

### 3.4.4 GS linkage mode

This section describes how to change the settings for GS linkage mode. After changing the settings, you need to reflect the changes in the operations following some procedures. Note that the change distribution procedures vary depending on the command used for changing the settings, and whether the settings were changed in a single system configuration (no cluster is used), or a cluster configuration.

#### Reflection Procedure

hanetconfig command	Single	Cluster
IP address to be assigned for the virtual (-i)	1	2
Virtual interface (-n)	1	2
Physical interface (-t)	1	2

hanetgw command	Single	Cluster
IP address for the virtual gateway (-g)	1	2

hanethvsrc command	Single	Cluster
Gateway address for the takeover virtual interface (-e)	-	2

hanetmask command	Single	Cluster
Subnet mask. (-m)	1	1

hanetoberv command	Single	Cluster
Virtual IP address of the communication target (-i)	3	2
Physical IP address of the communication target (-t)	3	2
Monitoring period (-s)	4	4
The number of monitoring (-c)	4	4
Monitoring period for recovery (-b)	4	4
Cluster switching (-f)	-	4
Link up waiting period (-p)	4	4

hanetparam command	Single	Cluster
Hostname resolution (-h)	4	4

Network configuration of OS	Single	Cluster
Network configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX, /etc/sysconfig/network), hosts file(/etc/hosts) etc.	5	5

#### Procedure 1

Perform one of the following procedures after changing settings.

- Deactivate and then activate the target virtual interface.
- Deactivate and then activate all the virtual interfaces in GS linkage mode.
- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 2

Perform one of the following procedures after changing settings.

- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 3

Perform one of the following procedures after changing settings.

- Deactivate and then activate all the virtual interfaces in GS linkage mode.
- Reboot the system.
- Execute the resethanet -s command.

#### Procedure 4

Changed settings are immediately reflected to the operation after executing the command to change settings. No reflection procedure is required.

## Procedure 5

If you modified the network configuration file for the operating system, you must reboot the system instead of manually restarting the network service (/etc/init.d/network restart, service network restart).

## Changing Procedure

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

1. Inactivate the target 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 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 "hanetobserv" command to change the following information. For information, see Section "[7.15 hanetobserv 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 "[7.15 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 information  
Use the "hanetgw" command to change the following information. For information, see Section "[7.14 hanetgw Command](#)".
  - Virtual interface
  - Virtual IP information (Virtual gateway)

## [Example 1]

The following shows the procedure for changing the IP address of the communication target of the virtual interface in cluster operation.

1. Check the setting.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)          = 5 sec
times(c)             = 5 times
idle(p)              = 60 sec
repair_time(b)        = 5 sec
fail over mode(f)     = YES
Destination Host Virtual Address    (Router Address+)NIC Address
```



+-----+-----+-----+-----+-----+-----+					
GS	192.168.110.10	192.168.10.10,192.168.20.10			
		<u>192.168.10.11,192.168.20.11</u>			
PQ	192.168.100.20	192.168.10.20,192.168.20.20			

2. Stop the cluster operation.
3. Change the IP address of the communication target.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n GS -i 192.168.110.10
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.20,192.168.20.20
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.21,192.168.20.21
```

4. Distribute the changes. Because the "IP address of the remote host monitoring" was changed in a cluster configuration, perform a "reboot the system" procedure, or "execute the resethanet -s command" procedure according to Procedure 2. The following is an execution example in which the system is rebooted.

```
# /sbin/shutdown -r now
```

### 3.4.5 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 "resethanet" command to delete the entire configured values of the virtual interface for Redundant Line Control function. For details on "resethanet" command, refer to "7.20 resethanet Command".

### 3.5.1 Fast switching mode

The following shows the procedure for deleting configuration information:

1. Inactivate the target virtual interface using the "stphanet" command. For information, see "7.3 stphanet Command".
2. Delete the configuration information of the target virtual interface. For information, see "7.1 hanetconfig Command".
3. Delete the subnet mask information of the target virtual interface using the "hanetmask delete" command. For information, see "7.5 hanetmask Command".

### 3.5.2 NIC switching mode

The following shows the procedure for deleting configuration information:

1. Stop the HUB monitoring function using the "hanetpoll off" command. For information, see ["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 "stpctl" command (only when using a standby patrol function). For information, see ["7.3 stphanet Command"](#) and ["7.11 stpctl Command"](#).
3. Delete the concerned monitoring destination information. For information, see ["7.7 hanetpoll Command"](#).
4. Delete the configuration information of the target virtual interface. For information, see ["7.1 hanetconfig Command"](#).
5. Delete the subnet mask information of the target virtual interface using the "hanetmask delete" command. For information, see ["7.5 hanetmask Command"](#).
6. Reboot the system.

### 3.5.3 Virtual NIC mode

---

The following shows the procedure for deleting configuration information:

1. Inactivate the target virtual interface using the "stphanet" command. For information, see ["7.3 stphanet Command"](#).
2. Delete the configuration information of the target virtual interface. For information, see ["7.1 hanetconfig Command"](#).

### 3.5.4 GS linkage mode

---

The following shows the procedure for deleting configuration information:

1. Inactivate the target virtual interface using the "stphanet" command. For information, see Section ["7.3 stphanet Command"](#).
2. Delete virtual gateway information. For information, see Section ["7.14 hanetgw Command"](#).
3. Delete the monitoring destination information of the concerned communication parties. For information, see Section ["7.15 hanetobserv Command"](#).
4. Delete the configuration information of the target virtual interface. For information, see Section ["7.1 hanetconfig Command"](#).
5. Delete the subnet mask information of the target virtual interface using the "hanetmask delete" command. For information, see ["7.5 hanetmask Command"](#).
6. Delete the route information for the virtual gateway defined in the /etc/sysconfig/network-scripts/route-"interface name" file.
7. Delete the host name defined as the /etc/hosts file.
8. Reboot the system.

### 3.5.5 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 takeover IP resource via "hanethvrsc create" command. In order to delete the virtual interface, use "hanethvrsc delete" command first to delete the takeover IP resource that is created with the target virtual interface, and then issue "hanetconfig delete" command to delete the virtual interface. Refer to ["7.17 hanethvrsc Command"](#) for the deletion method of a resource for a virtual interface.
- If deleting all configuration information at once, use "resethanet" command. See ["7.20 resethanet Command"](#) for detail.

## 3.6 Configuring interfaces

---

### 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 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".

## 3.6.3 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 "7.1 hanetconfig Command".

### GS linkage mode in a cluster configuration

When taking over the logical virtual IP address assigned to the logical virtual interfaces (shaX:2 to 64) of GS linkage mode, it is necessary to set the parameter (logical\_vip\_takeover) beforehand. In this case, perform the following procedure.

#### 1) Setting up the parameter

Add the setting of "logical\_vip\_takeover 1" to ctld.param. After that, restart the operating system and make the setting enabled.

/etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
# Each entry is of the form:
#
# <param> <value>
#
observ_msg      0
observ_polling_timeout  180
max_node_num    4
logical_vip_takeover  1      <- Added
```

#### 2) Setting up logical virtual interfaces

Set the same logical virtual IP address between active and standby nodes for the logical virtual interfaces (shaX:2 to 64). Also, set the virtual interface where the logical virtual IP address is set to takeover interface (shaX:65) of clusters.

Example of setting up active nodes

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.210.202
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:3 -i 192.168.210.203
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig print
(Omitted..)
```

Example of setting up standby nodes

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.210.202
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:3 -i 192.168.210.203
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
# /opt/FJSVhanet/usr/sbin/hanetconfig print
(Omitted..)
```



### Information

When setting up the communication target monitoring, it is not necessary to set a logical virtual IP address with the -i option of the hanetobserv command as a setting to monitor other nodes of PRIMECLUSTER. For the following examples, the settings for "192.168.210.202" and "192.168.210.203" are not necessary.

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

Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.210.200  c                eth3,eth4
sha0:2    192.168.210.202
sha0:3    192.168.210.203

# /opt/FJSVhanet/usr/sbin/hanetobserv print
(Omitted)
Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+-----+
HOST-B      192.168.210.200  192.168.10.90,192.168.20.90
            192.168.210.202  192.168.10.90,192.168.20.90 <- Not necessary
            192.168.210.203  192.168.10.90,192.168.20.90 <- Not necessary
```

### 3.6.4 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 ["7.1 hanetconfig Command"](#).

### 3.6.5 Transfer route multiplexing with Tagged VLAN interface

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



#### Note

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



#### See

If you use tagged VLAN interfaces on GLS, configure network. See ["3.2.2 Network configuration"](#).

#### 3.6.5.1 Operating tagged 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 3.2 Fast switching mode with tagged VLAN interface](#) illustrates bundled tagged VLAN architecture.



#### Note

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.

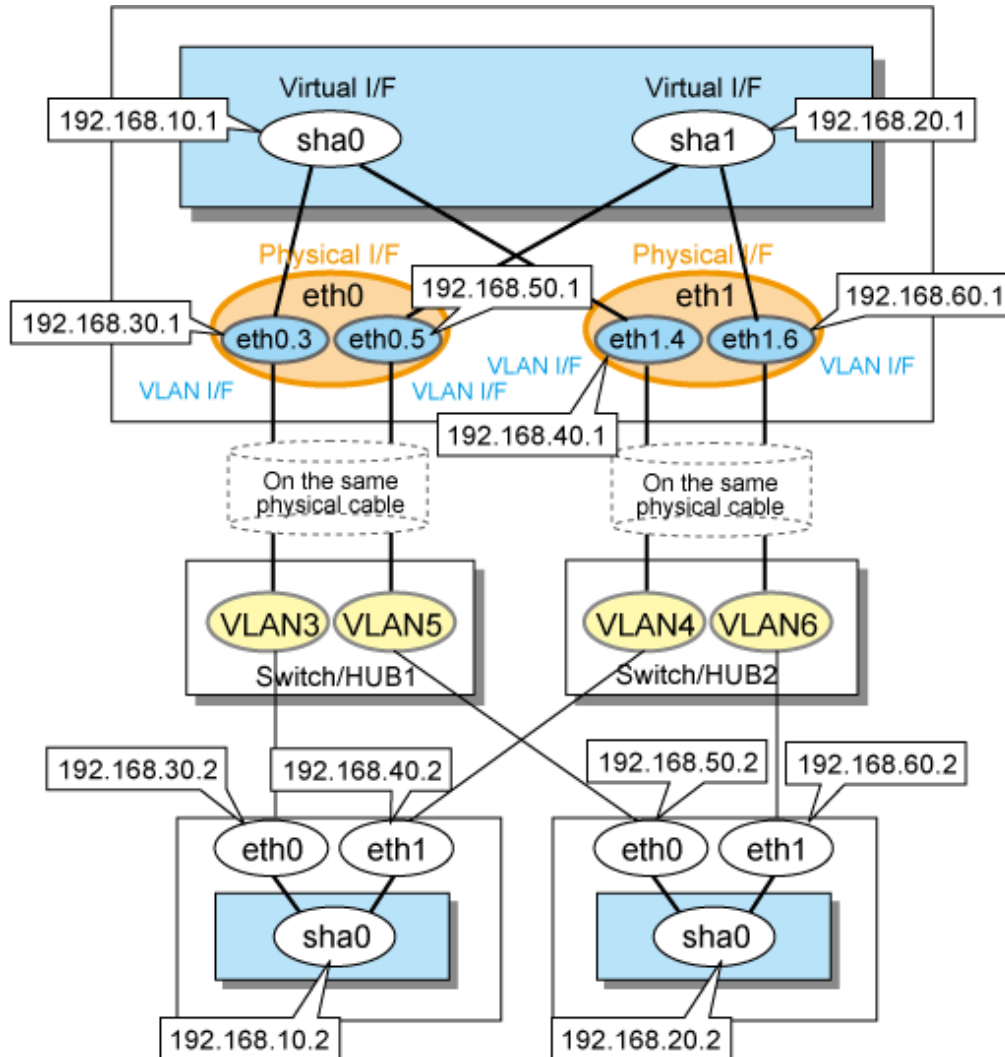


#### See

Refer to ["7.1 hanetconfig Command"](#) for configuring an interface bundled with Fast switching mode.

[Figure 3.2 Fast switching mode with tagged VLAN interface](#) illustrates an example of using tagged VLAN interface on Fast switching mode.

Figure 3.2 Fast switching mode with tagged VLAN interface



### 3.6.5.2 Operating tagged 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 "synchronous switching" or "asynchronous switching" operation is defined. Below, operation of "synchronous switching" and "asynchronous switching" is explained.

Table 3.10 Synchronous switching and asynchronous switching

Redundant network methods		Switchover	
		Synchronous	Asynchronous
NIC switching mode (Logical IP takeover)	IPv4	Enabled	Enabled
	IPv6	Enabled	Enabled
	Dual	Enabled	Enabled
NIC switching mode (Physical IP takeover)	IPv4	Disabled	Enabled

See

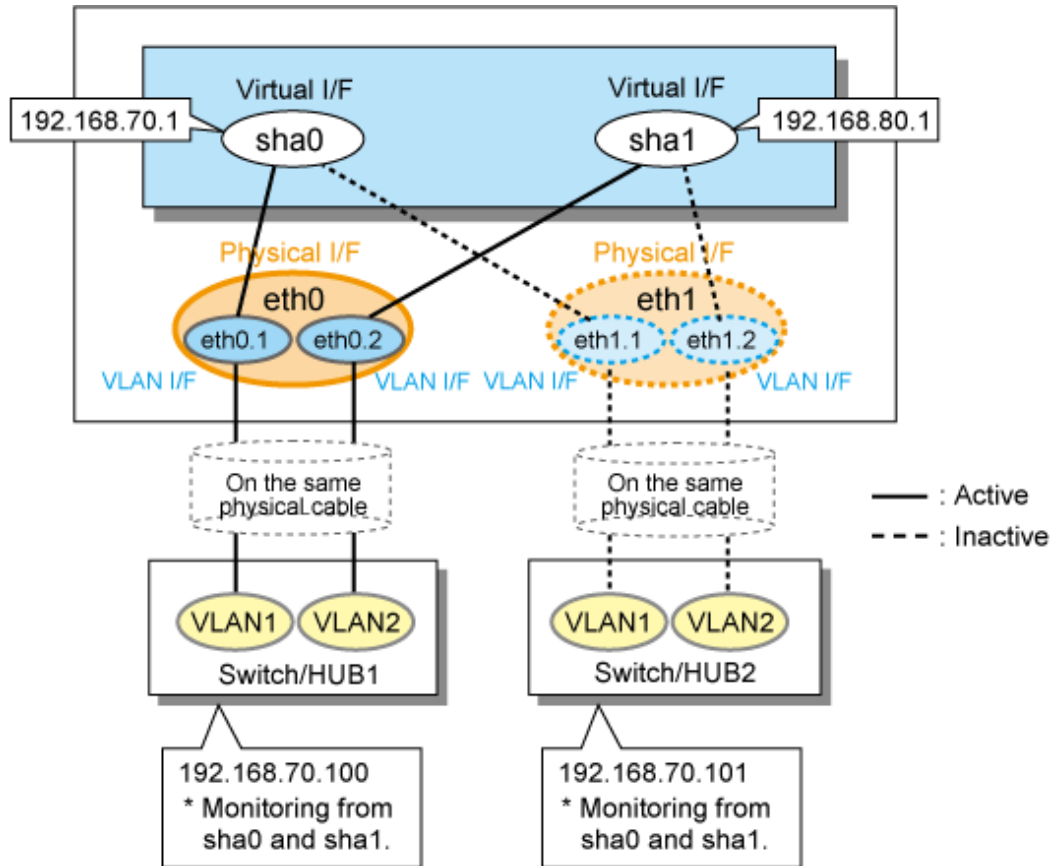
For configuration of monitoring target, refer to "7.7 hanetpoll Command".

## Synchronous switching

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 switch/HUB of a monitoring target has only one IP address, "synchronous switching" of a virtual interface is chosen.

Figure 3.3 NIC switching mode with tagged VLAN interface (synchronous switching) illustrates of synchronous switching architecture.

Figure 3.3 NIC switching mode with tagged VLAN interface (synchronous switching)



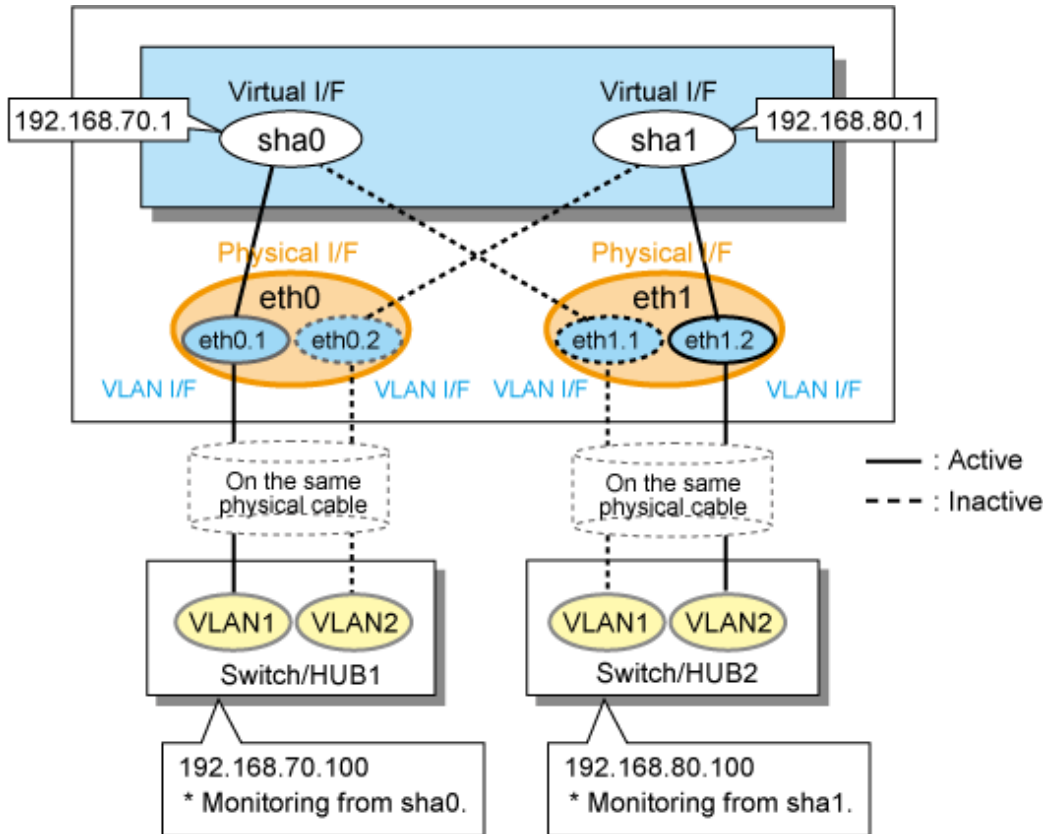
In the above figure, sha0 and sha1 of the network interfaces monitor the same IP address. If a transmission route failure is detected on sha0, virtual interface switching of sha1 as well as sha0 will occur,

## Asynchronous switching

Two or more virtual interfaces that bundle the tagged VLAN interface can be asynchronously switched. 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 are possible to switch/HUB used as a monitoring target, the asynchronous switching of the virtual interfaces is chosen to use Standby NIC effectively.

Figure 3.4 NIC switching mode with tagged VLAN interface (asynchronous switching) illustrates of asynchronous switching architecture.

Figure 3.4 NIC switching mode with tagged VLAN interface (asynchronous switching)



In the above figure, sha0 and sha1 of the network interfaces monitor the different IP addresses respectively. If a transmission route failure is detected on sha0, and virtual interface switching of sha0 occurs, that of sha1 will not occur.

### 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 "eth0.1" and "eth1.1", and similarly, another virtual interface (sha1) is created on "eth1.2" and "eth0.2", 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 "eth0.1" and "eth1.1", and another virtual interface is created on a pair of VLAN interfaces "eth1.2" and "eth2.2" because the physical interface "eth1" is the only shared physical interface here.
- If you specify two monitoring targets with synchronous 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 the physical IP address takeover function of the NIC switching mode is used, a virtual interface cannot be synchronous switched.
- If you want to share physical connections between a virtual interface bound to physical interfaces and a virtual interface bound to tagged VLAN interfaces, you cannot use asynchronous switching mode. Use synchronous switching mode.
- If you want to share physical connections between a virtual interface bound to physical interfaces and a virtual interface bound to tagged VLAN interfaces, set the standby patrol for each virtual interface. For example, as shown below, if the virtual interface sha0 uses "eth0" and "eth1," and the virtual interface sha1 uses "eth1.2" and "eth0.2", set the standby patrol (sha2 and sha3) for both virtual interfaces.

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

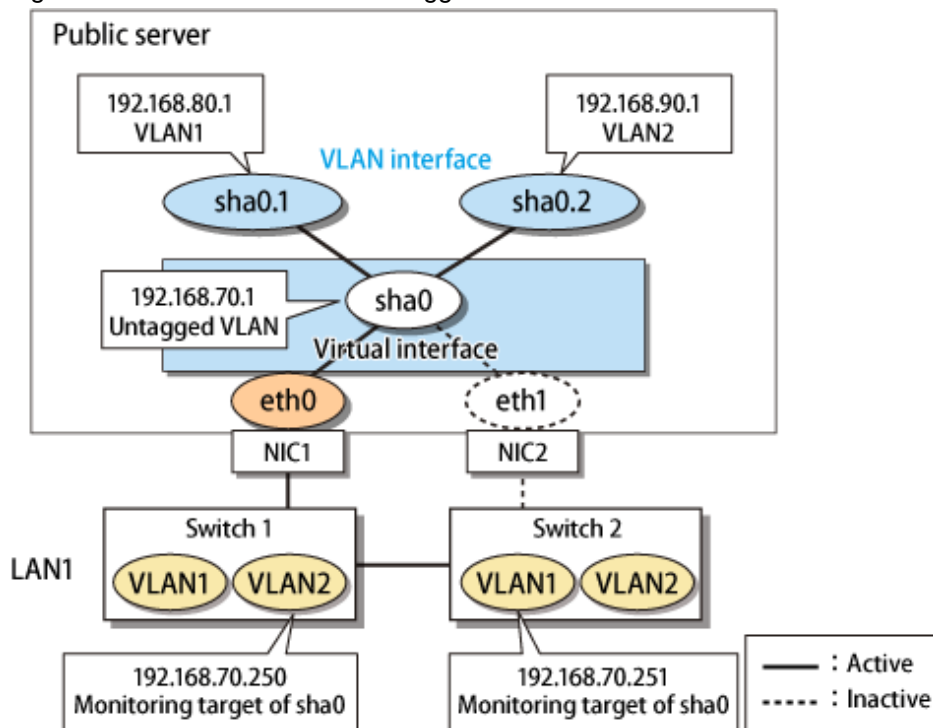
Name	Hostname	Mode	Physical	ipaddr	Interface List
sha0	192.168.10.110	d	192.168.10.10	eth0,eth1	
sha1	192.168.12.110	d	192.168.12.10	eth0.2,eth1.2	
sha2	-	p	-	sha0	
sha3	-	p	-	sha1	

### 3.6.5.3 Operating tagged VLAN interface on Virtual NIC mode

In Virtual NIC mode, you can generate a tagged VLAN interface on the virtual interface for communication. It is also possible to mix tagged and untagged communication.

The following [Figure 3.5 Virtual NIC mode with tagged VLAN interface](#) shows an example.

Figure 3.5 Virtual NIC mode with tagged VLAN interface



#### Note

You cannot bundle tagged VLAN interfaces (`ethX.Y`, `VLANX` etc.) in Virtual NIC mode.

## 3.7 Setting monitoring function of Fast switching mode

### 3.7.1 Communication target monitoring function

#### 3.7.1.1 Setting the monitoring destination information

Monitoring destinations are selected automatically. Therefore, no setting is required.

#### 3.7.1.2 Setting the monitoring interval

Specify the monitoring interval. To do this, use the "hanetparam" command. For information on how to specify the monitoring interval, see ["7.6 hanetparam Command"](#).



### 3.7.1.3 Setting the message output when a monitoring error occurs

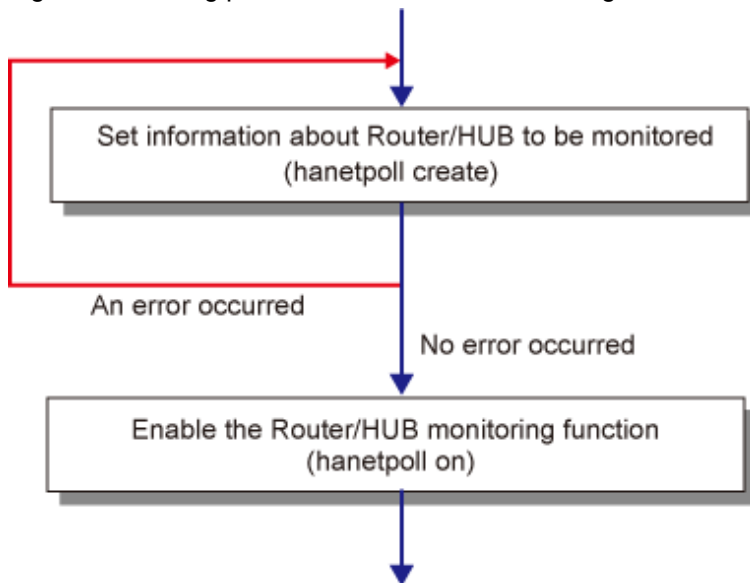
Specify the number of times that a target monitor must fail before the error message is sent. To do this, use the "hanetparam" command. For information on how to do this, see "7.6 hanetparam Command".

## 3.8 Setting monitoring function of NIC switching mode

### 3.8.1 HUB monitoring

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



#### 3.8.1.1 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".

#### 3.8.1.2 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 until the link up wait time (IDLE (seconds) in [Figure 3.7 Basic sequence of HUB monitoring](#)) passes even if the ping command fails. 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 router 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

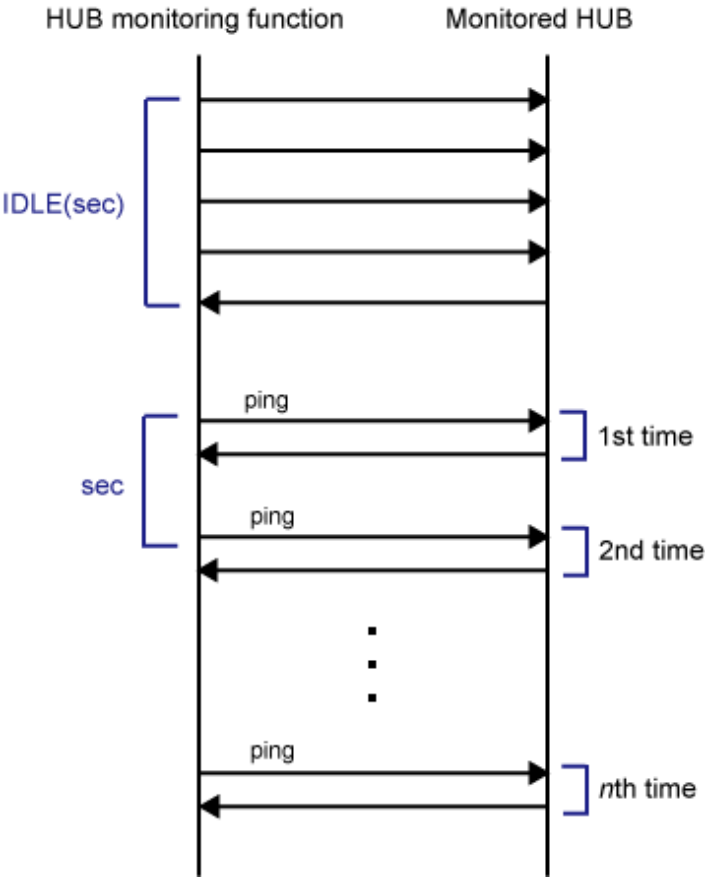
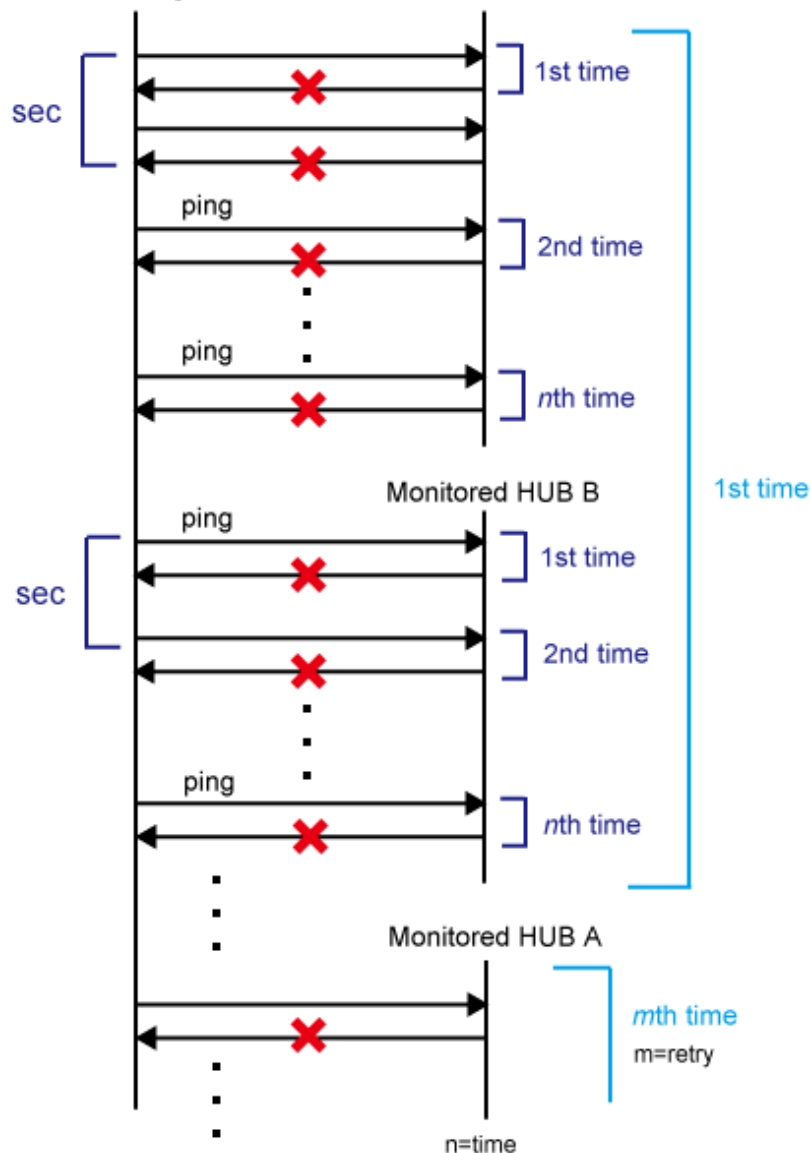


Figure 3.8 HUB monitoring sequence after detect line fault  
HUB monitoring function      Monitored HUB A



### 3.8.1.3 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 following are examples of the case of one monitoring target and two monitoring targets both using HUB-to-HUB monitoring feature.

#### One monitoring target:

Error detection time = monitoring interval (in seconds) X (monitoring frequency - 1) + ping time out period(\*1) + (0 to monitoring interval (in seconds))

\*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 time - 1) + 2 sec + 0 to 5 sec = 22 to 27 sec

#### Two monitoring targets:

```
Error detection time = monitoring interval(in seconds) X (monitoring frequency - 1) + ping time out period (*2) x 2 (0 to monitoring interval(in seconds))
```

\*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.

$$5 \text{ sec} \times (5 \text{ time} - 1) + 2 \text{ sec} \times 2 \text{ time} + 0 \text{ to } 5 \text{ sec} = 24 \text{ to } 29 \text{ sec}$$

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

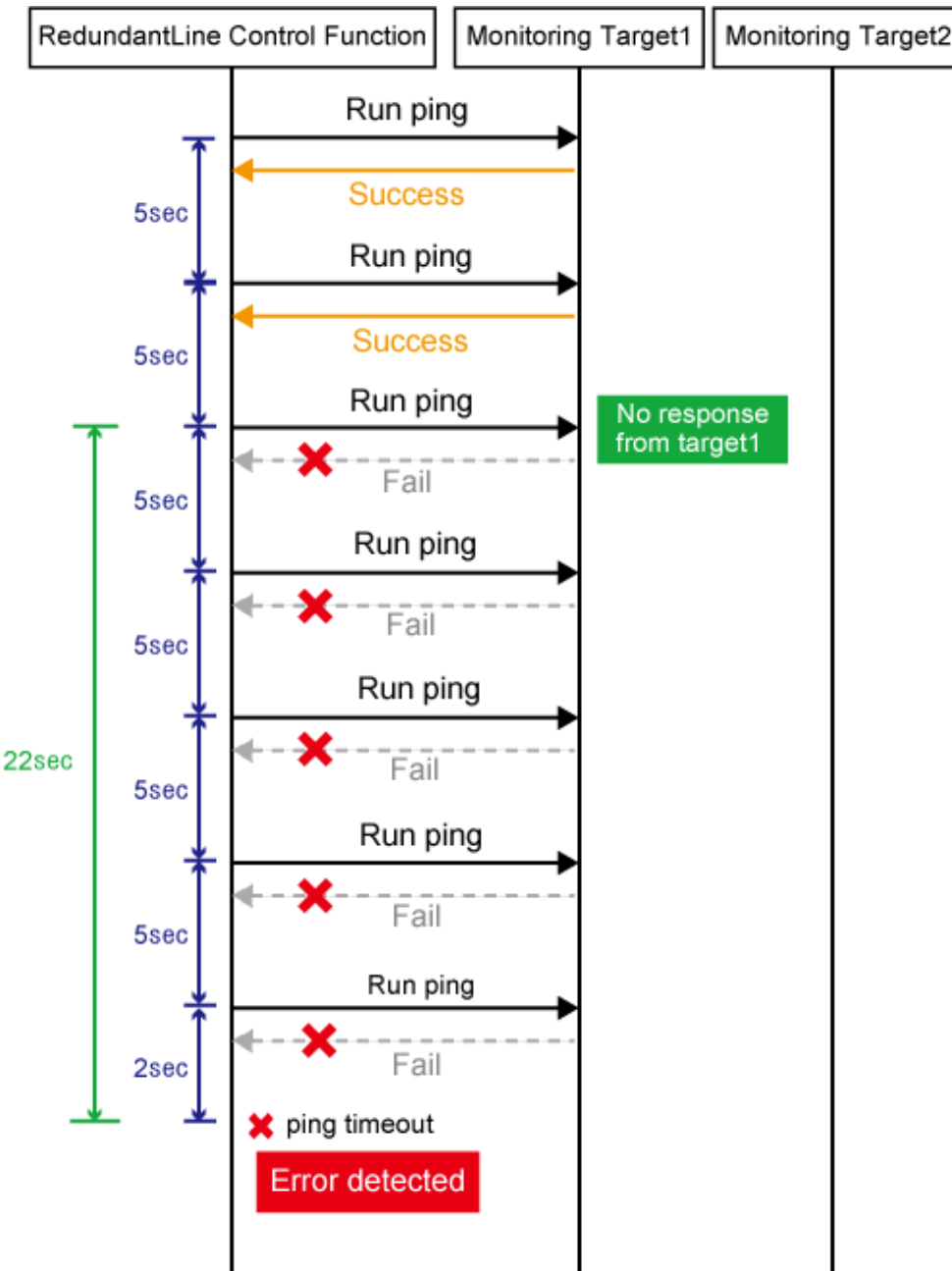
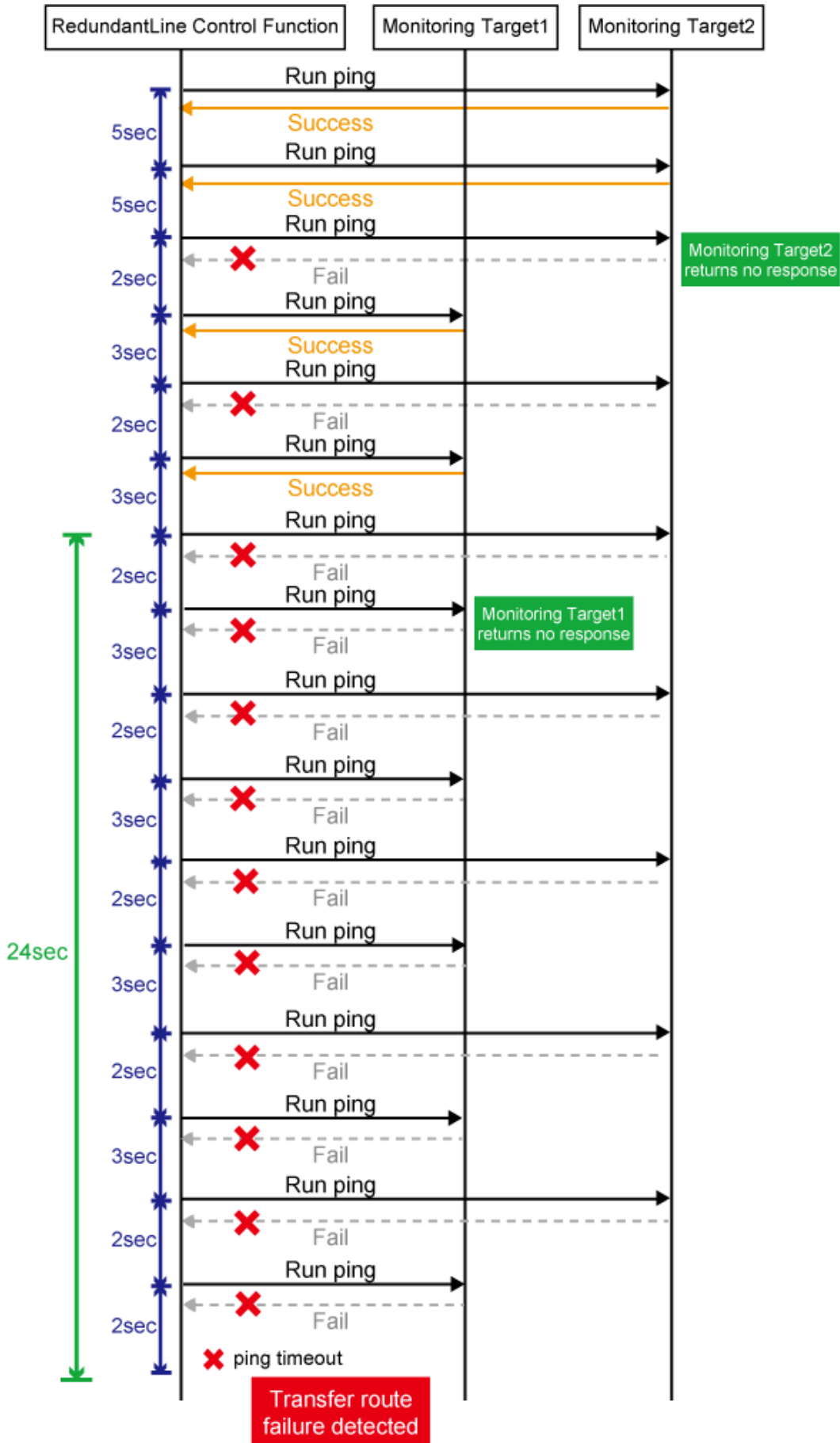


Figure 3.10 Transfer path error detection sequence (two monitoring target)



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 target:

Error detection time = ping time out period(\*3) + (0 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 sec + 0 to 5 sec = 2 to 7sec

### Two monitoring targets:

Error detection time = ping time out period (\*4) x 2 (0 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 sec x 2 time + 0 to 5 sec = 4 to 9 sec

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

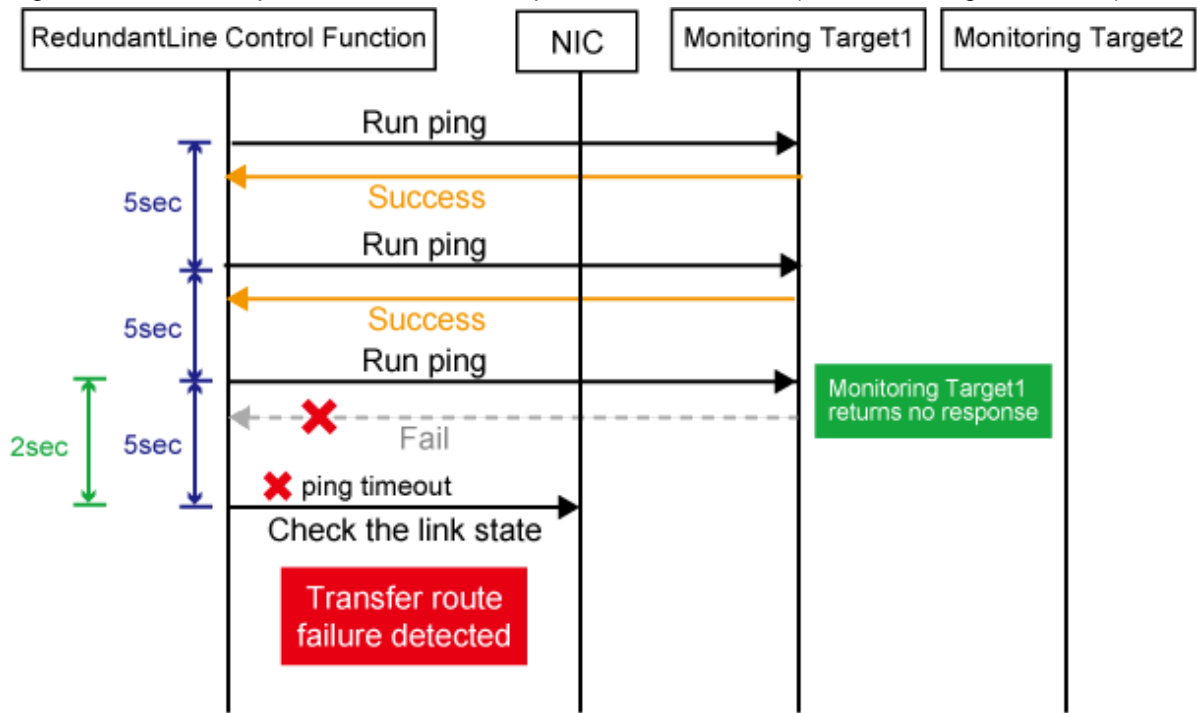
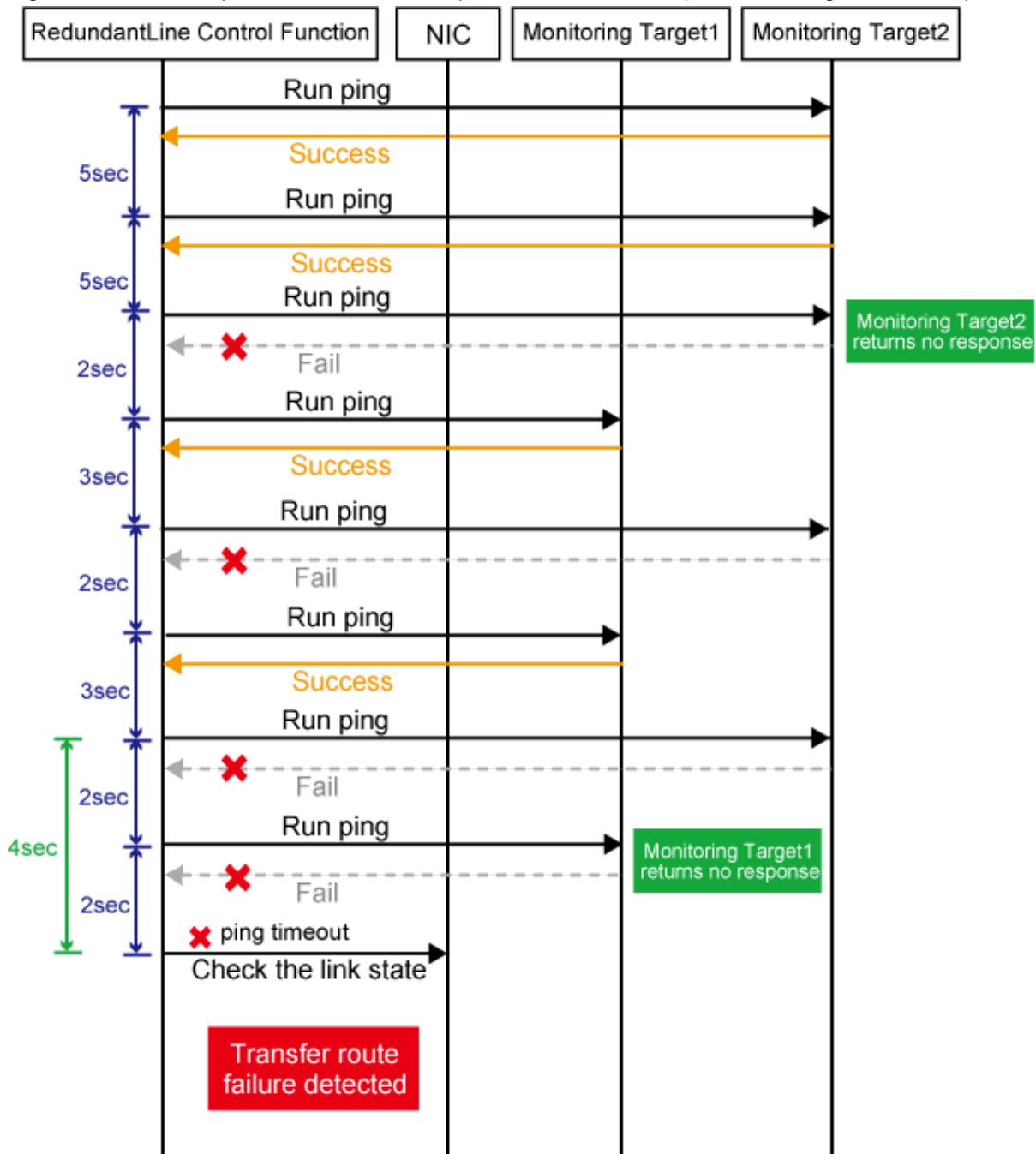


Figure 3.12 Transfer path error detection sequence with link down (two monitoring destinations)



### 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 pended until the waiting time for linkup elapses.
- In an environment where GLS is used on the host OS of the virtual machine function, 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 OS 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.

## 3.8.2 Standby patrol function

### 3.8.2.1 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 fail-back function when a primary interface is recovered using a standby patrol function. Use the "hanetconfig" command to set it. See "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.

### 3.8.2.2 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".

### 3.8.2.3 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".

## 3.8.3 Setting parameters for each virtual interface

In NIC switching mode, you can set the monitoring count and monitoring interval for each virtual interface. You can also set whether to perform a failover if a network failure occurs. Note that you cannot set parameters for each virtual interface in other modes.

Table 3.11 Available option functions in each mode

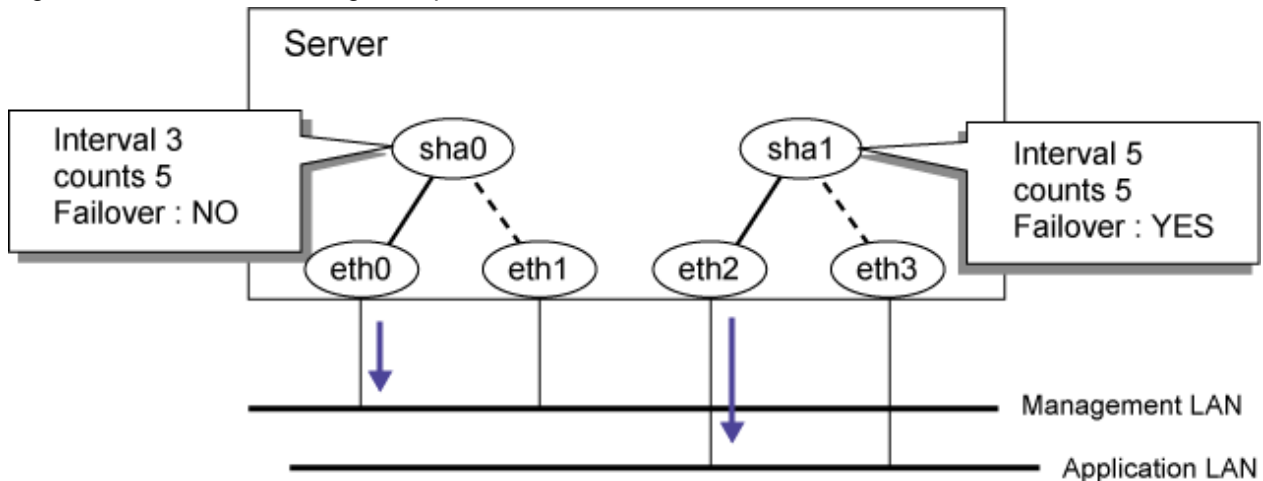
Function	Mode		
	Fast switching mode	NIC switching mode	GS linkage mode
Setting parameters for each virtual interface	X	A	X

[Meaning of the symbols] A: Allowed, X: Not allowed

Using this function allows you to determine the time it will take for a network error to be detected on each LAN and the behavior of the cluster as follows.

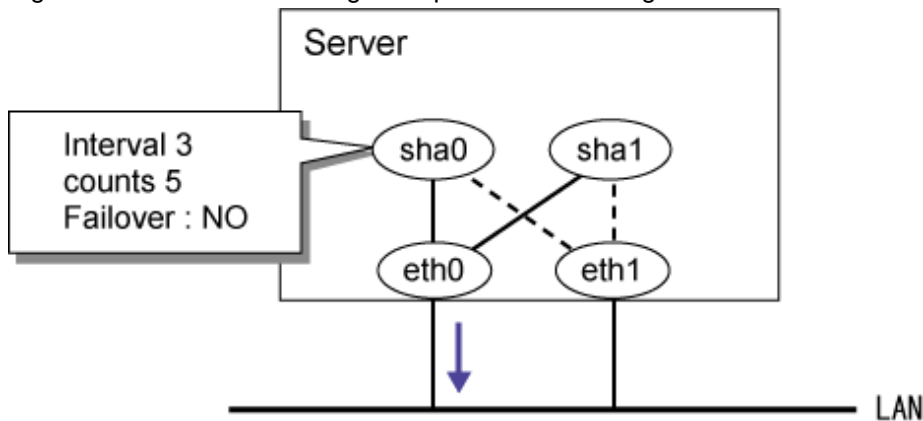


Figure 3.13 Parameter setting example for each virtual interface



Note that if NICs are shared, the settings of the virtual network interface that you made first are used. In the case of the following example, even if individual parameters have been set for sha1, the settings of sha0 that you made first will be used.

Figure 3.14 Parameter setting example for NIC sharing



The settings are made as follows. For more details, see ["7.7 hanetpoll Command"](#).

1. Set parameters by using the "hanetpoll" command after setting the ping monitoring destination. Note that the current state value will be set for any parameter options that are not set. In the following example, the monitoring count (-c) and others are not specified, so the entire parameter value (default: five times) will be set.

```
/opt/FJSVhanet/usr/sbin/hanetpoll devparam -n sha0 -s 3
```

2. Check individual parameters

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam
[ Standard Polling Parameter ]
Polling Status      = ON
  interval(idle)    = 5( 60) sec
    time            = 5 times
  repair_time       = 5 sec
  link detection     = NO
FAILOVER Status     = YES

[ Polling Parameter of each interface ]
Name  intvl idle  time  repar  link  Fover
+-----+-----+-----+-----+-----+-----+
sha0   3      60    5     5     NO    YES
```

3. Execute the "hanetpoll" command to delete them.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam -d -n sha0
```

4. Check that the individual parameters have been deleted. Note that corresponding individual parameters will be deleted if you use the "hanetpoll delete" command to delete the settings of the monitoring destination.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam
[ Standard Polling Parameter ]
Polling Status      = ON
    interval(idle) = 5( 60) sec
    time           = 5 times
    repair_time    = 5 sec
    link detection = NO
FAILOVER Status     = YES

[ Polling Parameter of each interface ]
Name   intvl idle  time  repara link  Fover
+-----+-----+-----+-----+-----+-----+
sha0   ---    ---    ---    ---    ---    ---
```

## 3.9 Setting monitoring function of Virtual NIC mode

### 3.9.1 Link status monitoring function

Link status monitoring is enabled automatically when you configure a virtual interface. Setting is not required.

### 3.9.2 Network monitoring function

For network monitoring, you have to configure the HUBs that are to be monitored. For details, see "[7.12 hanetpathmon Command](#)". Since the standby patrol is automatically activated, setting is not required.

#### 3.9.2.1 Disabling the network monitoring function

When network monitoring is running, stop monitoring temporarily. Use the "hanetpathmon off" command for this setting.

#### 3.9.2.2 Setting the monitoring destination information

Set the monitoring destination for HUB monitoring. Use the "hanetpathmon target" command for this setting.

#### 3.9.2.3 Enabling the network monitoring function

Enable the network monitoring function. Use the "hanetpathmon on" command for this setting.

#### 3.9.2.4 Transfer route error detection time for network monitoring function

This section describes the transfer route error detection sequence of the network monitoring function.

##### Error detection time:

The time required for the network monitoring function to detect an error after it has occurred at the monitoring target is shown below. Immediately after starting network monitoring, however, the formulas do not apply, since error detection is delayed for at least 45 seconds, taking into account the linkup delay time of the HUB.

##### Monitoring interval is 2 or more seconds:

```
Error detection time = monitoring interval (in seconds) X (monitoring frequency - 1) + time
out period (2 seconds) + (0 to monitoring interval (in seconds))
```

### Monitoring interval is 1 second:

Error detection time = time out period (2 seconds) X monitoring frequency + (0 to 1 (in seconds))

Example 1) Default setting (3 seconds interval and 5 times):

$3 \text{ sec} \times (5 \text{ time} - 1) + 2 \text{ sec} + (0 \text{ to } 3 \text{ sec}) = 14 \text{ to } 17 \text{ sec}$

Example 2) 1 second interval and 1 time:

$2 \text{ sec} \times 1 \text{ time} + (0 \text{ to } 1 \text{ sec}) = 2 \text{ to } 3 \text{ sec}$

Example 3) 10 seconds interval and 3 times:

$10 \text{ sec} \times (3 \text{ time} - 1) + 2 \text{ sec} + (0 \text{ to } 10 \text{ sec}) = 22 \text{ to } 32 \text{ sec}$



### Information

Since network 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 monitoring is performed. Therefore, it takes at least 14 seconds and up to 17 seconds to detect the failure after a failure has occurred by the default setting.

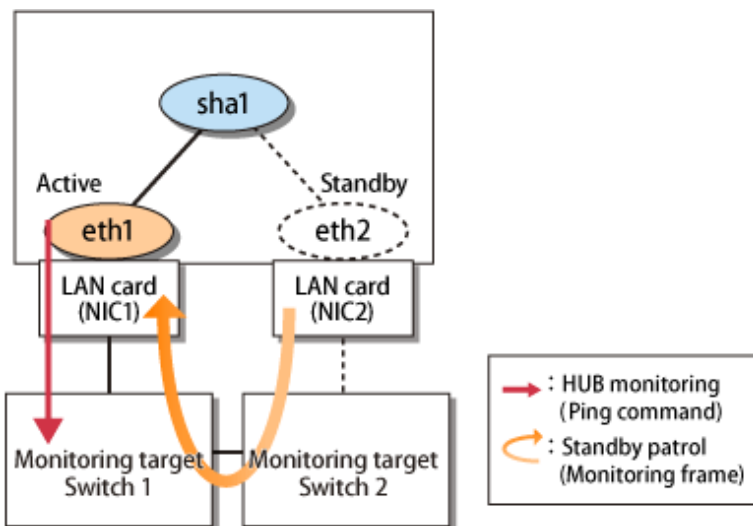
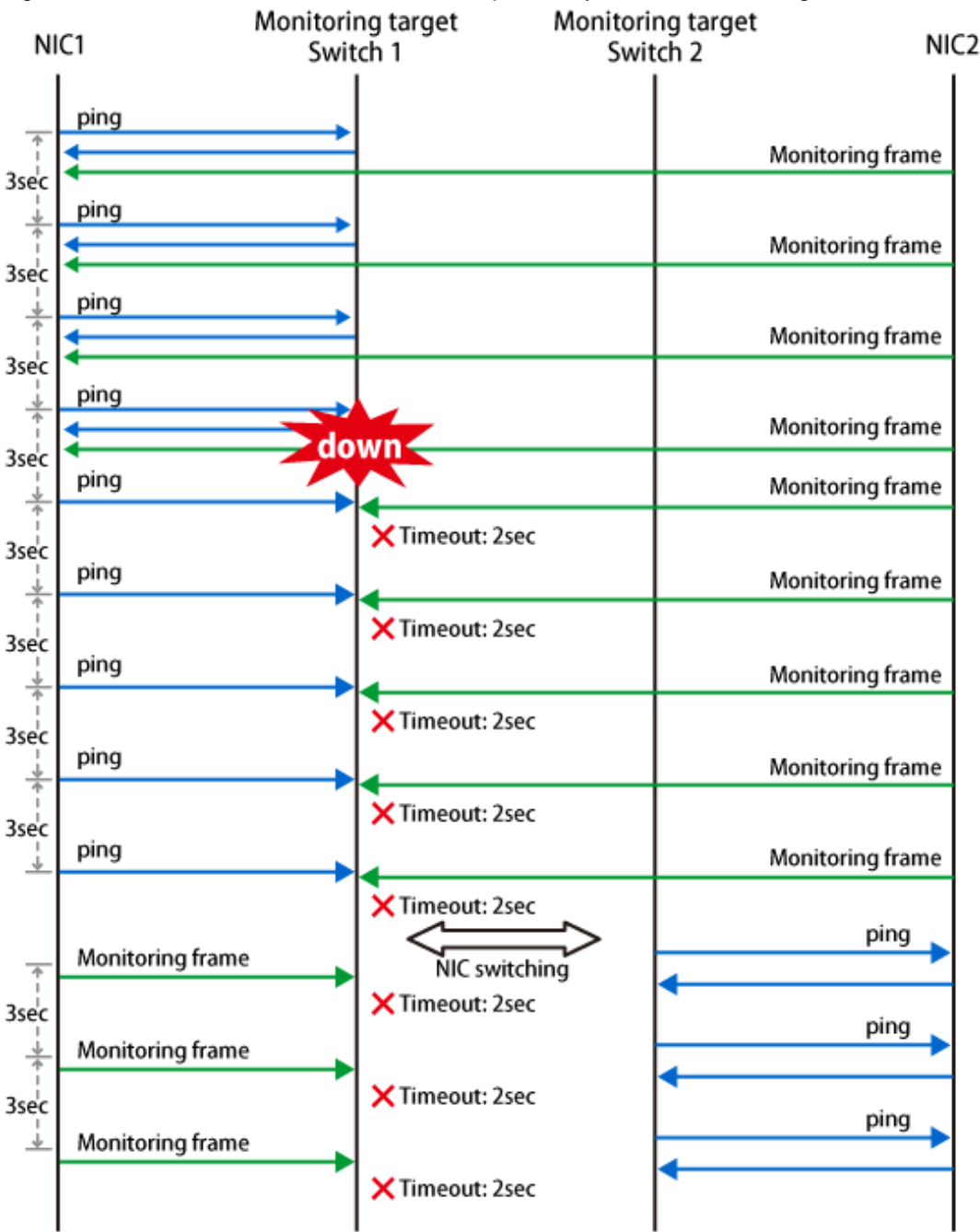


Figure 3.15 Transfer route error detection sequence by network monitoring function



3.9.2.5 Transfer route recovery detection time for network monitoring function

This section describes the transfer route recovery detection sequence of the network monitoring function.

Recovery detection time:

The following shows time required for going back to the normal monitoring after recovery of a monitoring target is detected in the recovery monitoring by the standby patrol of the network monitoring function and time required for performing the automatic fail-back:

When monitoring interval is 2 or more seconds:

$$\text{Recovery detection time} = \text{monitoring interval (in seconds)} \times (\text{recovery monitoring frequency} - 1) + (0 \text{ to monitoring interval (in seconds)})$$

When monitoring interval is 1 second:

Recovery detection time = response time (1 to 2 seconds) X recovery monitoring frequency + (0 to 1 (in seconds))

Example 1) Default setting (3 seconds interval and 2 times):

$3 \text{ sec} \times (2 \text{ time} - 1) + (0 \text{ to } 3 \text{ sec}) = 3 \text{ to } 6 \text{ sec}$

Example 2) 1 second interval and 1 time:

$(1 \text{ to } 2 \text{ sec}) = 1 \text{ time} + (0 \text{ to } 1 \text{ sec}) = 1 \text{ to } 3 \text{ sec}$

Example 3) 10 seconds interval and 3 times:

$10 \text{ sec} \times (3 \text{ time} - 1) + (0 \text{ to } 10 \text{ sec}) = 20 \text{ to } 30 \text{ sec}$

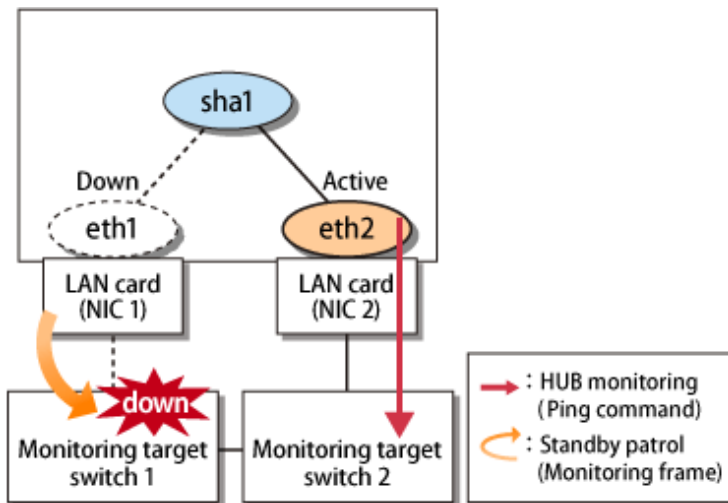
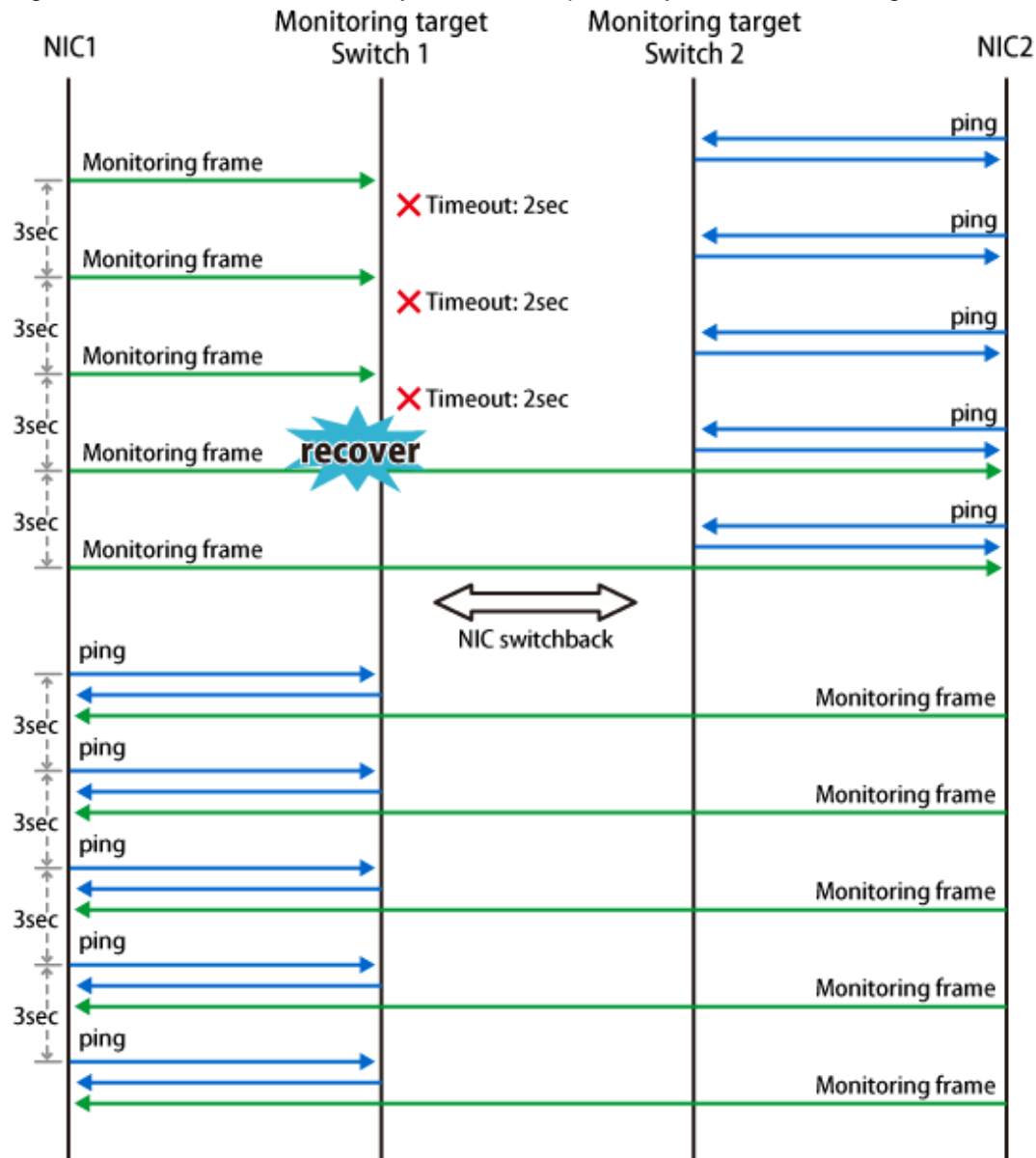


Figure 3.16 Transfer route recovery detection sequence by network monitoring function



## 3.10 Setting monitoring function of GS linkage mode

### 3.10.1 Monitoring the remote host

#### 3.10.1.1 Setting the monitoring destination information

In GS linkage mode, you need to set the following monitoring destination. Use the "hanetobserv create" command to set the monitoring destination. For more details on how to make settings, see "7.15 hanetobserv Command".

- Virtual IP address and real IP address of the target
- Physical IP addresses and takeover virtual IP addresses of other nodes that make up the cluster (applied only for the cluster configuration using PCL).

#### 1) Setting the target monitoring

Specify the real IP address and virtual IP address of the target. GLS monitors the real IP address that has been set by using ping. In addition, based on these settings, GLS switches the virtual IP address between nodes of the target and monitors the network.

This section describes the settings when the communication target is included in the following configurations:

- Single configuration
- Hot-standby (One virtual IP)
- Hot-standby (Two virtual IPs)
- Load sharing configuration (When virtual IPs are activated on all GSs)
- Load sharing configuration (When there is any GS in which virtual IP is not activated)



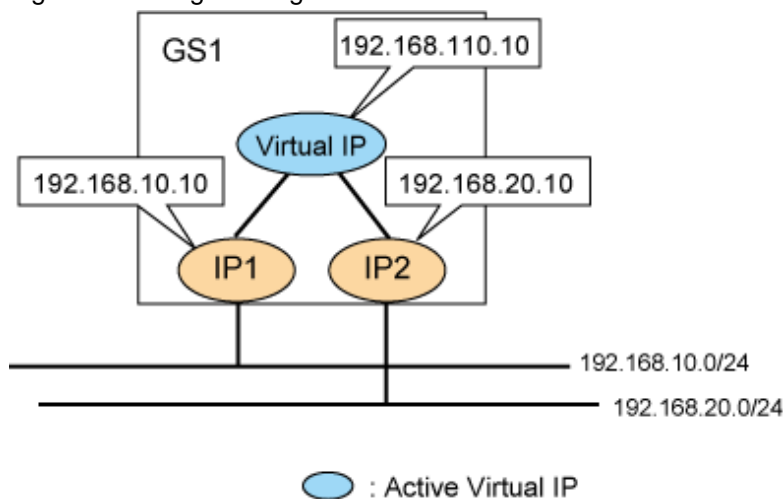
## Note

### When the communication target is included in the hot-standby configuration.

- The virtual IP address of a communication target can be transferred among 4 nodes (up to 16 nodes depending on the setting) as default. For information on how to set the virtual IP address, see "[3.1.2.6 Upper limit of configuration.](#)"
- Execute the TNOTIFY command from the host (GS) where the virtual IP address of a communication target exists to the virtual IP address.  
If multiple virtual IP addresses exist in the host (GS), execute the TNOTIFY command for each individual IP address.

### Single configuration

Figure 3.17 Single configuration



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t 192.168.10.10,192.168.20.10
```

2. Check the settings.

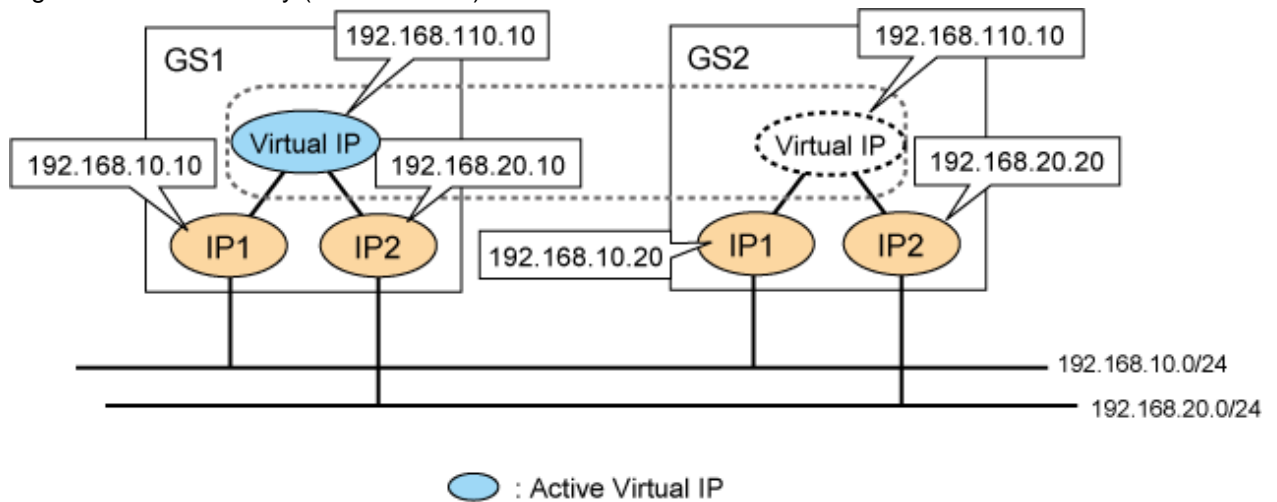
```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
```

Destination Host	Virtual Address	(Router Address+)NIC Address
GS	192.168.110.10	192.168.10.10,192.168.20.10

## Hot-standby (One virtual IP)

Figure 3.18 Hot-standby (One virtual IP)



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target. Set the same name, rather than a different name, with the "-n" option for each node when you set the nodes comprising the cluster.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.20,192.168.20.20
```

2. Check the settings.

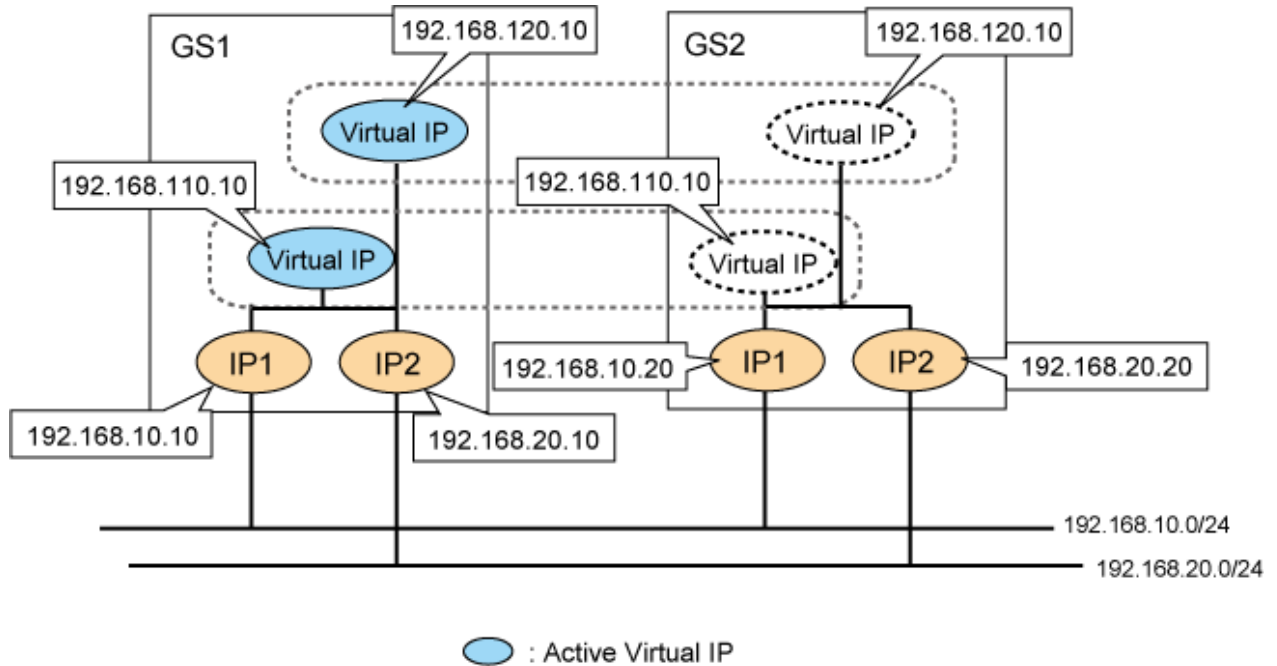
```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+
GS          192.168.110.10      192.168.10.10,192.168.20.10
                                   192.168.10.20,192.168.20.20
```



## Hot-standby (Two virtual IPs)

Figure 3.19 Hot-standby (Two virtual IPs)



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target. Set the same name, rather than a different name, with the "-n" option for each node when you set the nodes comprising the cluster.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.110.10 -t
192.168.10.20,192.168.20.20
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.10 -t
192.168.10.20,192.168.20.20
```

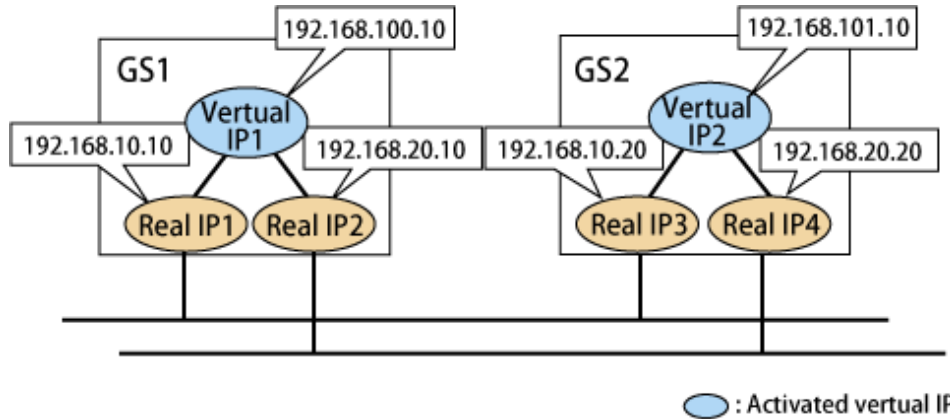
2. Check the settings.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+
GS          192.168.110.10             192.168.10.10,192.168.20.10
                                     192.168.10.20,192.168.20.20
          192.168.120.10             192.168.10.10,192.168.20.10
                                     192.168.10.20,192.168.20.20
```

Load sharing configuration (If virtual IPs are activated on all GSs)

Figure 3.20 Load sharing configuration (When virtual IPs are activated on all GSs)



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target. Set a combination of a virtual IP address and a physical IP address per GS in which every virtual IP address is activated.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS1 -i 192.168.100.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS2 -i 192.168.101.10 -t
192.168.10.20,192.168.20.20
```

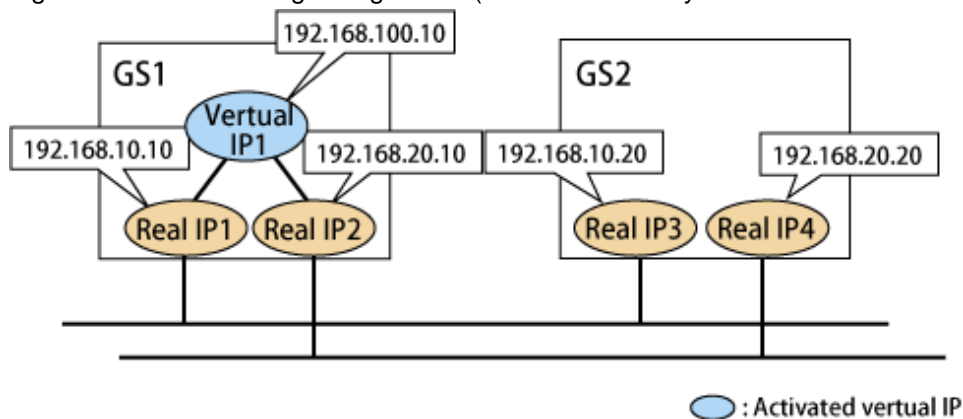
2. Check the settings.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = NO

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+
GS1      192.168.100.10  192.168.10.10,192.168.20.10
GS2      192.168.101.10  192.168.10.20,192.168.20.20
```

Load sharing configuration (When there is any GS in which virtual IP is not activated)

Figure 3.21 Load sharing configuration (When there is any GS in which virtual IP is not activated)



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target. Set a combination of any activated virtual IP address and a GS physical IP address with non-activated virtual IP address.

If physical IP addresses of several GSs are set for a single virtual IP address, the GS with the physical IP address set first is recognized as communication target of GLS.

```
# /opt/FJSSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.100.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.100.10 -t
192.168.10.20,192.168.20.20
```

2. Check the settings.

```
# /opt/FJSSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = NO

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+-----+
GS          192.168.100.10      192.168.10.10,192.168.20.10
                                   192.168.10.20,192.168.20.20
```

## 2) Setting PCL monitoring for other nodes

If the local system is running on a clustered system, it switches a node when GS of the communication target 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 GSs of the communication targets stop 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 systems stop 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.

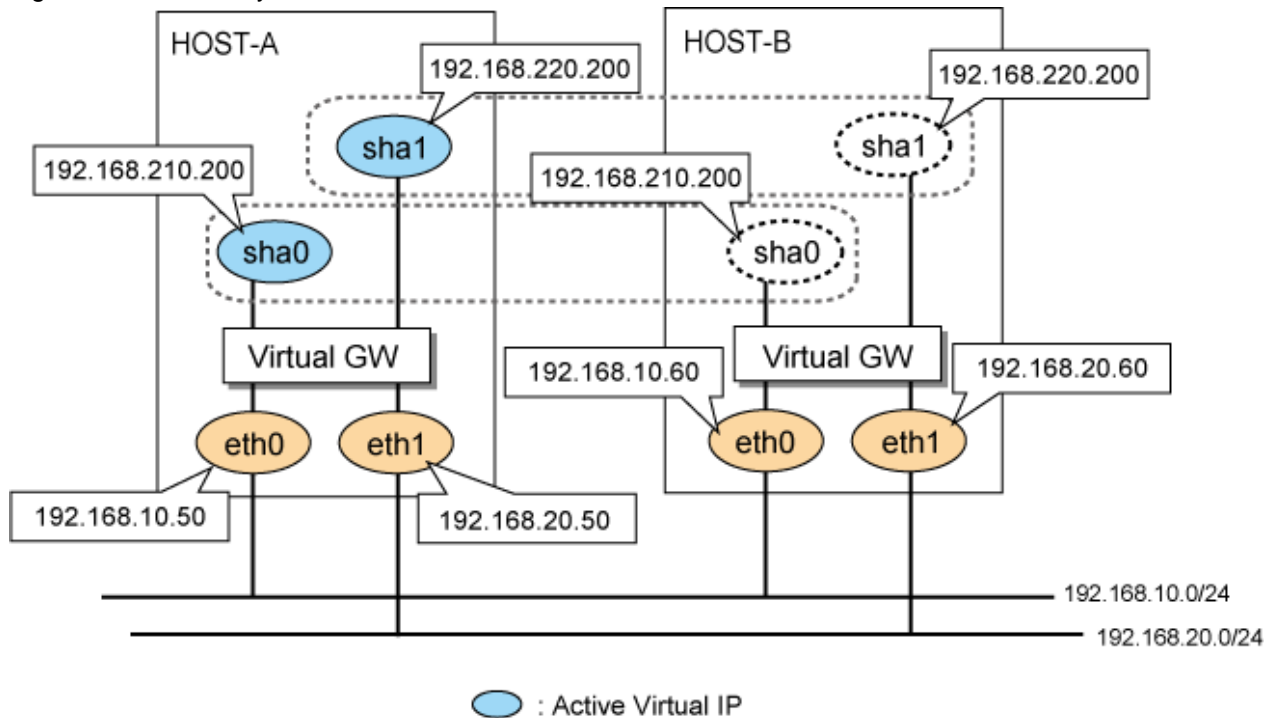


### Note

If all the GSs of the communication targets are stopped and the destination cluster node is restarted, a resource failure occurs and cluster applications are stopped. To prevent the resource failure if the local NIC has no failure, specify management IP addresses of neighboring switches as monitoring destinations.

## Cluster system

Figure 3.22 Cluster system



1. Use the "hanetobserv" command to register the virtual IP address and real IP address of the target. Set the name of another node in a cluster configuration in the "-n" option.

```
Settings on HOST-A
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i
192.168.210.200 -t 192.168.10.60,192.168.20.60
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i
192.168.220.200 -t 192.168.10.60,192.168.20.60
Settings on HOST-B
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i
192.168.210.200 -t 192.168.10.50,192.168.20.50
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i
192.168.220.200 -t 192.168.10.50,192.168.20.50
```

2. Check the settings.

```
Settings on HOST-A
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+
HOST-B          192.168.210.200      192.168.10.60,192.168.20.60
                192.168.220.200      192.168.10.60,192.168.20.60

Settings on HOST-B
# /opt/FJSVhanet/usr/sbin/hanetobserv print
[ Standard Polling Parameter ]
```

```

interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES

```

Destination Host	Virtual Address	(Router Address+)NIC Address
HOST-A	192.168.210.200	192.168.10.50,192.168.20.50
	192.168.220.200	192.168.10.50,192.168.20.50

### 3.10.1.2 Transfer route error detection time in GS linkage mode

This section describes the transfer route error detection sequence.

In GS 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 physical IP address of another node of the cluster. The time it takes for an error to be detected is as follows. 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 "hanetobserv param" command. For more details on how to make settings, see "[7.15 hanetobserv Command](#)".

#### Error detection time:

```

Error detection time = monitoring interval(in seconds) X (monitoring frequency -
1) + ping time out period(*1) + (0 to monitoring interval (in seconds))

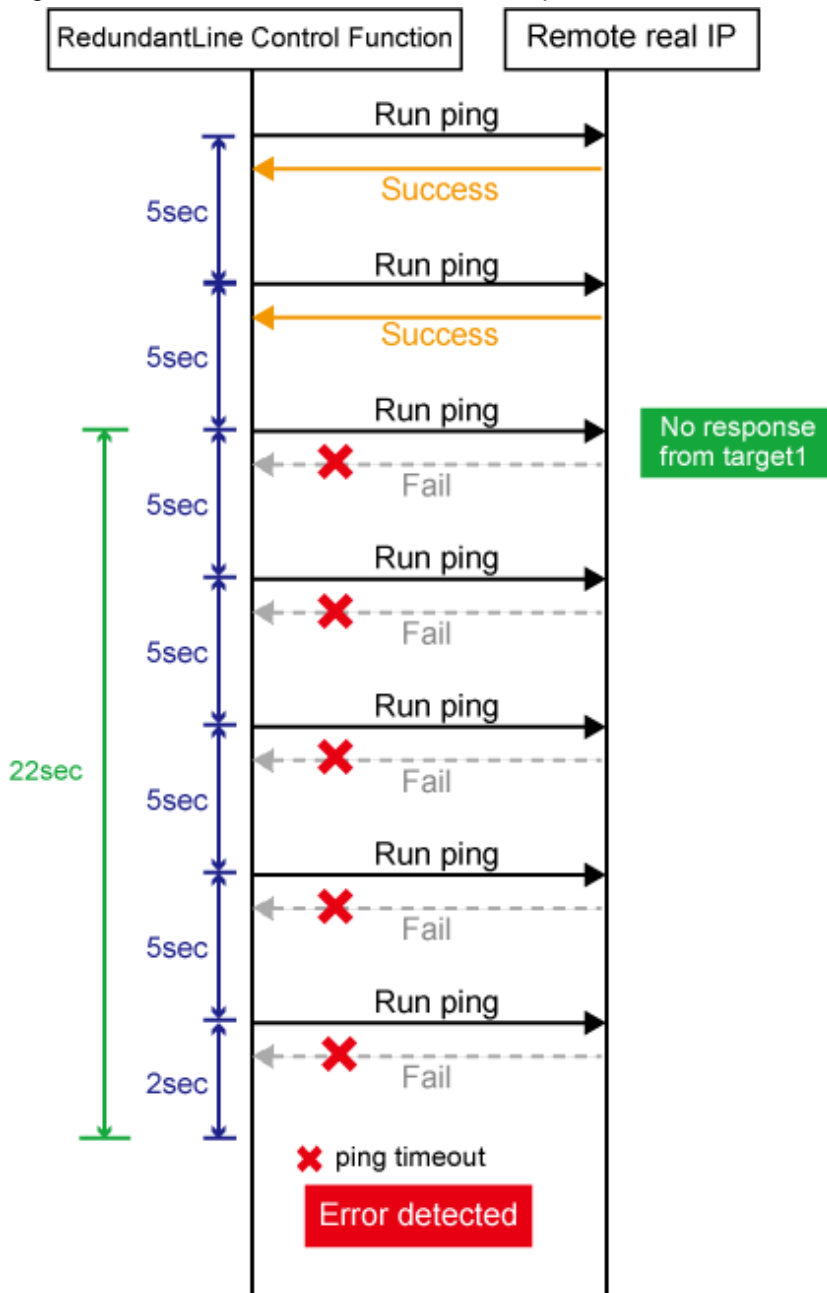
```

\*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 time - 1) + 2 sec + 0 to 5 sec = 22 to 27 sec

Figure 3.23 Transfer route 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 at least 22 seconds and up to 27 seconds 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 before GLS changes the route.
- Just after starting error monitoring for transfer routes, or switching recovery monitoring to error monitoring, error detection will be pended until the waiting time for linkup elapses.

### 3.10.1.3 Transfer route recovery detection time in GS linkage mode

This section describes the transfer route recovery detection sequence.

In GS 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, GLS performs recovery monitoring by ping to monitor the state of the recovery of the GLS transfer route. The time it takes for recovery to be detected is as follows. 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 "hanetobserv param" command. For more details on how to make settings, see ["7.15 hanetobserv Command"](#).

### Recovery detection time:

Recovery detection time = recovery monitoring interval (in seconds) + recovery monitoring interval (in seconds) x retry count + (0 to recovery monitoring interval (in seconds))

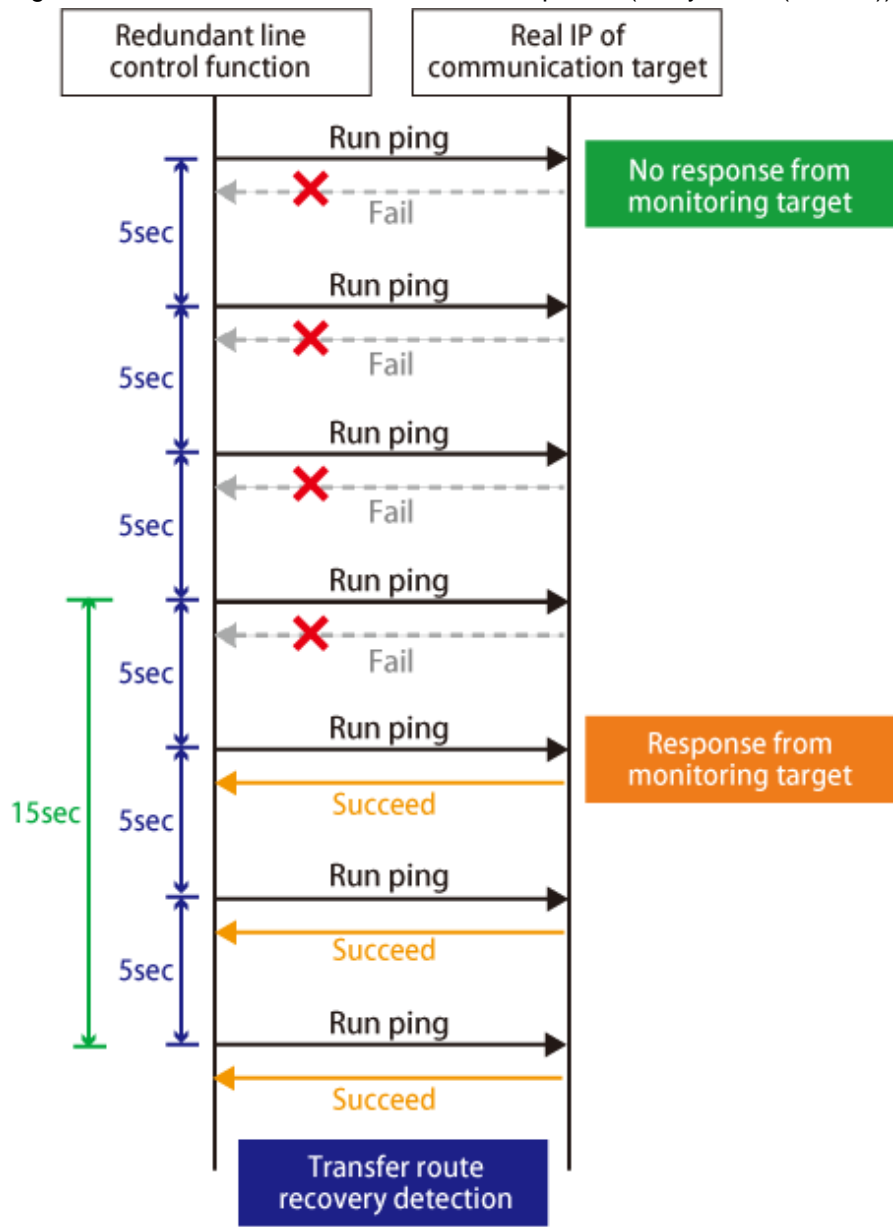
The default value would look like the following.

5 sec x 0 time + 0 to 5 sec = 0 to 5 sec

When the retry count is 2 times, the value would look like the following.

5 sec x 2 time + 0 to 5 sec = 10 to 15 sec

Figure 3.24 Transfer route error detection sequence (Retry count (2 times))



## 3.11 Setting other monitoring function

---

### 3.11.1 Interface status monitoring feature

---

The interface status monitoring function is started automatically. Therefore, no setting is required.

### 3.11.2 Self-checking feature

---

#### 3.11.2.1 How to set up the self-checking function

The self-checking function can be enabled as follows.

1. Enable the self-checking function

```
# /opt/FJSVhanet/usr/sbin/hanetparam -e yes
```

2. Check the changed parameters.

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
[Fast switching]
  Line monitor interval(w)           :5
  Line monitor message output (m)     :0
  Cluster failover (l)                :5
  Cluster failover in unnormality (c):OFF
  Line status message output (s)      :OFF

[NIC switching]
  Standby patrol interval(p)          :15
  Standby patrol message output(o)    :3

[Virtual NIC]
  LinkDown detection time (q)         :0
  LinkUp detection time (r)           :1
  Link monitor starting delay (g)     :5

[Common Setting]
  Hostname resolution by file(h)       :NO
  Self-checking function(e)           :YES
```

3. Reboot the system. After reboot, the self-checking function will be enabled.

The self-checking function can be disabled as follows.

1. Disable the status monitoring function

```
# /opt/FJSVhanet/usr/sbin/hanetparam -e no
```

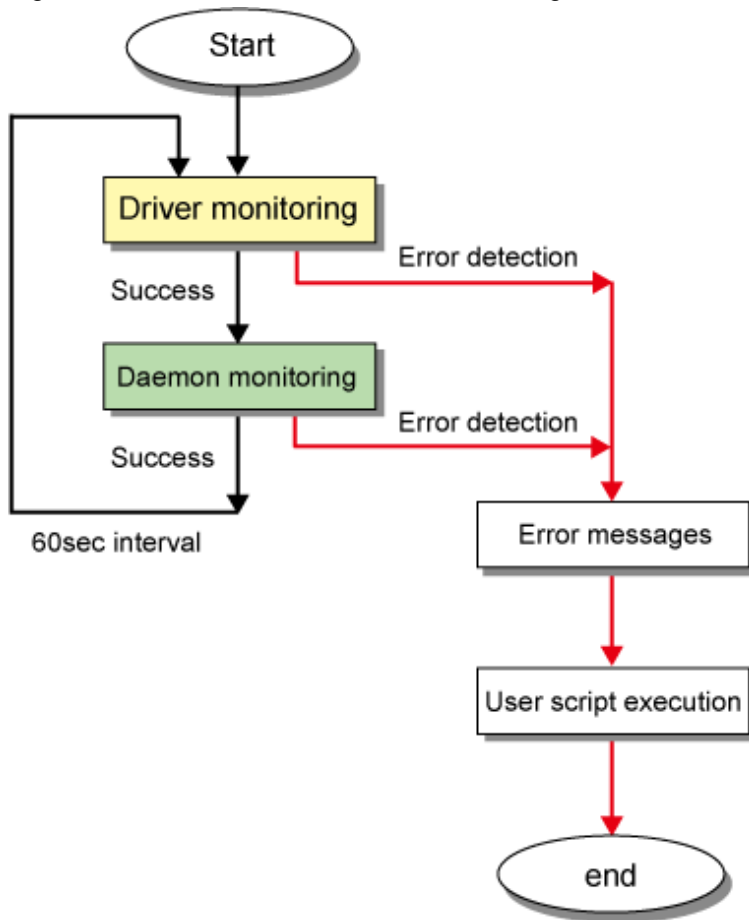
2. Reboot the system. After reboot, the self-checking function will be disabled.

#### 3.11.2.2 Error detection of the self-checking function

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



Figure 3.25 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 15 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, a message similar to the following will be output to the system log.

- An error occurred in the virtual driver

The following message is output and the monitoring function stopped. Reboot the system after collecting troubleshooting information.

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

xxx: error type (hung-up 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 (hung-up, I/O error, or stopped process)

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

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

If the above message is not output, reboot the system after collecting troubleshooting information.

Note that placing a script in the following location allows the script to be executed when an error is detected. For more details, see "[3.12.2 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-checking function can be restored by restarting it as below.

```
# /opt/FJSVhanet/etc/sbin/hanetmond
```

If the self-checking 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.

## 3.12 Setting Linkage function

### 3.12.1 Cluster switching behavior for failure of all the transfer paths

Use the following commands for cluster switching behavior for failure of all the transfer paths:

- Fast switching mode

Use the "hanetparam" command. For details, see "[7.6 hanetparam Command](#)".

- NIC switching mode

Use the "hanetpoll" command. For details, see "[7.7 hanetpoll Command](#)".

- Virtual NIC mode

Use the "hanetpathmon param" command. For details, see "[7.12 hanetpathmon Command](#)".

- GS linkage mode

Use the "hanetobserv param" command. For details, see "[7.15 hanetobserv Command](#)".

### 3.12.2 Setting user command execution function

In NIC switching mode and GS linkage mode, a command pre-defined by a user can be executed at specific timing. For information on execution timing, see "[2.8.2 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. The following settings must be made to execute a user command. 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 linkage mode

- /etc/opt/FJSVhanet/script/host/node\_event.sam

#### Sample file for Self-checking function

- /etc/opt/FJSVhanet/script/system/monitor.sam

#### [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/shaX (When detected a standby patrol error or recovery)

\* shaX is the created virtual interface name for NIC switching mode.

#### Setup file for GS linkage mode

- /etc/opt/FJSVhanet/script/node\_event

#### Setup file for Self-checking function

- /etc/opt/FJSVhanet/script/system/monitor



#### Note

- Do not call the operational command for redundancy line control function in the script file.
- If you execute the command that operates a cluster resource in the script file, make sure to execute it on the background adding "&" at the end of the command. Do not use commands such as the "wait" command of the operating system to wait for the completion of the command that was executed on the background.
- When the execution of the user command is set, GLS waits for the completion of the shell script. If time-consuming processing was described in the shell script, the subsequent processing may be delayed. In order to make the shell script finish immediately, make sure to describe the execution of the time-consuming processing on the background in the shell script.
- 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 commands such as the "logger" command of the operating system to output the messages.
- 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.
- Create a script file for each virtual interface. If both of IPv4 address and IPv6 address is set to a single virtual interface (or dual stack configuration), define the script file for each address family.
- You cannot use the script for the self-checking function to automatically reboot the control daemon of GLS. Reboot the system to recover the control daemon.
- In the environment where SELinux is enabled when executing a command which has the specific policy in the user script, the access violation for the internal log of GLS (/var/opt/FJSVhanet/log/sh.log) may be recorded. If it affects the action of the script, define the exception of the access privilege with the SELinux module to avoid it. For details, refer to "Linux documentation".

### 3.12.2.1 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: Activated

inactivate: Inactivated

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 2004
#
#ident  "%W% %G% %U% - FUJITSU"
#
#
#      Control interface for HA-Net
#
#
#      Params
#
#      $1      activate or inactivate
#      $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
#

# echo "execute script before activate interface on" $INTERFACE > /dev/
console

#if [ ! $INTERFACE = "ethX" ]
#then
#    ifconfig $INTERFACE
#else
#    ifconfig $INTERFACE
#fi

;;

'after')
#
# script after activate interface
#

# echo "execute script after activate interface on" $INTERFACE > /dev/
console

#if [ ! $INTERFACE = "ethX" ]
#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
#

# echo "execute script before inactivate interface on" $INTERFACE
> /dev/console
;;

'after')
#
# script after inactivate interface
#

# echo "execute script after inactivate interface on" $INTERFACE
> /dev/console

;;

*)
    ;;
esac

;;

*)
    ;;
esac

fi

if [ $ADDRESS_FAMILY = "inet6" ]
then

case "$1" in
'activate')

#
# Activate interface
#

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

# echo "execute script before activate interface on" $INTERFACE > /dev/
console

;;

'after')
#

```

```

# script after activate interface
#

# echo "execute script after activate interface on" $INTERFACE > /dev/
console

;;

*)
    ;;
esac

;;

'inactivate')
#
# inactivate interface
#

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

# echo "execute script before inactivate interface on" $INTERFACE
> /dev/console

;;

'after')
#
# script after inactivate interface
#

# echo "execute script after inactivate interface on" $INTERFACE
> /dev/console

;;

*)
    ;;
esac

;;

*)
    ;;
esac

fi

exit 0

```

## (2) When detected an error in a transfer route

[Script file call format]

/bin/sh shaX param1

param1

Primary: Error in a Primary interface

Secondary: Error in a Secondary interface

all: Error in both Primary/Secondary interfaces

#### [Definition file sample]

```
#!/bin/sh
#
#       All Rights Reserved, Copyright (c) FUJITSU LIMITED 2004
#
#ident    "%W% %G% %U% - FUJITSU"
#
# Control interface for HA-Net
#
#
#       Params
#
#       $1    communication line state    primary/secondary/all
#
#
# Set Params
#
#STATE=$1
#PROC="process_name"
#kill -15 `/bin/ps -e | /bin/sed -n \
#       -e '/'$PROC'$s/[^0-9 \t].*//p' \
#       ` > /dev/null 2>/dev/null
#if [ $STATE = "primary" ]
#then
# echo "execute script Polling fail : primary" > /dev/console
#fi
#if [ $STATE = "secondary" ]
#then
# echo "execute script Polling fail : secondary" > /dev/console
#fi
#if [ $STATE = "all" ]
#then
# echo "execute script Polling failover" > /dev/console
#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 ethX

unknown: Standby NIC undecided

#### [Definition file sample]



```

#!/bin/sh
#
#      All Rights Reserved, Copyright (c) FUJITSU LIMITED 2004
#
#ident  "%W% %G% %U% - FUJITSU"
#
# Control interface for HA-Net
#
#
#      Params
#
#      $1  standby NIC state    establish/recovery/fail
#      $2  standby NIC name     ethX
#
#
# Set Params
#
#STATE=$1
#NIC=$2
#if [ $STATE = "fail" ]
#then
# echo "execute script Patrol fail ($NIC)" > /dev/console
#fi
#if [ $STATE = "establish" ]
#then
# echo "execute script Patrol establish ($NIC)" > /dev/console
#fi
#if [ $STATE = "recover" ]
#then
# echo "execute script Patrol recover ($NIC)" > /dev/console
#fi

```

### 3.12.2.2 Settings for GS linkage mode

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

[Script file call format]

/bin/sh node\_event

[Definition file sample]

```

#!/bin/sh
#
#      All Rights Reserved, Copyright (c) FUJITSU LIMITED 2005
#
#ident  "%W% %G% %U% - FUJITSU"
#
#
# Control interface for HA-Net
#
#
#      Params
#
#      $1      local ip address
#      $2      remote ip address
#      $3      event(NODE_DOWN, POLLING_TIMEOUT, or RESOURCE_OFFLINE)
#
#
case $# in

```

```

3)
    LOCAL_ADDR=$1
    REMOTE_ADDR=$2
    EVENT=$3
;;
*)
;;
esac

case $EVENT in
'NODE_DOWN')
#
# NODE_DOWN invokes when failover occurs at remote host.
#
# execution format) node_event 0.0.0.0 remote ip address NODE_DOWN
;;
'POLLING_TIMEOUT')
#
# POLLING_TIMEOUT invokes when all routes to a virtual ip address
# of remote host failed to hold communication for 3 minutes.
#
# execution format) node_event 0.0.0.0 remote ip address
POLLING_TIMEOUT
;;
'RESOURCE_OFFLINE')
#
# RESOURCE_OFFLINE invokes when a virtual interface changes
# its state to inactive over a cluster system.
#
# execution format) node_event local ip address 0.0.0.0
RESOURCE_OFFLINE
;;
*)
;;
esac

exit 0

```

## Information

You can set the time from detecting monitoring failures of a communication target until executing the user command. Execute the user command with the POLLING\_TIMEOUT option to the user script "node\_event".

The default is 180 seconds (about 3 minutes). The setting value is specified within a range of 0 to 7200. When 0 is specified, the user script is not executed.

Since the time until the execution is controlled by the timer by 5 seconds, if you compare the setting time and the actual execution time, there is a difference up to 5 seconds.

The following shows the setting examples.

1. Change the internal parameter of GLS.

The value of "observ\_polling\_timeout" described in ctld.param is changed into the shortest value (1) from the default value (180).

/etc/opt/FJSVhanet/config/ctld.param

```

#
# HA-Net Configuration File
#

```

```
#      Each entry is of the form:
#
#      <param> <value>
#
observ_msg      0
observ_polling_timeout  1    <-Changed
max_node_num     4
```

## 2. Restart GLS.

Distribute the changes by restarting GLS daemon with the `resethanet -s` command when restarting the operating system.

### 3.12.2.3 Settings for 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 2007
#
#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

```

## 3.13 Setting Maintenance function

---

### 3.13.1 Setting dynamic addition/deletion/switching function of physical interfaces

---

#### 3.13.1.1 Dynamic addition of physical interfaces

In Fast switching mode, Virtual NIC mode, and GS 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 a "hanetnic add" command. See "[7.9 hanetnic Command](#)" as to how to set.



#### Note

In GS linkage mode, you can only temporarily delete and add (dynamically delete and then dynamically add) a redundant physical interface. If you dynamically delete a physical interface, make sure to add it dynamically afterwards.

#### 3.13.1.2 Dynamic deletion of physical interfaces

In Fast switching mode, Virtual NIC mode, and GS 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 a "hanetnic delete" command. See "[7.9 hanetnic Command](#)" as to how to set.



#### Note

In GS linkage mode, you can only temporarily delete and add (dynamically delete and then dynamically add) a redundant physical interface. If you dynamically delete a physical interface, make sure to add it dynamically afterwards.

#### 3.13.1.3 Dynamic switching of physical interfaces

In NIC switching mode and Virtual NIC 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 a "hanetnic change" command. See "[7.9 hanetnic Command](#)" as to how to set.

### 3.13.2 Active maintenance of NIC (PCI card)

---

Active maintenance allows for replacing any malfunctioning NICs without disrupting ongoing operation. Making any settings for active maintenance before starting system operation is not required. For details on the active maintenance procedure for NICs, see "[6.3 NIC maintenance \(for RHEL5\)](#)" or "[6.4 NIC maintenance \(for RHEL6\)](#)".

## 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 router 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
	/opt/FJSVhanet/usr/sbin/dspobserv	Displaying the polling status of a remote node	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 cluster application 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 cluster application 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 "[7.2 strhanet Command](#)".



### Note

- 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.

## 4.2.2 Inactivating virtual interfaces

---

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

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



### Note

Be sure to use a stphanet command to deactivate a virtual interface. Do not use an ifconfig command to do the operation.

## 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. For details about this command, see "[7.4 dsphanet Command](#)".

## 4.4 Displaying Monitoring Status

---

To display the monitoring status, use the following commands:

- Fast switching mode  
To check the status of communication target monitoring, see "[7.4 dsphanet Command](#)".
- NIC switching mode  
To check the status of HUB monitoring, see "[7.8 dspoll Command](#)".  
To check the status of the standby patrol, see "[7.4 dsphanet Command](#)".
- Virtual NIC mode  
To check the status of network monitoring, see "[7.13 dsppathmon Command](#)".
- GS linkage mode  
To check the status of remote host monitoring, see "[7.16 dspobserv Command](#)".

## 4.5 Recovery Procedure from Line Failure

---

This section explains the recovery procedure in various modes after a line failure has occurred.

### 4.5.1 Recovery procedure from line failure in Fast switching mode and GS 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.

### 4.5.2 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/FJSVhanet/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
```

### 4.5.3 Recovery procedure from line failure in Virtual NIC mode

---

The following shows the recovery procedure from a line failure in Virtual NIC 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. When a fail-back has been performed by the automatic fail-back function, this action is not required.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

#### [Both-system (currently active and standby NICs) failure]

When either active NIC or standby NIC is recovered, communication is restarted by using a NIC on the recovered side. Therefore, special operation is not required.

## 4.6 Backing up and Restoring Configuration Files

---

This section explains how to back up and restore configuration files of Redundant Line Control Function.

### 4.6.1 Backing up Configuration Files

---

Use the hanetbackup command to back up configuration files.

For details about this command, see "[7.18 hanetbackup Command](#)".

### 4.6.2 Restoring Configuration Files

---

Use the hanetrestore command to restore configuration files.

For details about this command, see "[7.19 hanetrestore Command](#)".

After executing this command, restart the system immediately. The correct operation of Redundant Line Control Function cannot be assured if the system is not restarted.



## 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 (1:1 and N:1)
- Mutual standby
- Cascade
- Priority transfer
- Duplicate transfer path for SIS

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	Mutual standby System	Cascade System	Priority transfer system	Duplicate transfer path for SIS
Fast switching mode	A	A	A	A	X
NIC switching mode	A	A	A	A	A
Virtual NIC mode	A	A	A	A	X
GS linkage mode	A	A	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.

In addition, physical interfaces used by virtual interfaces cannot be set as takeover targets (MAC address and IP address) for the cluster.

In Virtual NIC mode, IP addresses are not taken over, and only node switching can be performed independently in the event of a line failure.

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
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



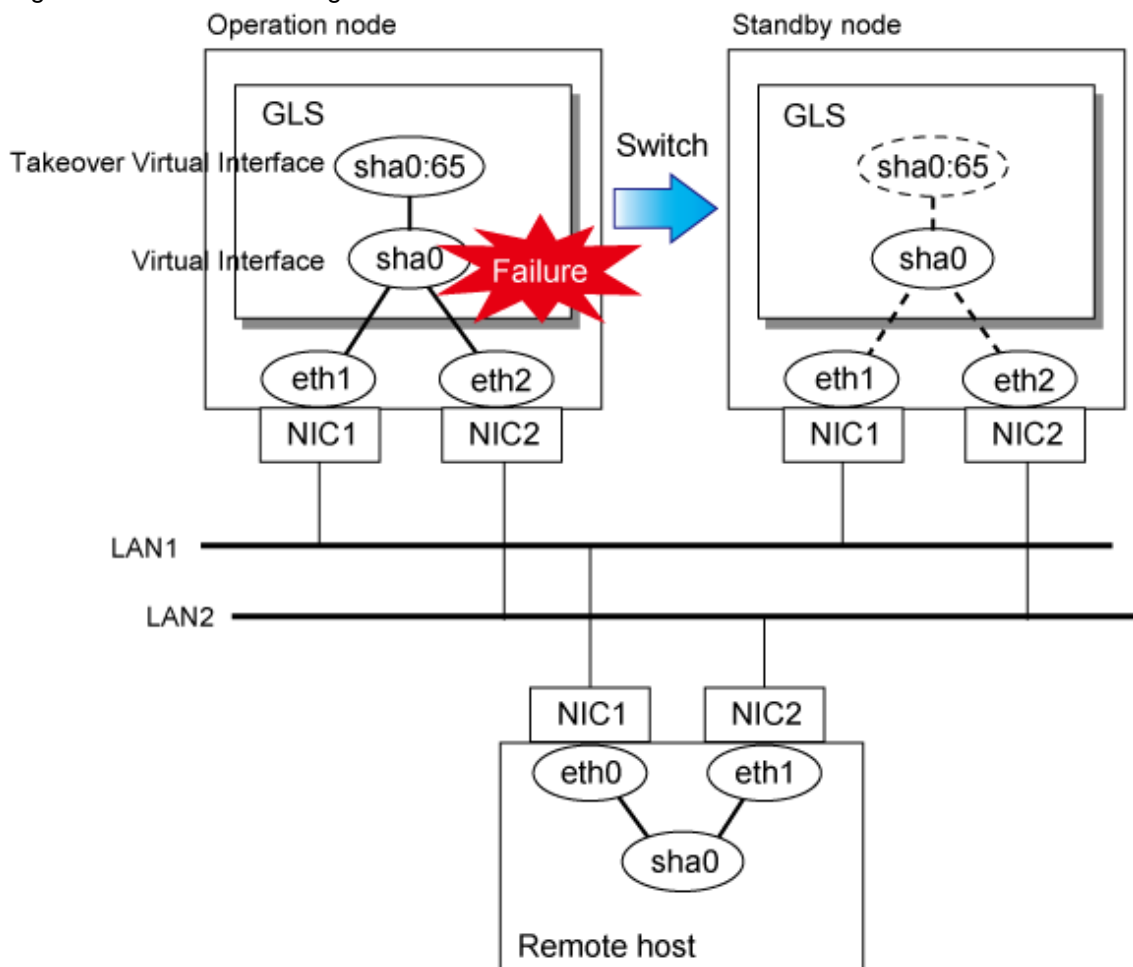
#### Note

- 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 on the transfer route monitoring host due to simultaneous detection of transfer route failure on operation node and standby node.
- When multiple virtual machines are created on one server to set up a cluster configuration, and Fast switching mode is used, an error will not occur to the cluster resources, even if a failure occurs to a switch which exists outside of the server. This is because a configuration is for successful monitoring at any time in the virtual switch in which multiple virtual machines are connected.
- When two or more GLs resources are registered to one cluster application, if an anomaly in one of the GLs resources is detected, a failover of the cluster applications will occur.

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)

## 5.2 Configuration for Cluster system

This section explains configurations required for operating the cluster system.



### Note

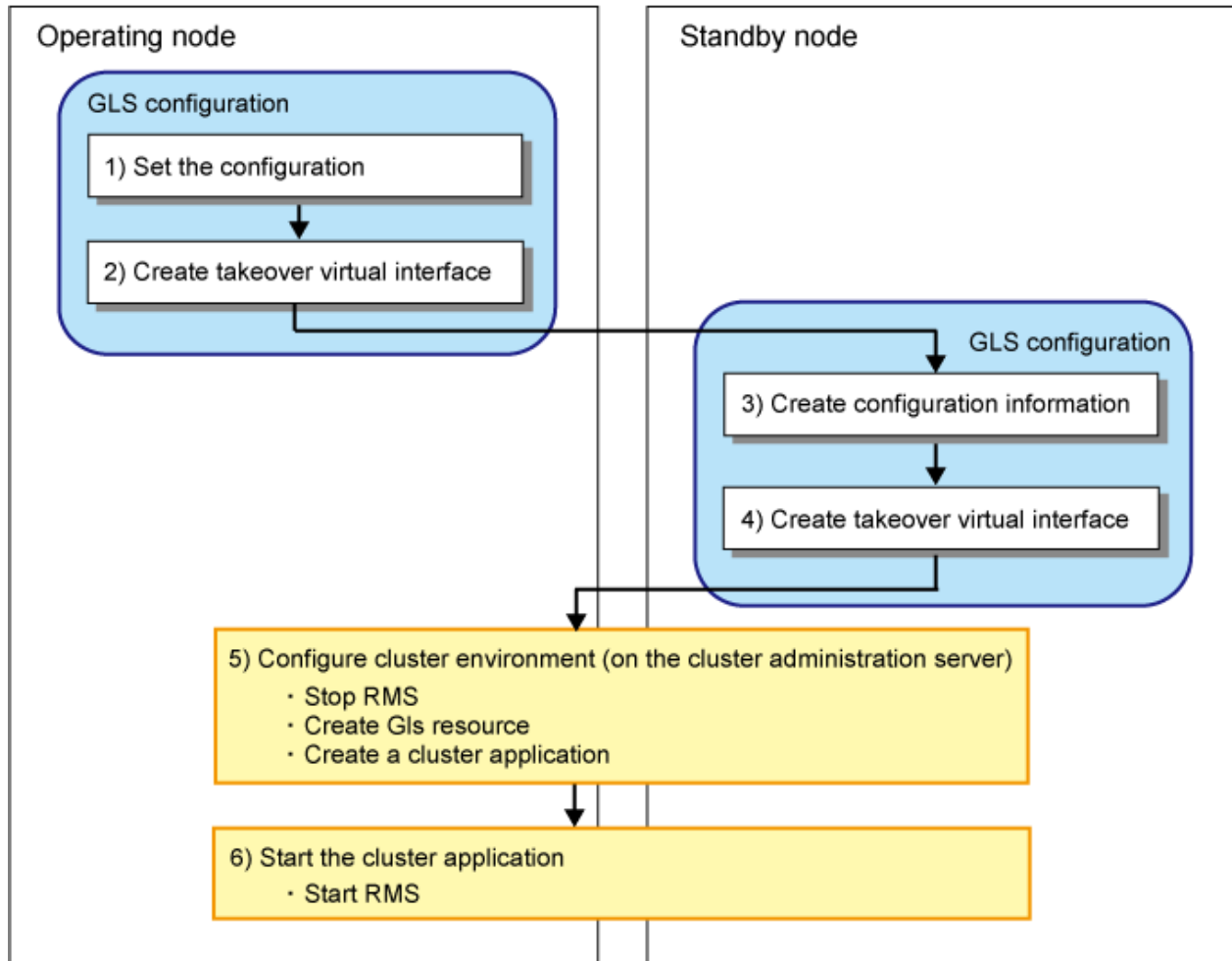
If you modified the configuration information for the cluster operation and the takeover virtual interface information, enable the modified settings by rebooting the system or by executing the `resethanet -s` option before operating GLS.

## 5.2.1 Adding configuration

In addition to configuring standard environment, configuration of takeover virtual interface and cluster environment is required for the cluster system.

Figure 5.2 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 5.2 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
Configuration of a virtual interface and the takeover resources.	/opt/FJSVhanet/usr/sbin/hanethvrsc	Registration/deletion/display of a virtual interface and the takeover resources.	Super user

### 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](#)".

## 2) Creating Takeover virtual interface

Takeover virtual interface for registering with userApplication is set up. It is necessary to perform this setup on all the nodes. When setting for Fast switching mode, it is necessary to set a "takeover IP address". (It is not necessary to set for NIC switching mode and GS linkage mode) An example of the setting is as follows. See "[7.17 hanethvsc Command](#)" for the detail of the command.

### [Configuring a takeover virtual interface]

```
# /opt/FJSVhanet/usr/sbin/hanethvsc create -n "virtual-interface-name" [-i takeover-IP-address]
```

## 3) Creating configuration information

Create the necessary configuration information for constructing a virtual interface.

## 4) Creating Takeover virtual interface

Takeover virtual interface for registering with userApplication is set up.

## 5) Configuring cluster system

Register the takeover virtual interface created as GLs resource, and create a userApplication. Cluster system can be configured using RMS Wizard. Refer to "PRIMECLUSTER Installation and Administration Guide" for details.

## 6) Starting an userApplication

After completing the configuration for a cluster system, start the userApplication on both cluster operating nodes. Refer to "PRIMECLUSTER Installation and Administration Guide" for details.

## 5.2.2 Modifying configuration for Cluster system

---

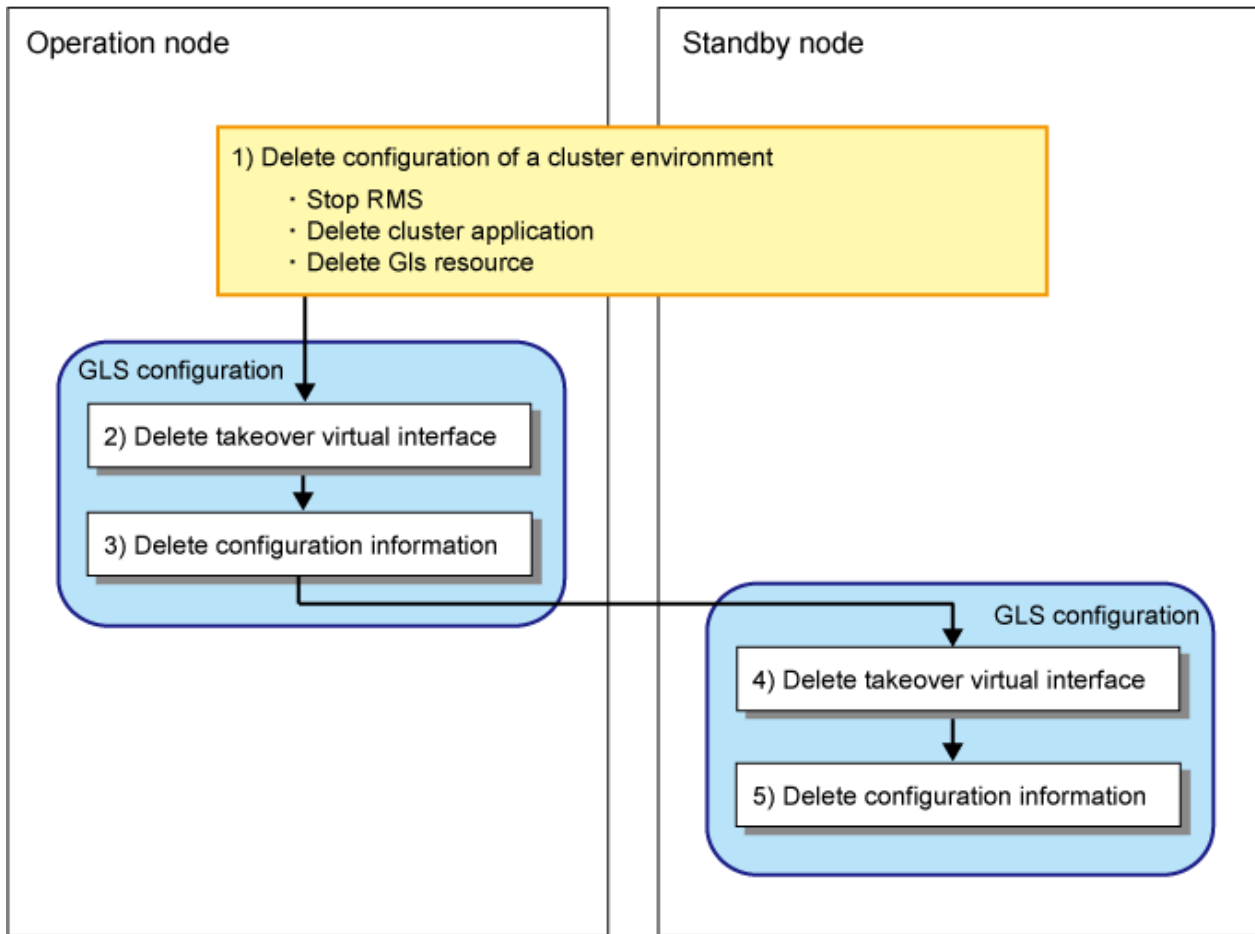
Configuration information and takeover resource information operated by the cluster system cannot be changed directly. Delete the takeover resource information first, and after changing corresponding configuration information, register the takeover resources information again.

## 5.2.3 Deleting configuration

---

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.

Figure 5.3 Flowchart for deleting configuration for cluster system



### 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.

### 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 the nodes.

An example of deletion is as follows. See "[7.17 hanethvrsc Command](#)" for the detail of the command.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n "logical-virtual-interface-
name"
```

### 3) Deleting configuration

Delete configuration information. Perform deletion process on the operating node and standby node. For deletion procedure, refer to "[3.5 Deleting configuration information](#)".

### 4) Deleting Takeover virtual interface

Delete a virtual interface to control a cluster from the resources database. The procedure is the same as 2).

### 5) Deleting configuration

Delete configuration information. The procedure is the same as 3).

## 5.3 Configuration for user application

When you register cluster applications or GLS resources with the cluster, you can change the linked operation of the cluster and GLS by specifying additional attributes. For more details, see "PRIMECLUSTER Installation/Administration Guide".

Table 5.4 Cluster definition operation commands

Configuration for user application	Function
StandbyTransitions attribution	When a network error has been detected on a standby node of the cluster, GLS notifies the cluster that the standby node cannot be used.

### 5.3.1 Monitoring resource status of standby node

In a userApplication for standby operation, it is possible to monitor standby node as well as a status of resource used in an operating node of GLS.

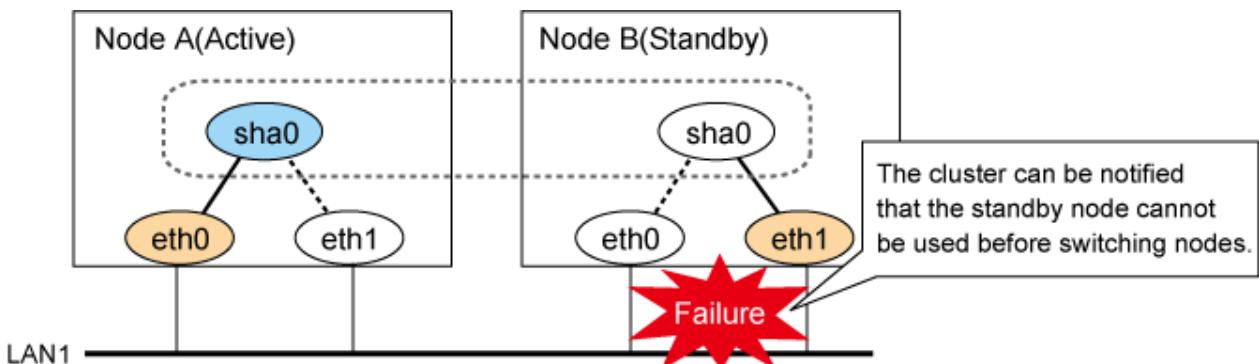
The following describes about monitoring GLS resource status of standby node.

#### 5.3.1.1 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).



#### 5.3.1.2 Configuration

Refer to "PRIMECLUSTER Installation and Administration Guide" for configuration of monitoring GLS resource status for a standby node.

#### 5.3.1.3 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 using "Cluster Admin" for Web-Based Admin View. (Use hvutil -c)

From this operation, GLS resource for standby node is reconfigured in a userApplication as a standby status.

## 5.4 Operation on cluster systems

### 5.4.1 Active Standby (Fast switching mode)

#### 5.4.1.1 Starting

With userApplication startup, the takeover virtual interface (sha0:65) over operating node will be activated, enabling communication using the takeover virtual IP address.

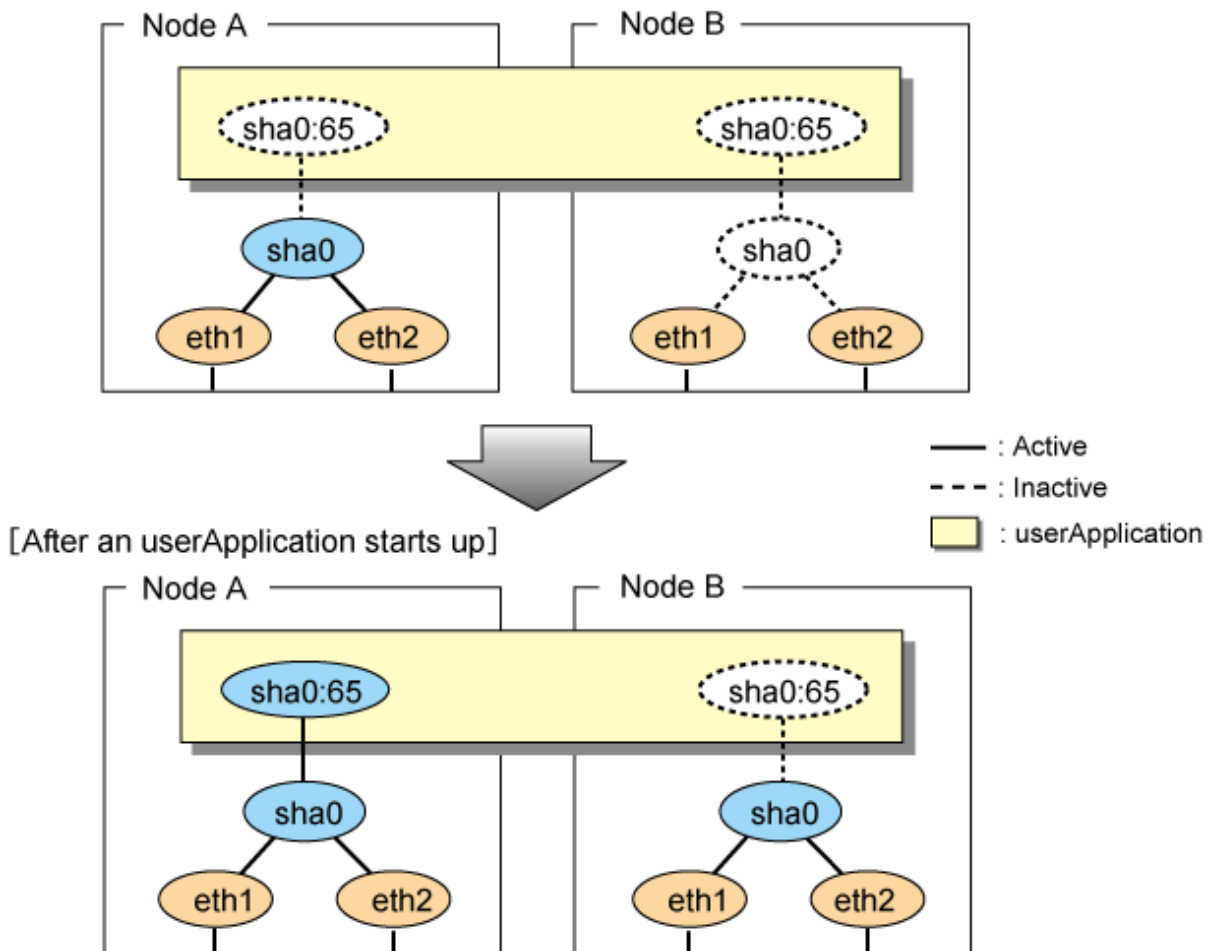
When operating, Fast switching mode uses the redundant line control function to communicate with the remote system.

Note that the virtual interface (such as sha0) is activated just after the redundant line control function starts up.

Once it becomes active, regardless of stopping or restarting userApplication, it remains to be active until the system stops.

Figure 5.4 Startup behavior of Fast switching mode shows behavior of Fast switching mode after starting up

Figure 5.4 Startup behavior of Fast switching mode  
[Before an userApplication starts up]



#### 5.4.1.2 Switching

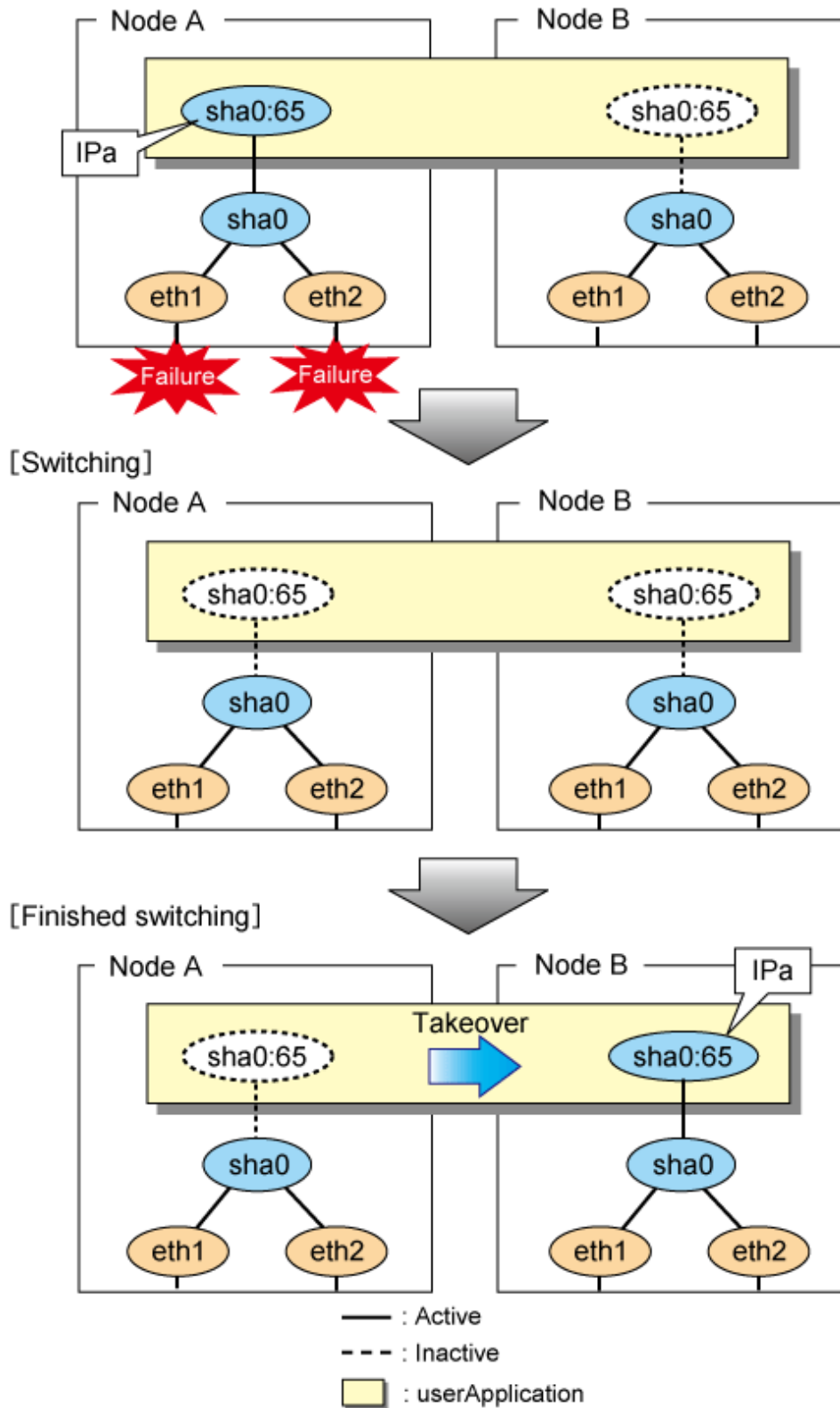
During normal operation, the system communicates with the remote system using Redundant Line Control Function on the operating node.

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.

Figure 5.5 Switching behavior of Fast switching mode indicates switching behavior of Fast switching mode.

In the following figure, the takeover 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 takeover IP address (IPa) becomes active. Note that the virtual interface (sha0) in node A remains unchanged.

Figure 5.5 Switching behavior of Fast switching mode  
[Operating (Failure occurred in node A)]





### 5.4.1.3 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).

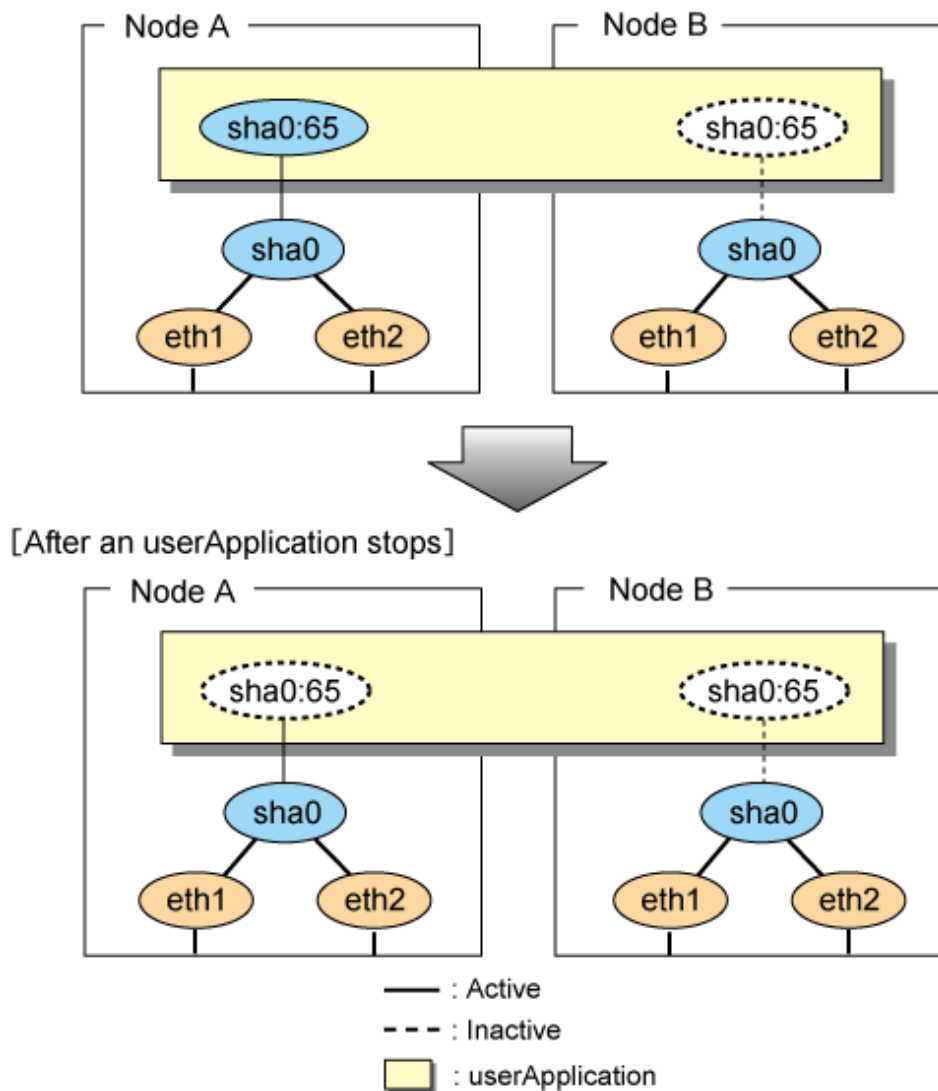
#### 2) Restore the original operation status.

Restore the original operation status by performing fail-back operation for userApplication from "Cluster Admin" in Web-Based Admin View.

### 5.4.1.4 Stopping

Figure 5.6 Stopping behavior of Fast switching mode illustrates stopping process of userApplication.

Figure 5.6 Stopping behavior of Fast switching mode  
[Before an userApplication stops]



## 5.4.2 Active Standby (NIC switching mode)

---

### 5.4.2.1 Starting

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.

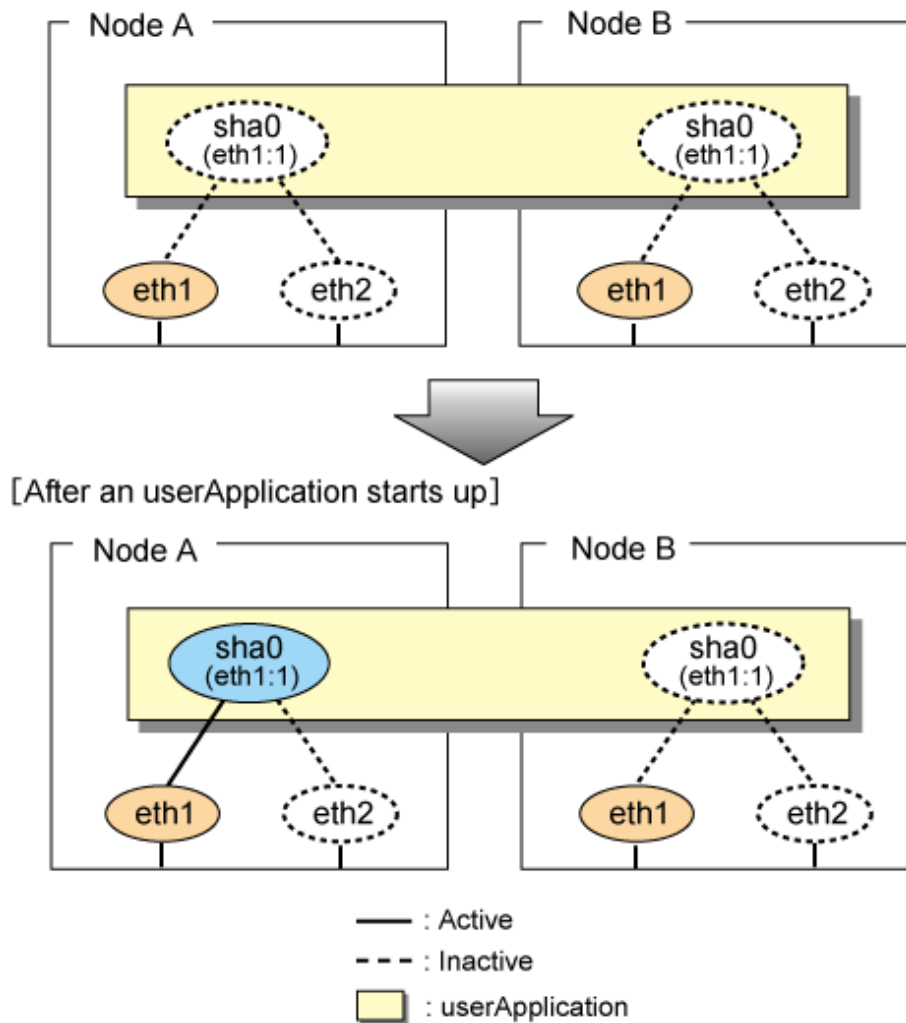
This function allows a connection to be made for each of the active and standby nodes independently. However, IP address of the standby node changes according to the status transition of the userApplication. Thus, when clusters are switched, the TCP connection to the standby node is cleared. For the 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 5.7 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 (eth1:1) of the secondary interface (eth1) is assigned the takeover virtual IP address (IP-A) and activated. If switching occurs due to a failure, the takeover virtual interface (eth1:1) that has been assigned the takeover IP address (IP-A) is inactivated. Then, on standby node B, the logical interface (eth0:1) that has been assigned the takeover IP address (IP-A) on the already activated primary interface (eth0) is activated.

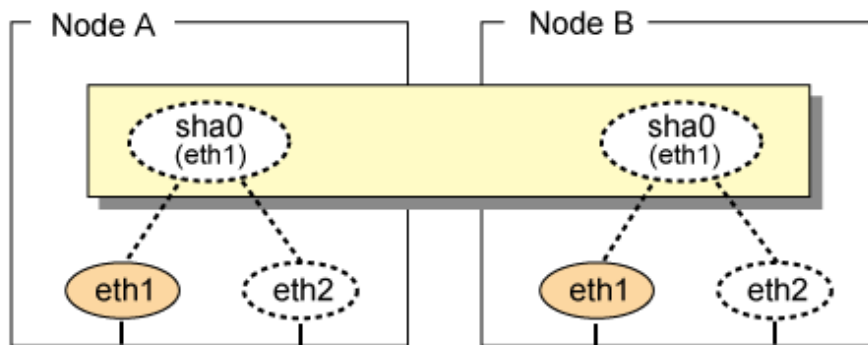
Figure 5.7 Startup behavior of NIC switching mode (take over logical IP)  
[Before an userApplication starts up]



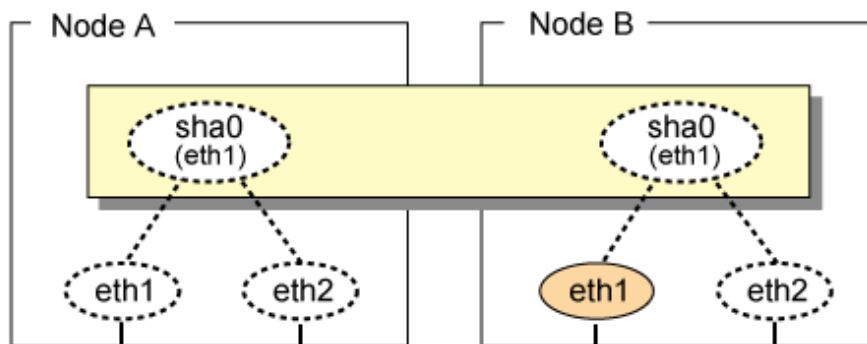
For taking over physical IP address I, activate the physical interface (eth1) for operating node and standby node when the redundant line control function starts up. After the userApplication starts, it will activate the physical interface by allocating a takeover IP address to the physical interface on the operating node. At this time, a physical interface (eth1) over the standby node remains to be inactive.

Figure 5.8 Startup behavior of NIC switching mode (takeover physical IP address I) shows a startup behavior of takeover physical IP address I

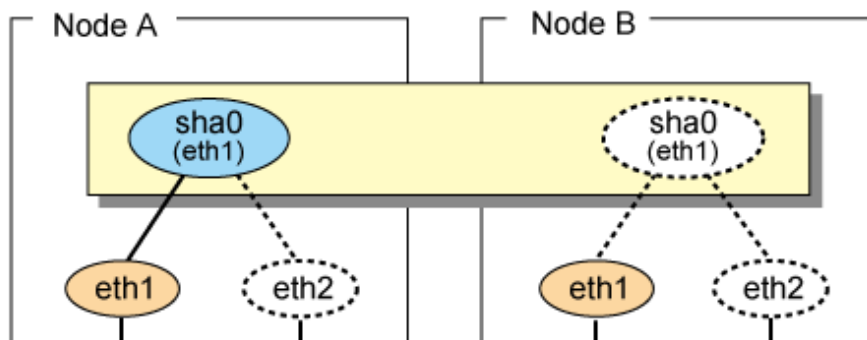
Figure 5.8 Startup behavior of NIC switching mode (takeover physical IP address I)  
[Before an userApplication starts up]



[Starting an userApplication]



[After an userApplication starts up]

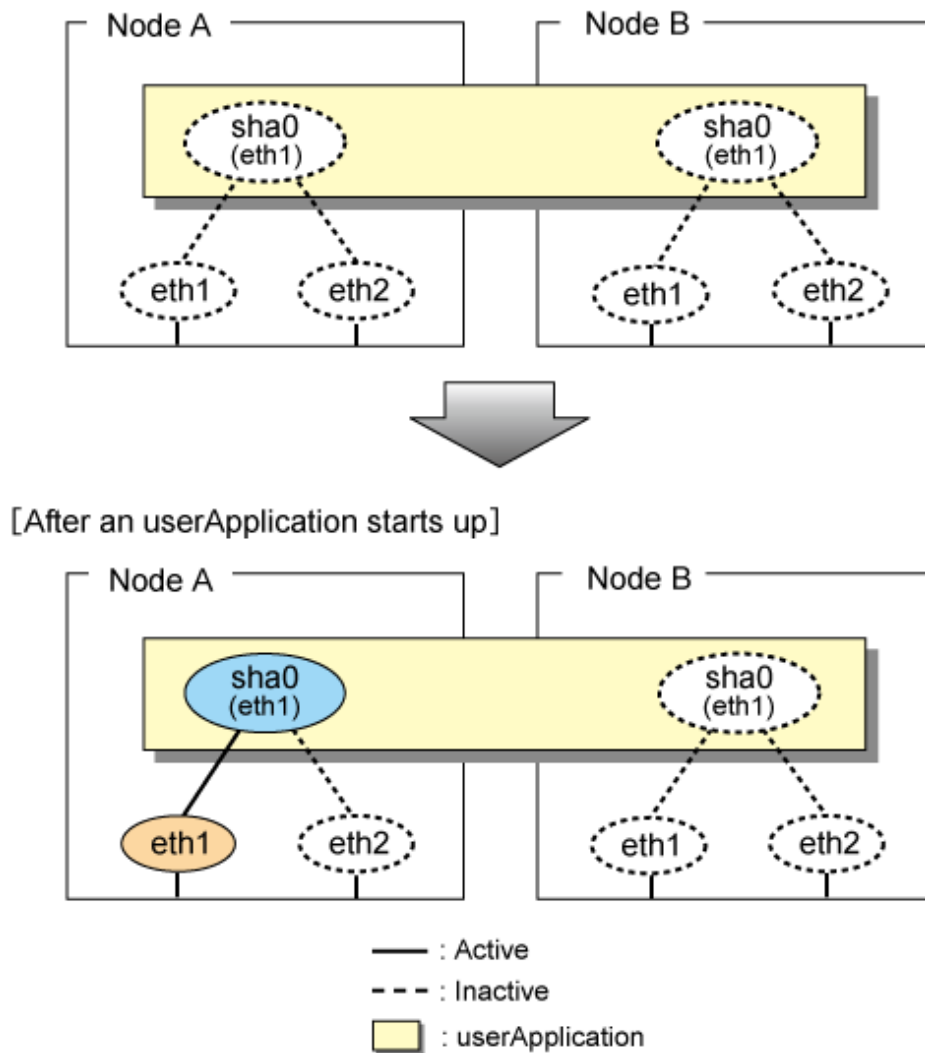


— : Active  
 --- : Inactive  
 [Yellow Box] : userApplication

For taking over physical IP address II, it does not activate the physical interface (eth1) for both operating node and standby node when redundant line control function starts up. Instead it allocates a takeover IP address to the physical interface (eth1) on the operating node and then it activates the physical interface. In this case, the physical interface (eth1) for standby node remains inactive.

Figure 5.9 Startup behavior of NIC switching mode (takeover physical IP address II) shows a startup behavior of the takeover physical IP address II

Figure 5.9 Startup behavior of NIC switching mode (takeover physical IP address II)  
[Before an userApplication starts up]



### 5.4.2.2 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.

[Figure 5.10 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 takeover virtual IP address (IPa) in the operating node A is allocated to the logical interface (eth2.1) for the secondary interface. Once IPa is allocated, the logical interface (eth2.1) 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 takeover IP address (IPa) in the operating node A. Then it allocates the takeover IP address to the primary interface (eth1) and finally activates the logical interface (eth1:1).

Figure 5.10 Switching behavior of NIC switching mode (takeover logical IP)  
[Operating (Failure occurred in node A)]

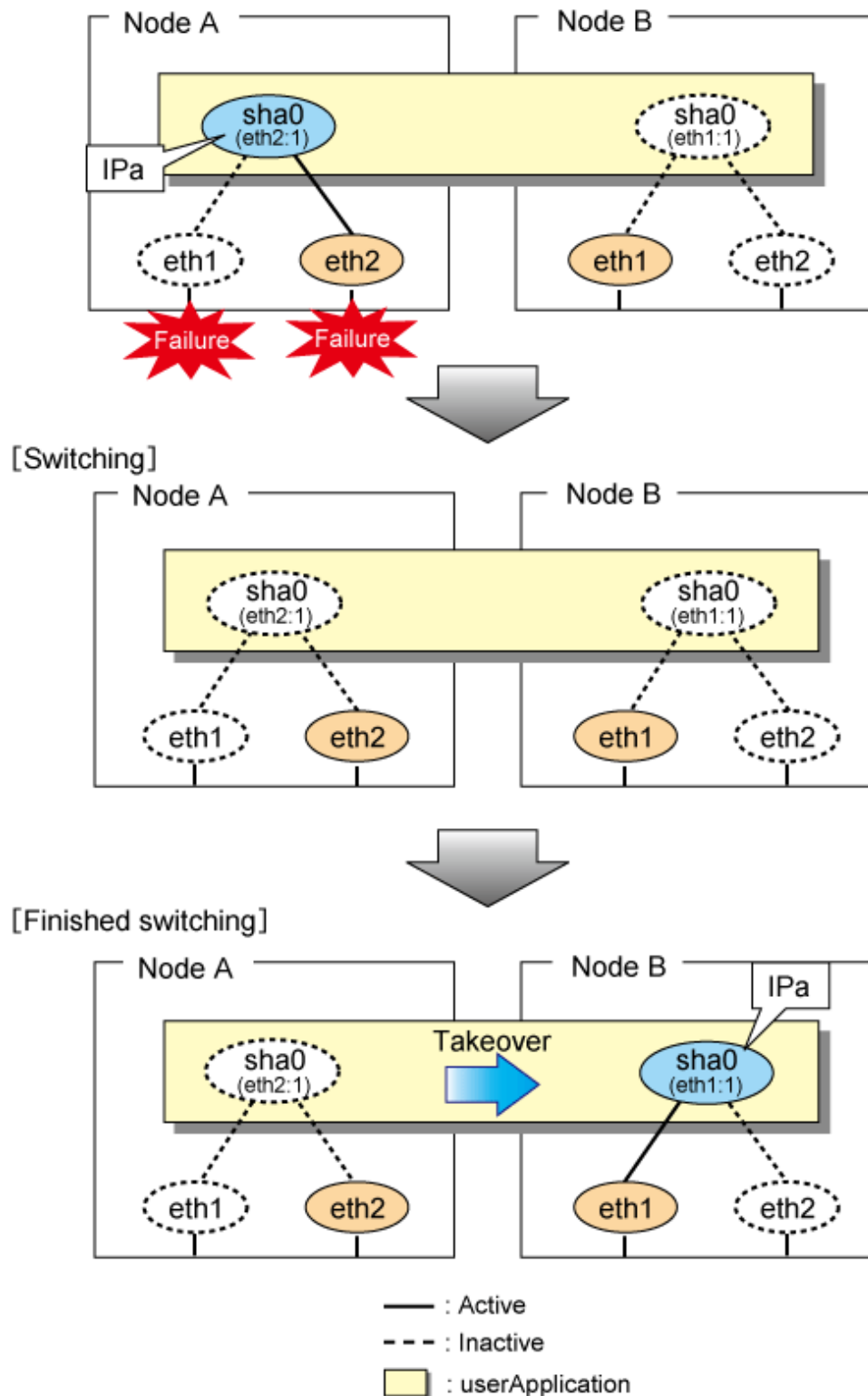


Figure 5.11 Switching behavior of NIC switching mode (takeover physical IP I) (continued) and Figure 5.12 Switching behavior of NIC switching mode (takeover physical IP I) (end) illustrate switching behavior of NIC switching mode (takeover physical IP address I).

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 (eth1), which has been active in the standby node B. Then it allocates the takeover IP address (IPa) to activate the primary interface (eth1). Once the primary interface activates, different IP address is allocated to the secondary interface (eth2) by means of inactivating eth2.

Figure 5.11 Switching behavior of NIC switching mode (takeover physical IP I) (continued)  
[Operating (Failure occurred in node A)]

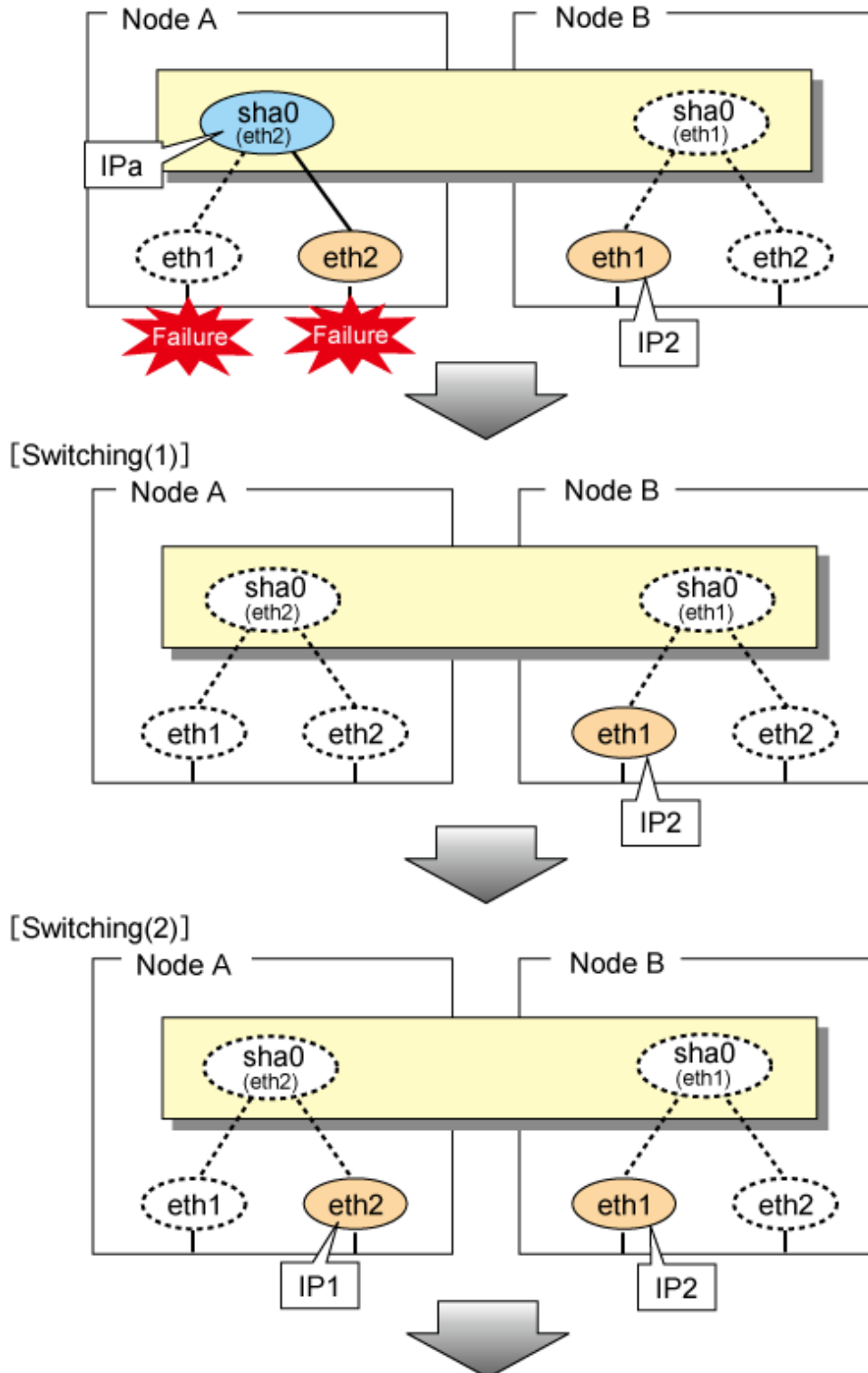


Figure 5.12 Switching behavior of NIC switching mode (takeover physical IP I) (end)  
[Switching(3)]

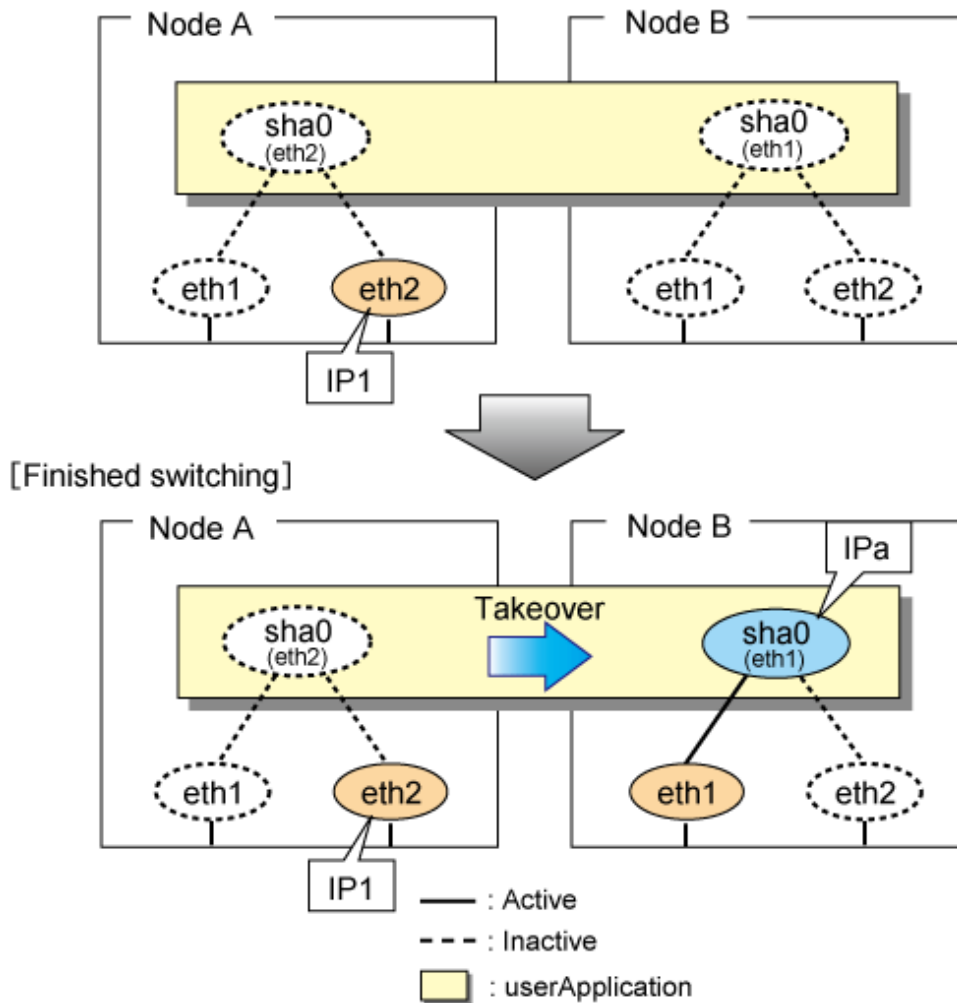


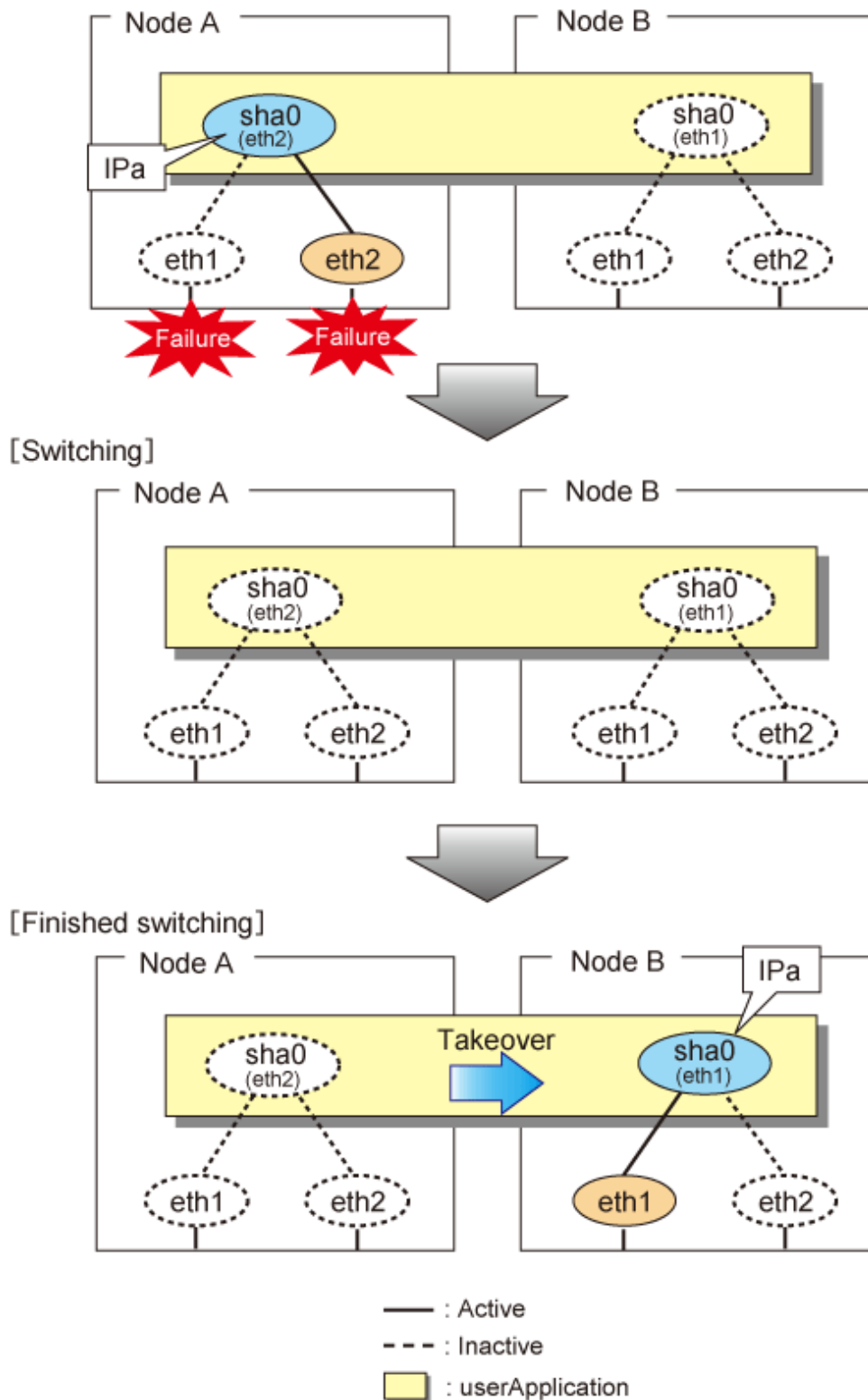
Figure 5.13 Switching behavior of NIC switching mode (takeover physical IP address II) illustrates switching behavior of NIC switching mode (takeover physical IP address II).

In the following figure, the takeover 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 takeover IP address (IPa) to the primary interface (eth1). After the IP address is successfully passed over to the standby node, the secondary interface (eth2), which previously owned the takeover IP address (IPa) in node A becomes inactive.



Figure 5.13 Switching behavior of NIC switching mode (takeover physical IP address II)  
 [Operating (Failure occurred in node A)]



### 5.4.2.3 Fail-back

The procedure for performing fail-back is the same as in Fast switching mode. For details, see "[5.4.1.3 Fail-back](#)".

#### 5.4.2.4 Stopping

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 stops]

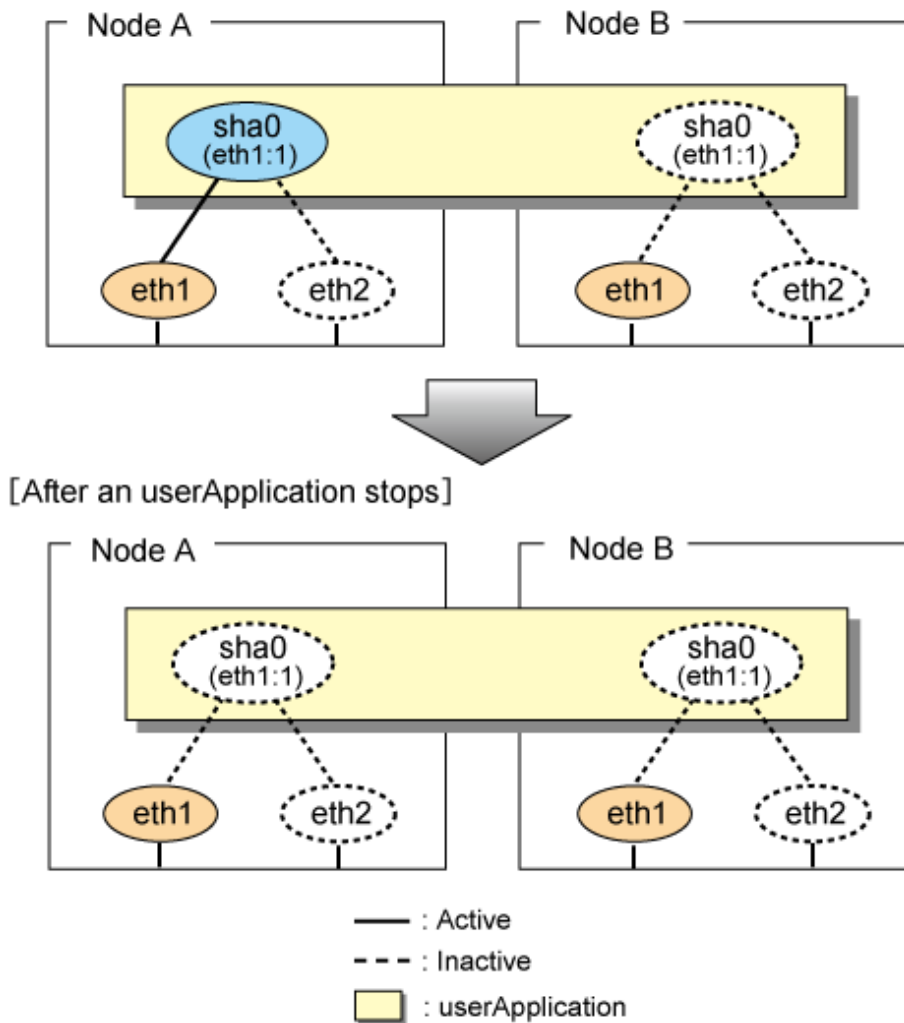
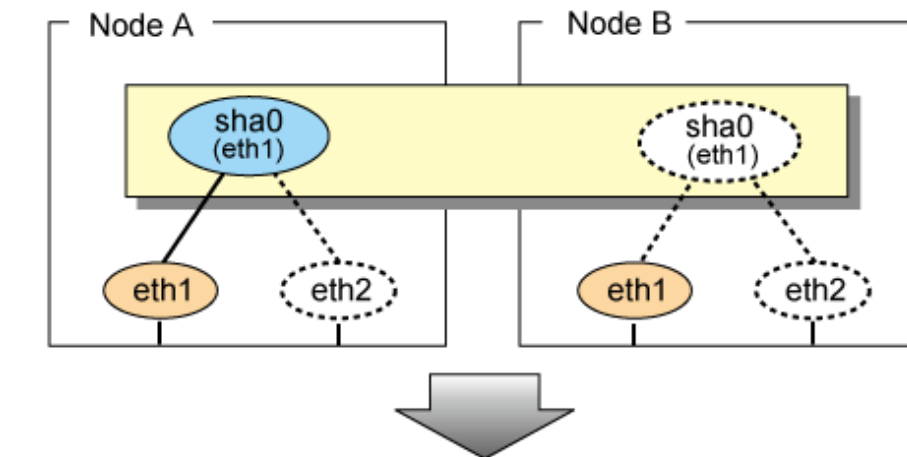
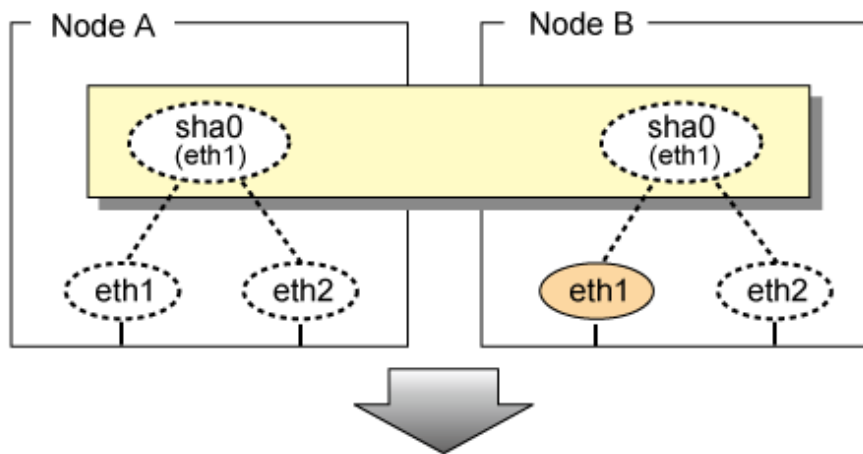


Figure 5.15 Stopping process of NIC switching mode (physical IP takeover I) illustrates stopping behavior of userApplication for the physical IP takeover I.

Figure 5.15 Stopping process of NIC switching mode (physical IP takeover I)  
[Before an userApplication stops]



[Stopping]



[After an userApplication stops]

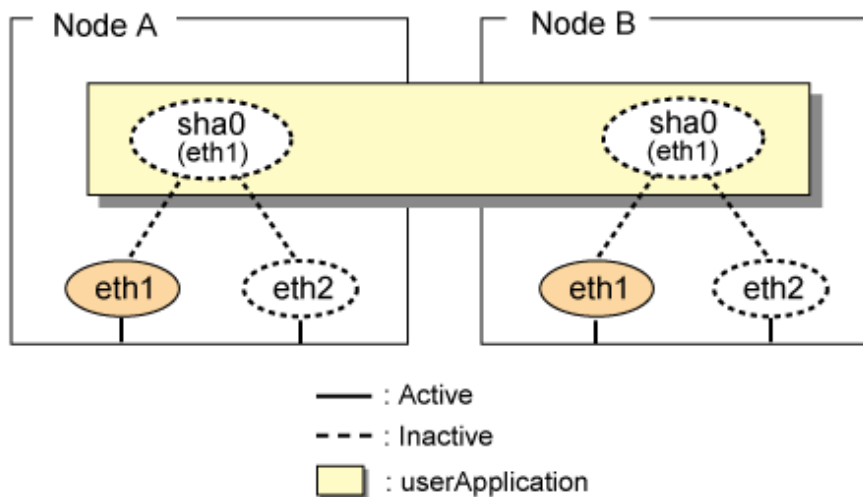
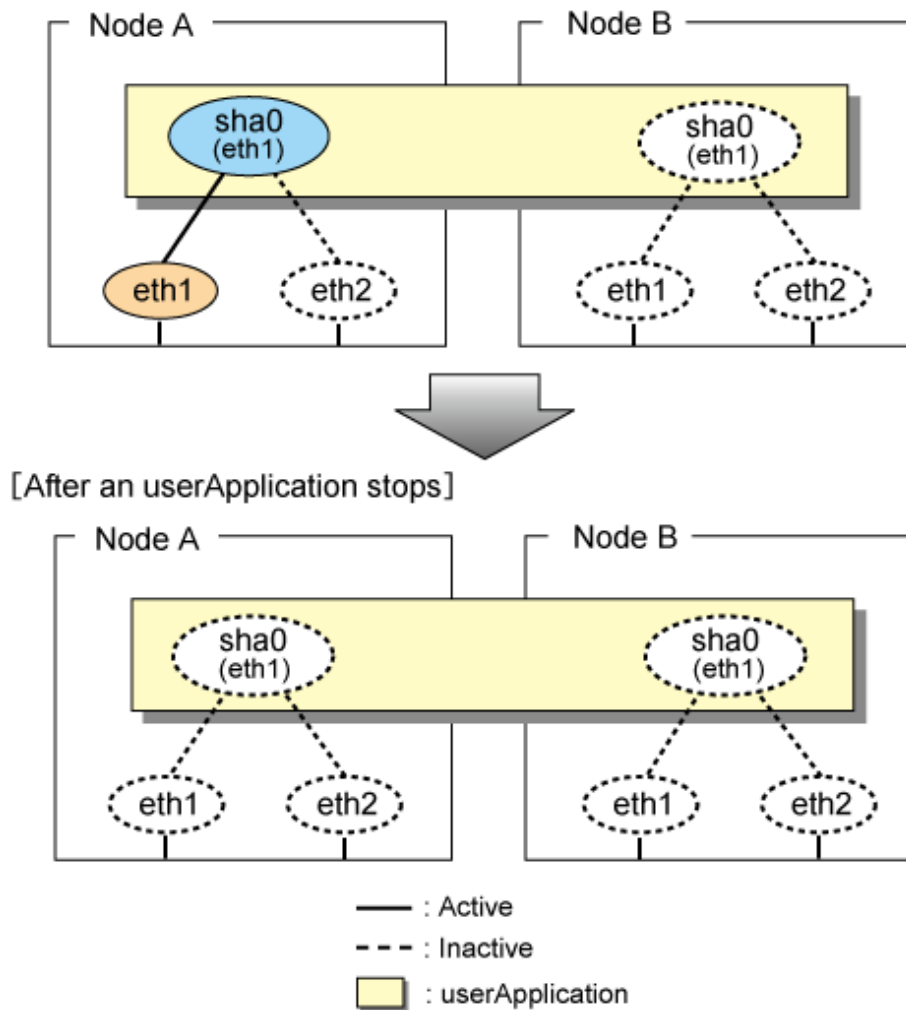


Figure 5.16 Stopping process of NIC switching mode (physical IP takeover II) illustrates stopping behavior of userApplication for the physical IP takeover II.

Figure 5.16 Stopping process of NIC switching mode (physical IP takeover II)  
[Before an userApplication stops]



### 5.4.3 Active Standby (Virtual NIC mode)

#### 5.4.3.1 Starting

With userApplication startup, the takeover virtual interface (`sha0:65`) over operating node will be activated, enabling communication using the takeover virtual IP address.

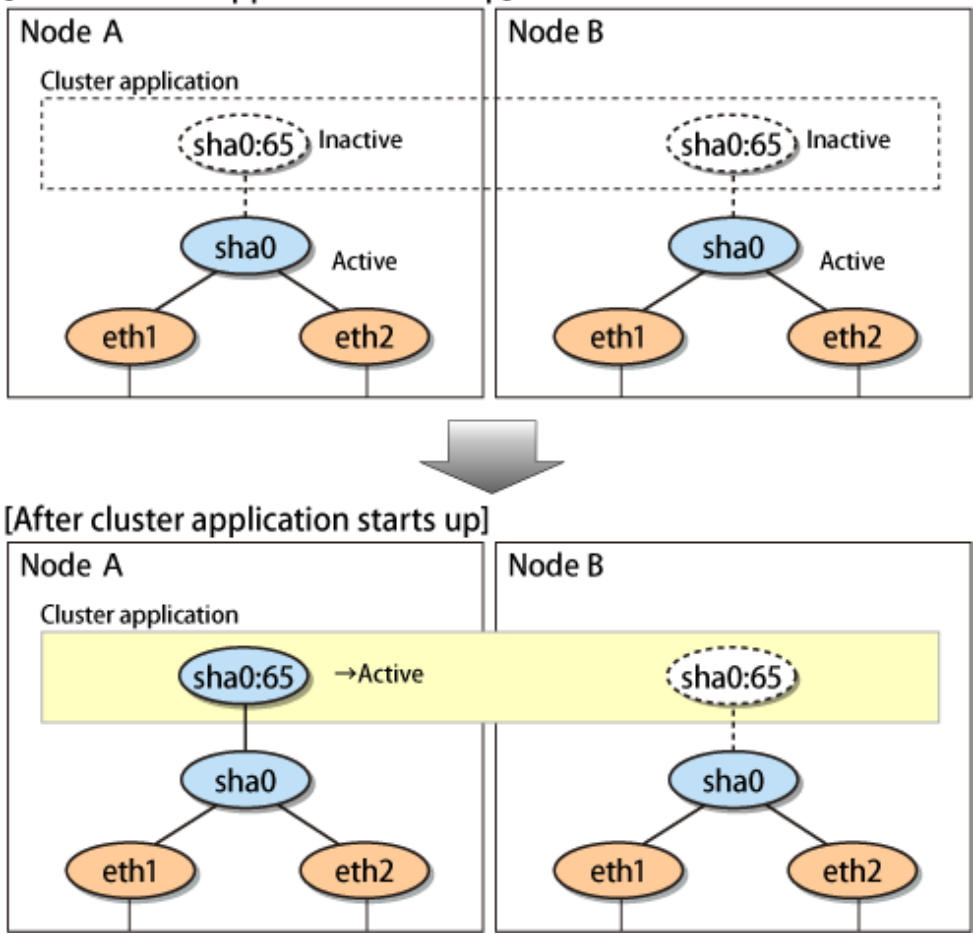
When operating, Virtual NIC mode uses the redundant line control function to communicate with the remote system.

Note that the virtual interface (such as `sha0`) is activated just after the redundant line control function starts up.

Once it becomes active, regardless of stopping or restarting userApplication, it remains to be active until the system stops.

Figure 5.17 Startup behavior of Virtual NIC mode shows behavior of Virtual NIC mode after starting up

Figure 5.17 Startup behavior of Virtual NIC mode  
**[Before cluster application starts up]**



### 5.4.3.2 Switching

During normal operation, the system communicates with the remote system using Redundant Line Control Function on the operating node.

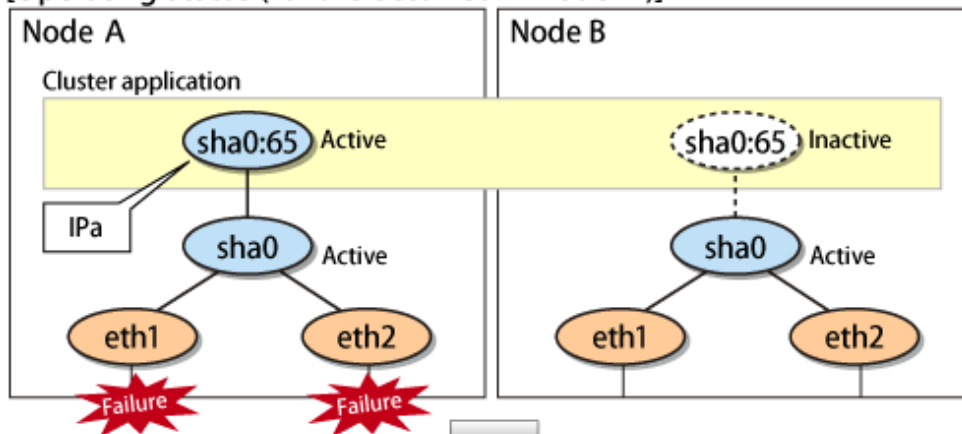
If a failure (panic, hang-up, or line failure) occurs on the operating node, Redundant Line Control Function switches the resources to the standby node. Then, applications make reconnection to take over the communication from the operating node.

**Figure 5.18 Switching behavior of Virtual NIC mode** indicates switching behavior of Virtual NIC mode.

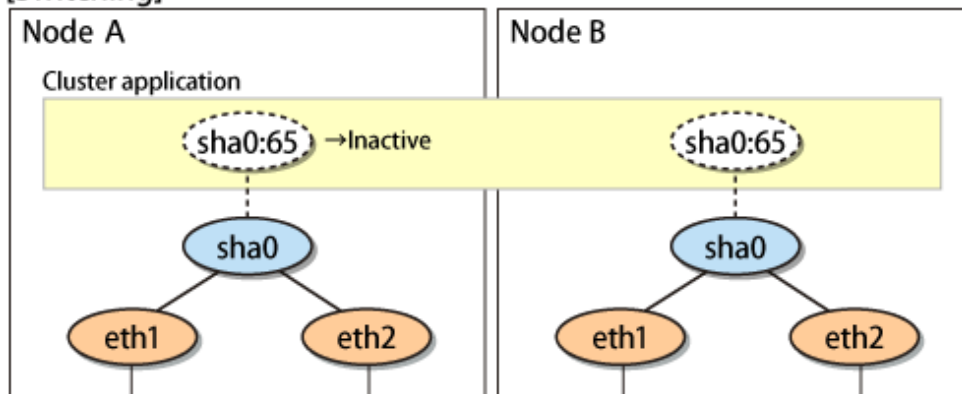
In the following figure, the takeover IP address (IPa) is allocated to the takeover virtual interface (`sha0:65`) for operating node A. Then it activates the takeover virtual interface. When switching the interface due to failures in the transfer path, the takeover virtual interface (`sha0:65`) for operating node A becomes inactive. Then in standby node B, the takeover virtual interface (`sha0:65`), which has allocated the takeover IP address (IPa) becomes active. Note that the virtual interface (`sha0`) in node A remains unchanged.

Figure 5.18 Switching behavior of Virtual NIC mode

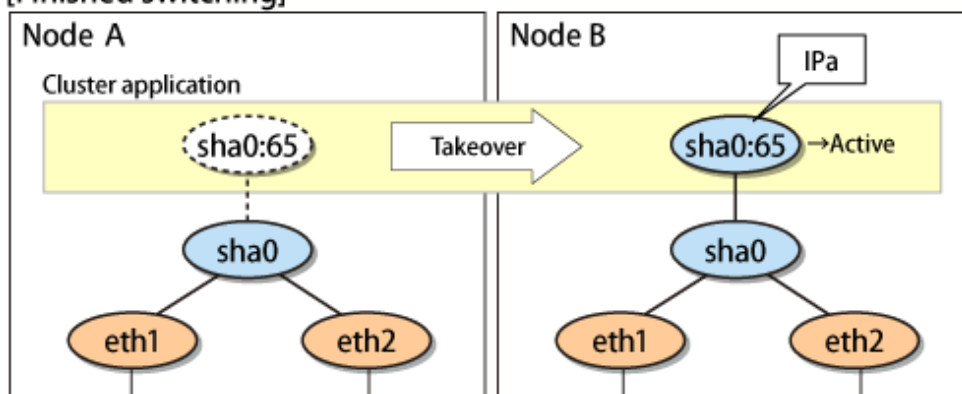
[Operating Status (Failure occurred in node A)]



[Switching]



[Finished switching]



### Point

The switching operation on the cluster system can be suppressed. For details on the switching operation of suppression function, see "[7.12 hanetpathmon Command](#)".

### 5.4.3.3 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.

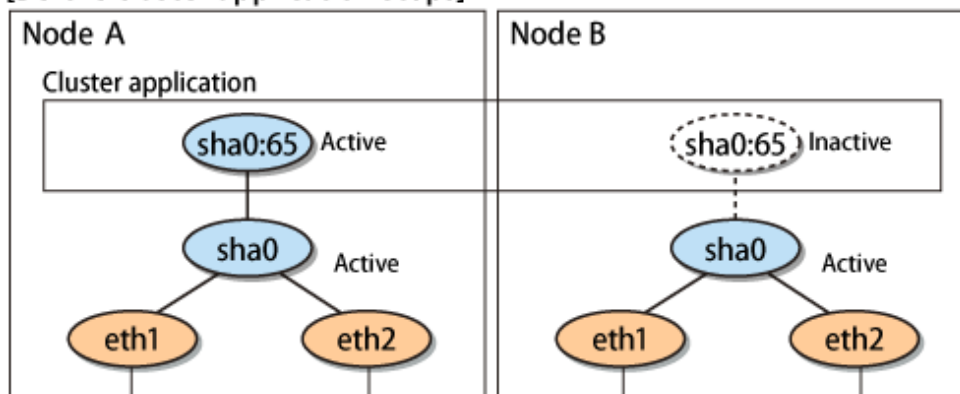
Restore the original operation status by performing fail-back operation for userApplication from "Cluster Admin" in Web-Based Admin View.

## 5.4.3.4 Stopping

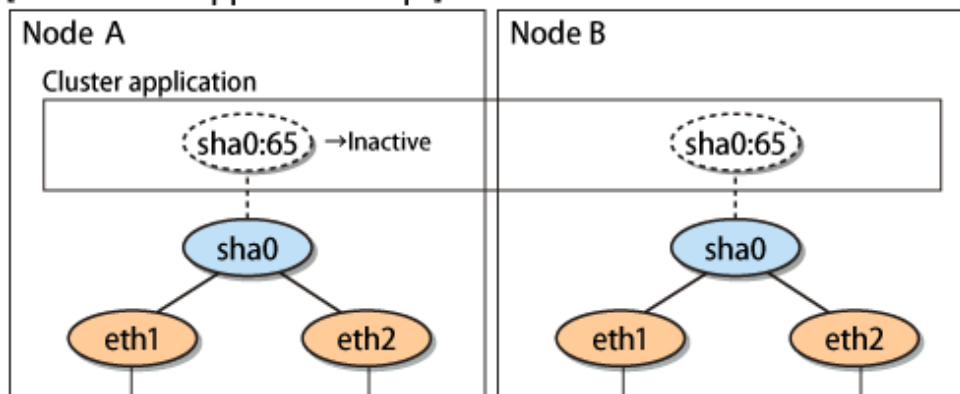
Figure 5.19 Stopping behavior of Virtual NIC mode illustrates stopping process of userApplication.

Figure 5.19 Stopping behavior of Virtual NIC mode

[Before cluster application stops]



[After cluster application stops]



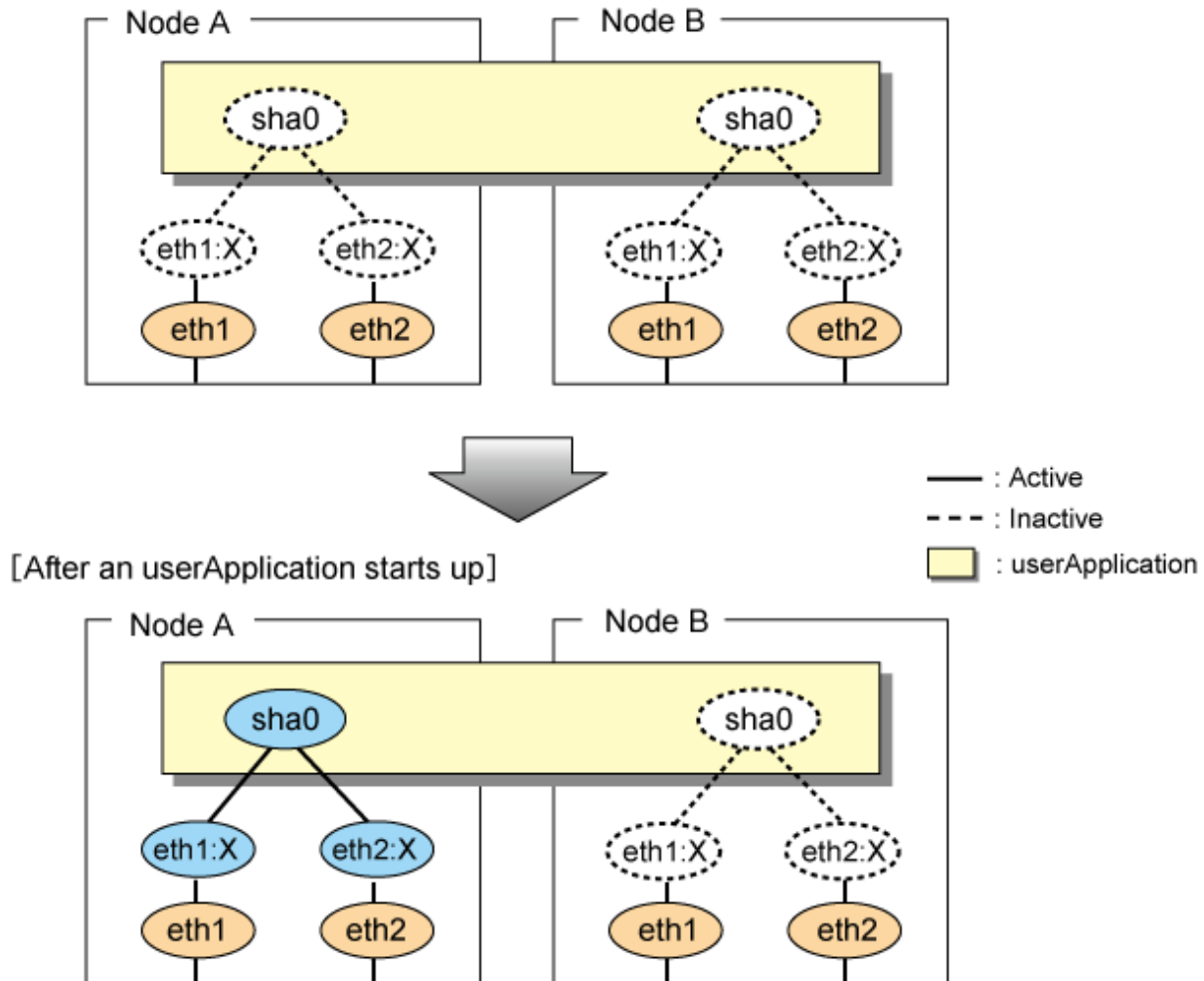
## 5.4.4 Active Standby (GS linkage mode)

### 5.4.4.1 Starting

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 linkage mode uses the Redundant Line Control function to communicate with the remote system.

Figure 5.20 Startup behavior of GS linkage mode shows startup behavior of GS linkage mode

Figure 5.20 Startup behavior of GS linkage mode  
[Before an userApplication starts up]



#### Note

Activate logical interfaces (eth1:X, eth2:X) only when they are connected to GS via router.

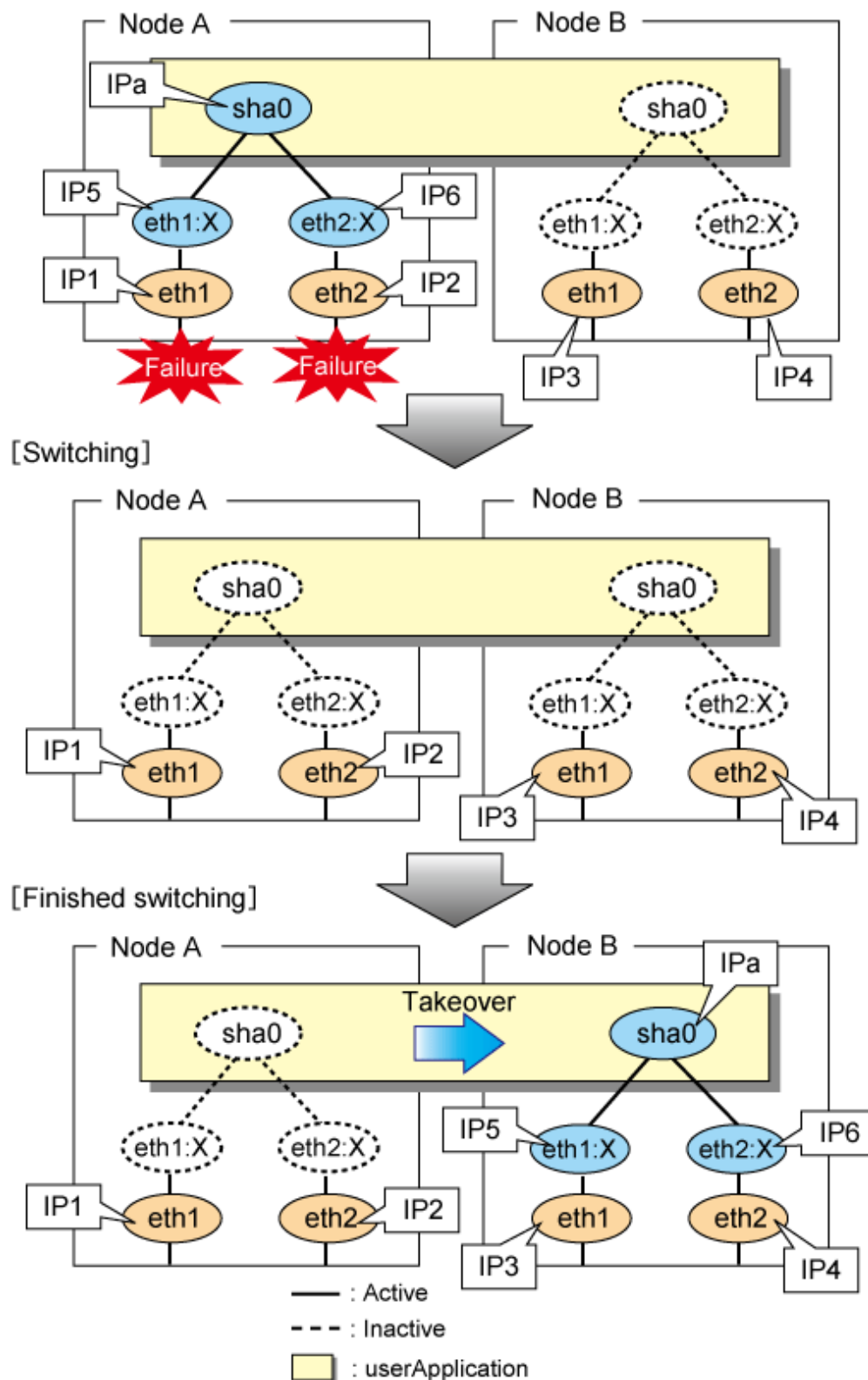
### 5.4.4.2 Switching

Figure 5.21 Switching behavior of GS linkage mode illustrates switching behavior of GS 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 physical interfaces (eth1:X, eth2:X) in node A. On standby node B, it activates the takeover virtual interface (sha0), which bundles the physical interfaces (eth1, eth2).



Figure 5.21 Switching behavior of GS linkage mode  
[Operating (Failure occurred in node A)]



#### Note

Activate or deactivate logical interfaces (eth1:X, eth2:X) only when they are connected to GS via router.

### 5.4.4.3 Fail-back

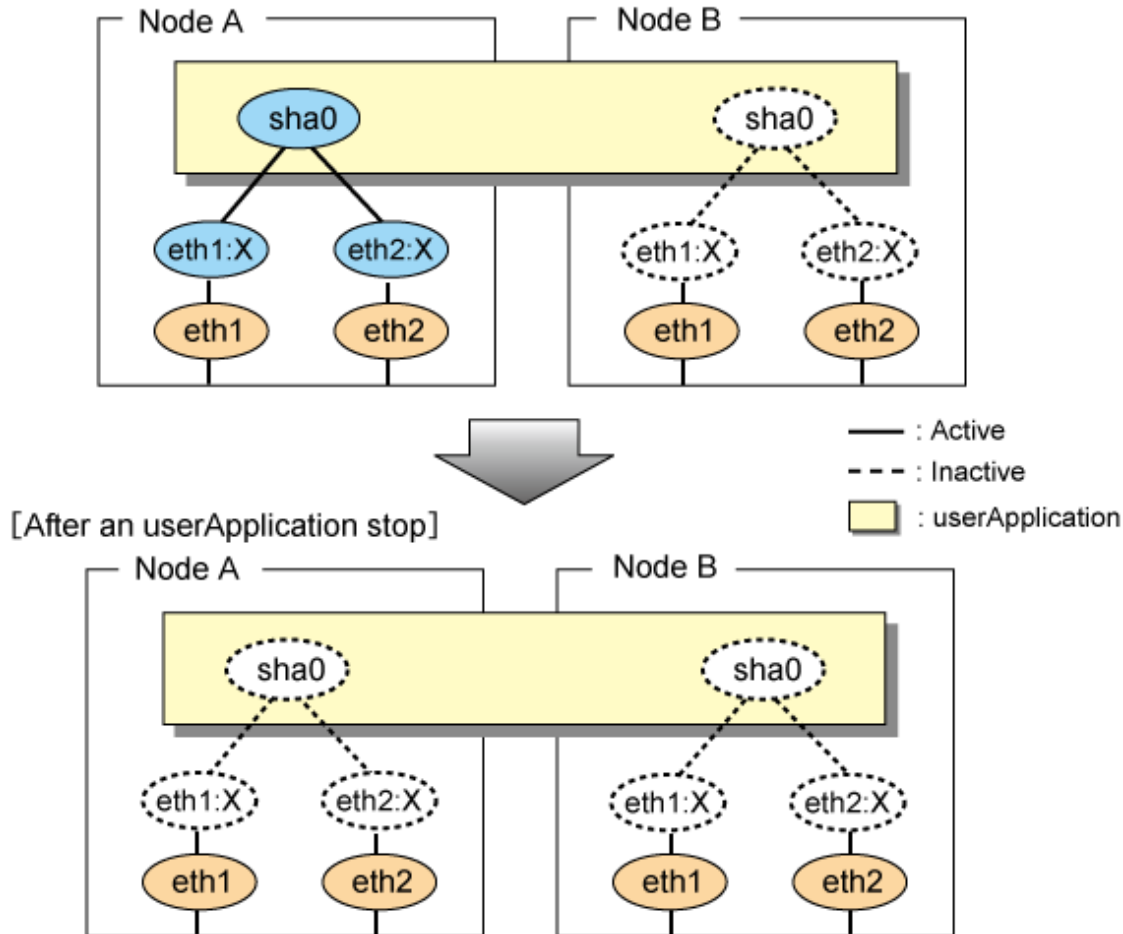
The procedure for performing fail-back is the same as in Fast switching mode. For details, see "5.4.1.3 Fail-back".

### 5.4.4.4 Stopping

Figure 5.22 Stopping process of GS linkage mode illustrates stopping behavior of userApplication.

Figure 5.22 Stopping process of GS linkage mode

[Before an userApplication stop]



#### Note

Activate or deactivate logical interfaces (eth1:X, eth2:X) only when they are connected to GS via router.

## 5.4.5 Mutual standby (Fast switching mode)

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

### 5.4.5.1 Starting

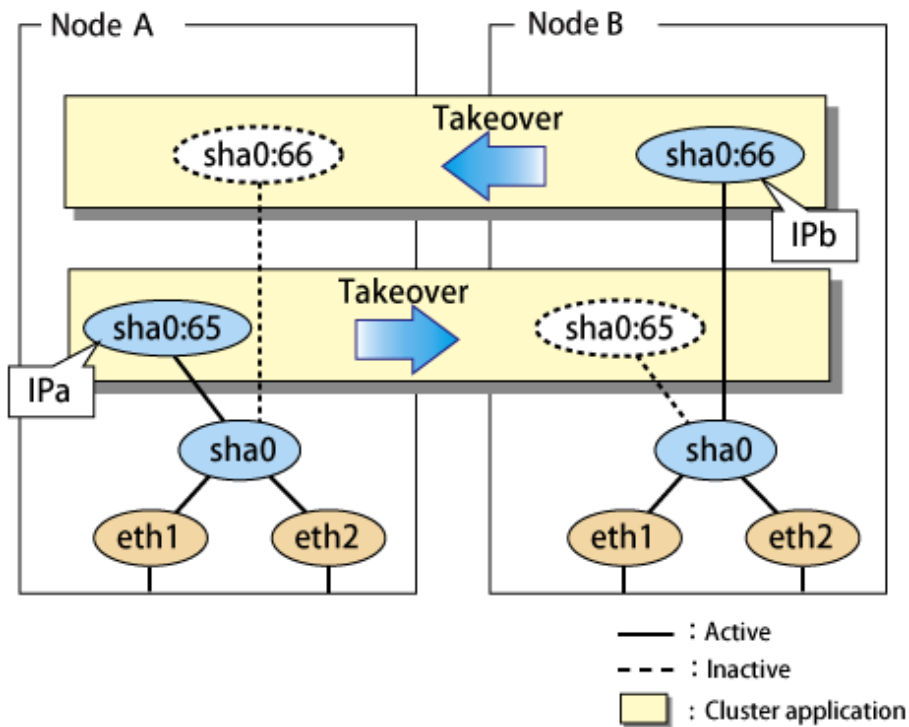
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "5.4.1.1 Starting".

### 5.4.5.2 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.

Figure 5.23 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 more information, see "5.4.1.2 Switching".

Figure 5.23 Mutual standby configuration diagram in Fast switching mode



### 5.4.5.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For details, see "5.4.1.3 Fail-back".

### 5.4.5.4 Stopping

Stopping operation is equivalent to active standby connection. For details, see "5.4.1.4 Stopping".

## 5.4.6 Mutual standby (NIC switching mode)

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

### 5.4.6.1 Starting

Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "5.4.2.1 Starting".

### 5.4.6.2 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.

Figure 5.24 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 more information, see "5.4.2.2 Switching".

Figure 5.24 Mutual standby configuration diagram in NIC switching mode (NIC non-sharing)

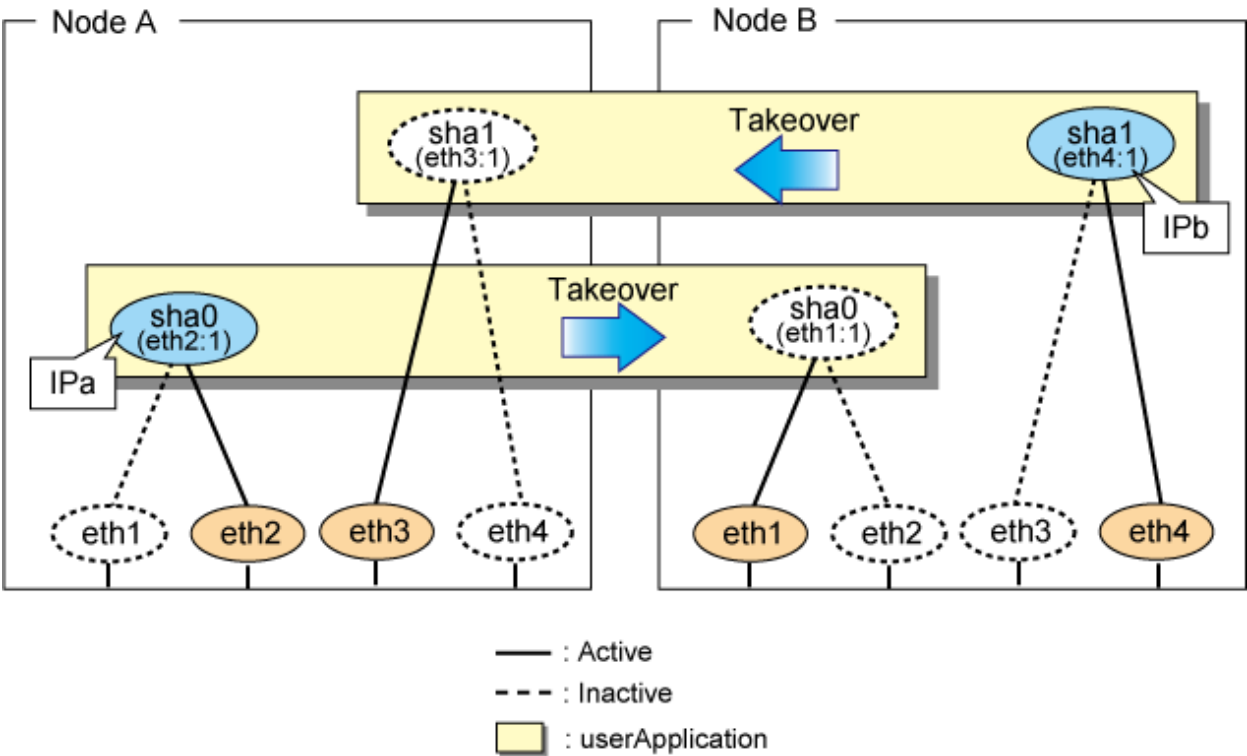
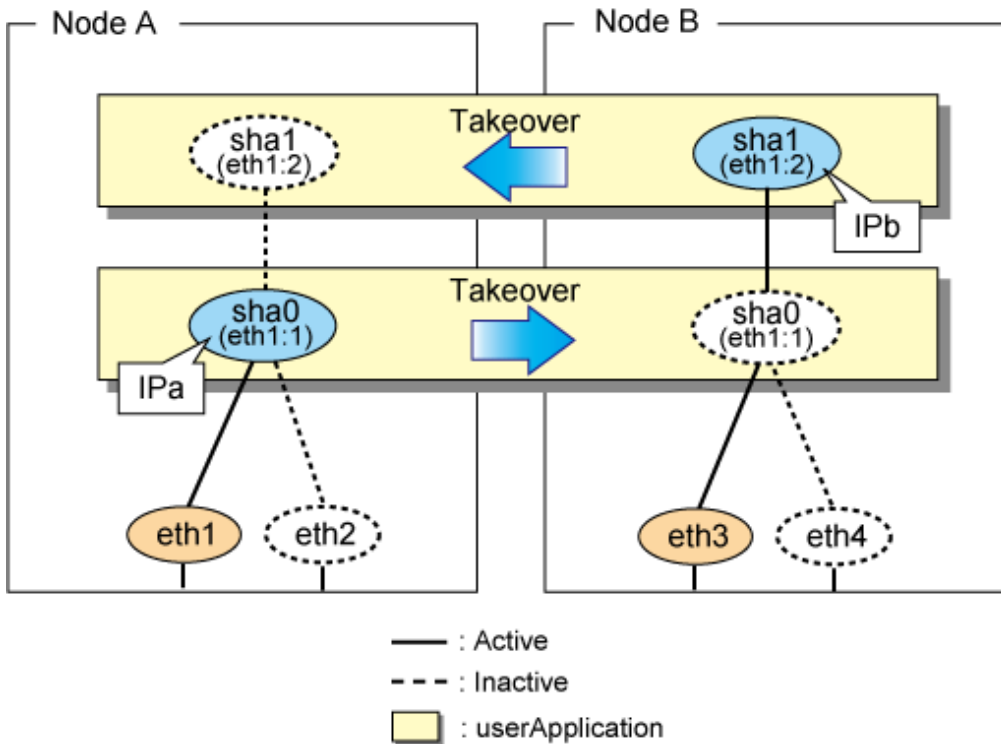


Figure 5.25 Mutual standby configuration diagram in NIC switching mode (NIC sharing) shows the mutual standby configuration diagram in NIC switching mode (NIC sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For more information, see "5.4.2.2 Switching".

Figure 5.25 Mutual standby configuration diagram in NIC switching mode (NIC sharing)



#### 5.4.6.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For details, see "[5.4.1.3 Fail-back](#)".

#### 5.4.6.4 Stopping

Stopping operation is equivalent to active standby connection. For details, see "[5.4.2.4 Stopping](#)".

### 5.4.7 Mutual standby (Virtual NIC mode)

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

#### 5.4.7.1 Starting

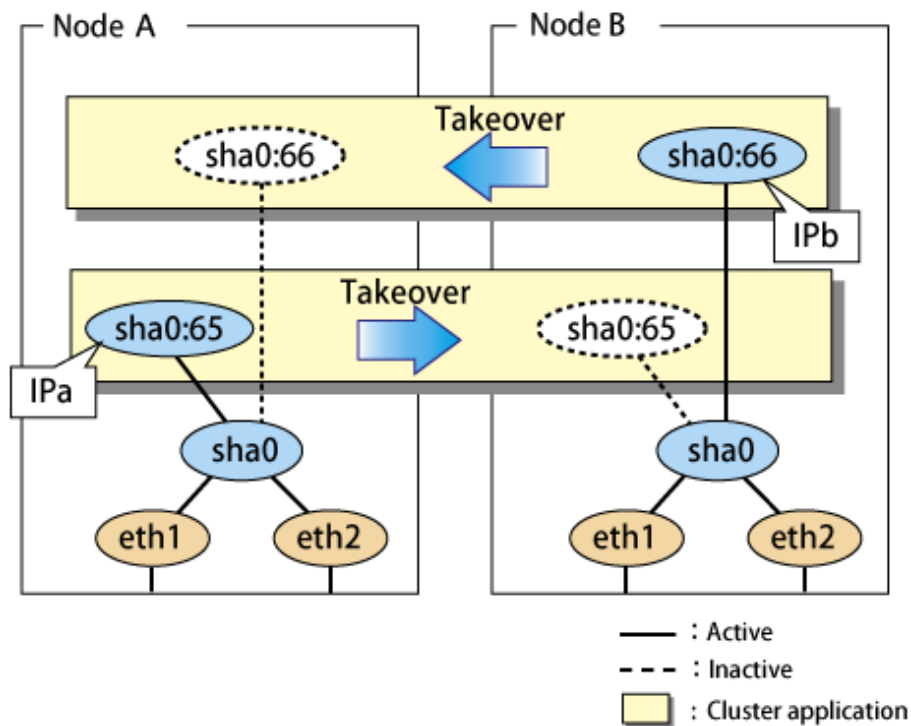
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "[5.4.3.1 Starting](#)".

#### 5.4.7.2 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.

[Figure 5.26 Mutual standby configuration diagram in Virtual NIC mode](#) shows the mutual standby configuration diagram of duplicated operation in Virtual NIC mode. The takeover of an address, etc. is performed in the same way as for the active standby configuration. For more information, see "[5.4.3.2 Switching](#)".

Figure 5.26 Mutual standby configuration diagram in Virtual NIC mode



### 5.4.7.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For details, see ["5.4.3.3 Fail-back"](#).

### 5.4.7.4 Stopping

Stopping operation is equivalent to active standby connection. For details, see ["5.4.3.4 Stopping"](#).

## 5.4.8 Mutual standby (GS linkage mode)

A mutual standby operation can be achieved by defining several virtual interfaces and by configuring each resource as a separate userApplication.

### 5.4.8.1 Starting

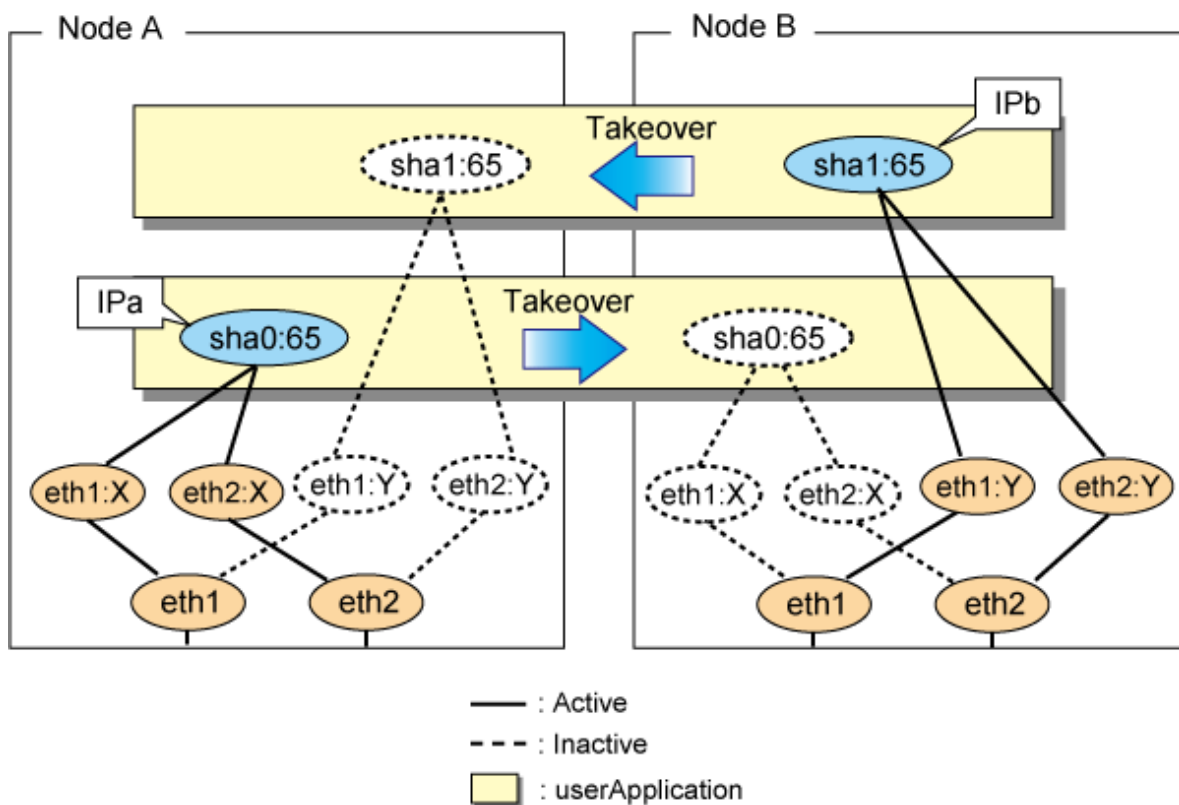
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see ["5.4.4.1 Starting"](#).

### 5.4.8.2 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.

[Figure 5.27 Mutual standby configuration diagram in GS linkage mode](#) shows the mutual standby configuration diagram of duplicated operation in GS linkage mode. The takeover of an address, etc. is performed in the same way as for the active standby configuration. For more information, see ["5.4.4.2 Switching"](#).

Figure 5.27 Mutual standby configuration diagram in GS linkage mode



### 5.4.8.3 Fail-back

The fail-back is performed in the same way as for the active standby configuration. For details, see ["5.4.1.3 Fail-back"](#).

### 5.4.8.4 Stopping

Stopping operation is equivalent to active standby connection. For details, see ["5.4.4.4 Stopping"](#).

## 5.4.9 Cascade (Fast switching mode)

### 5.4.9.1 Starting

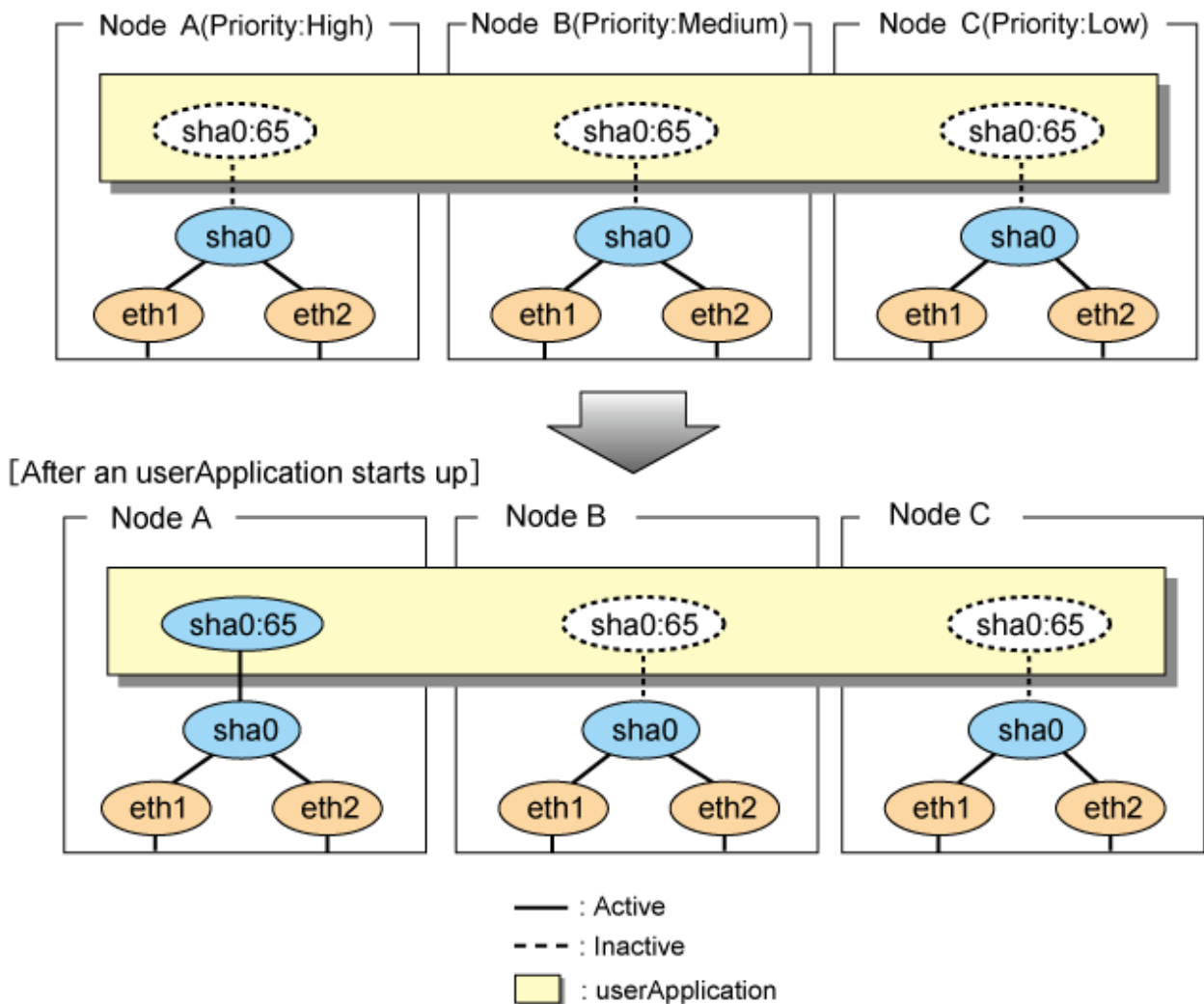
When the userApplication starts up, the takeover virtual interface (sha0:65) becomes active on the operating node, allows to hold communication using the takeover virtual IP address.

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 5.28 Start-up behavior of Fast switching mode](#) illustrates start-up behavior of Fast switching mode

Figure 5.28 Start-up behavior of Fast switching mode  
[Before an userApplication starts up]



#### 5.4.9.2 Switching

During normal operation, userApplication communicates with the remote system using the takeover virtual interface on the operating node.

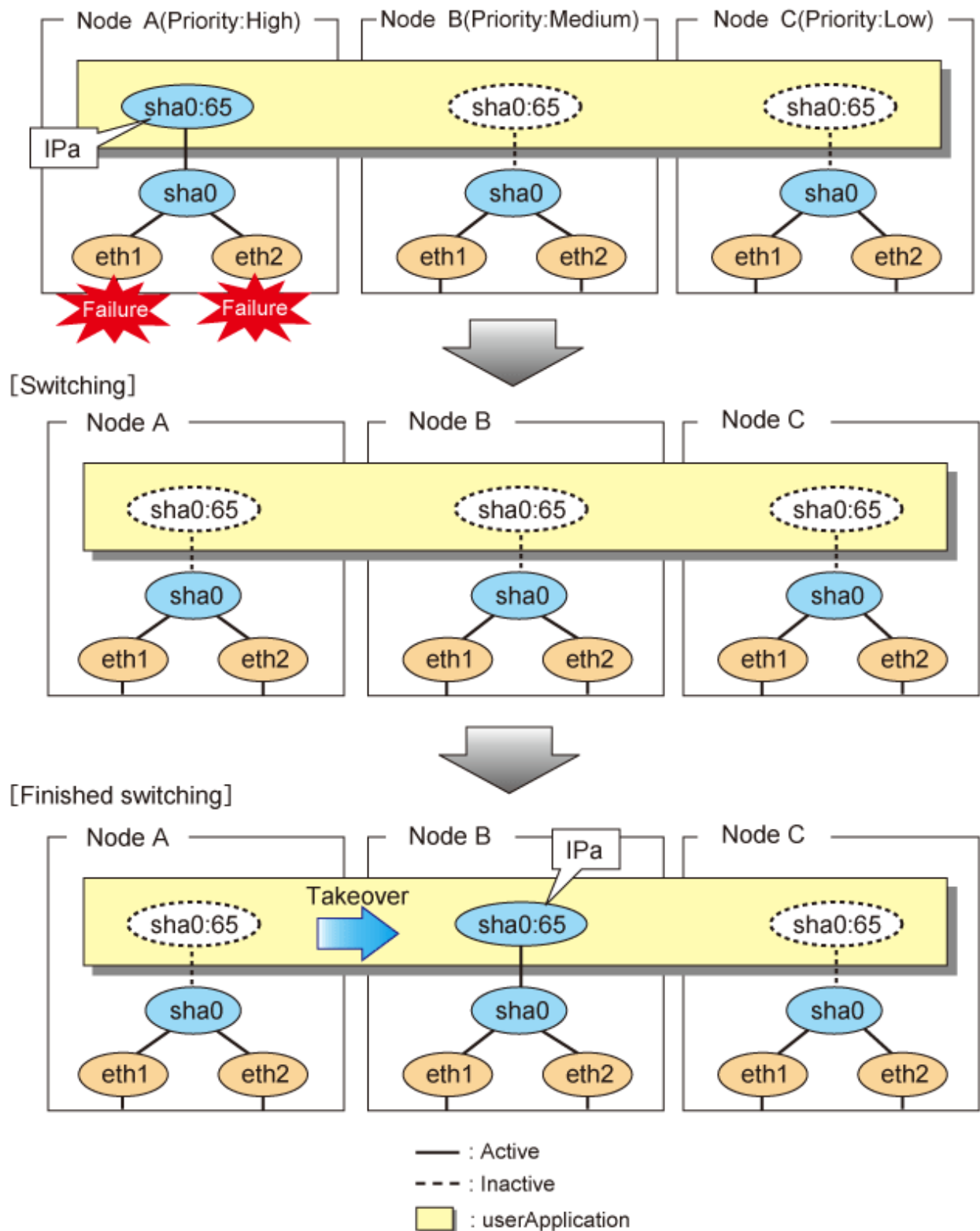
When a failure (panic, hang, detecting failure in transfer route) occurs in the operating node, redundant control function allows switching to the standby node, which has a higher priority within a several other standby nodes. It inherits the communication of operating node by reconnecting to the node using the application.

Figure 5.29 Switching operation of Fast switching mode illustrates switching behavior of Fast switching mode.

In the following figure, the takeover 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 takeover IP address (IPa) becomes active. Note that the virtual interface (sha0) in node A stays unchanged.



Figure 5.29 Switching operation of Fast switching mode  
 [Operating Status (Failure occurred in node A)]



### 5.4.9.3 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

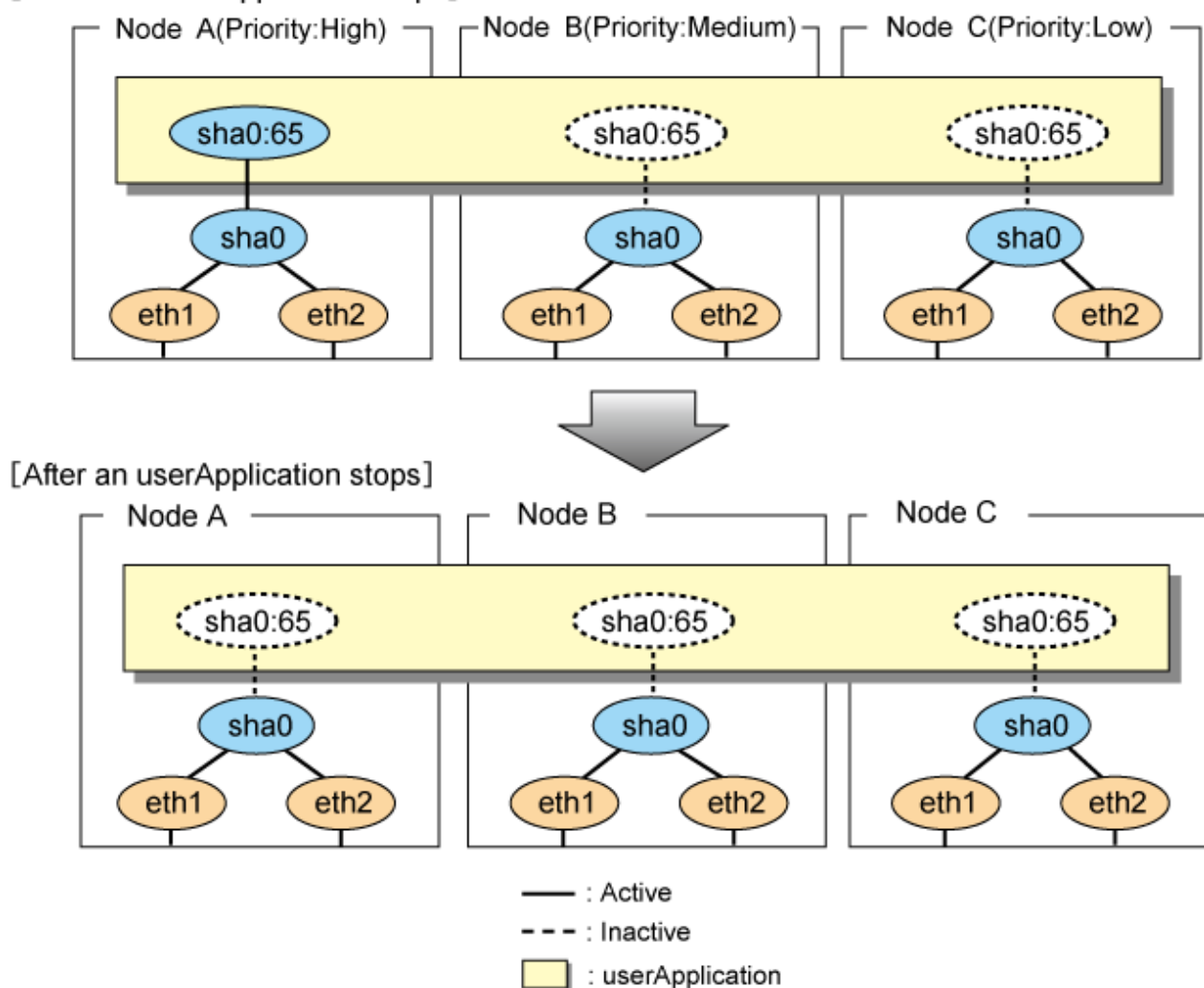
Fail-back the userApplication to an arbitrary node on standby using "Cluster Admin" of Web-Based Admin View.

### 5.4.9.4 Stopping

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 stops]



## 5.4.10 Cascade (NIC switching mode)

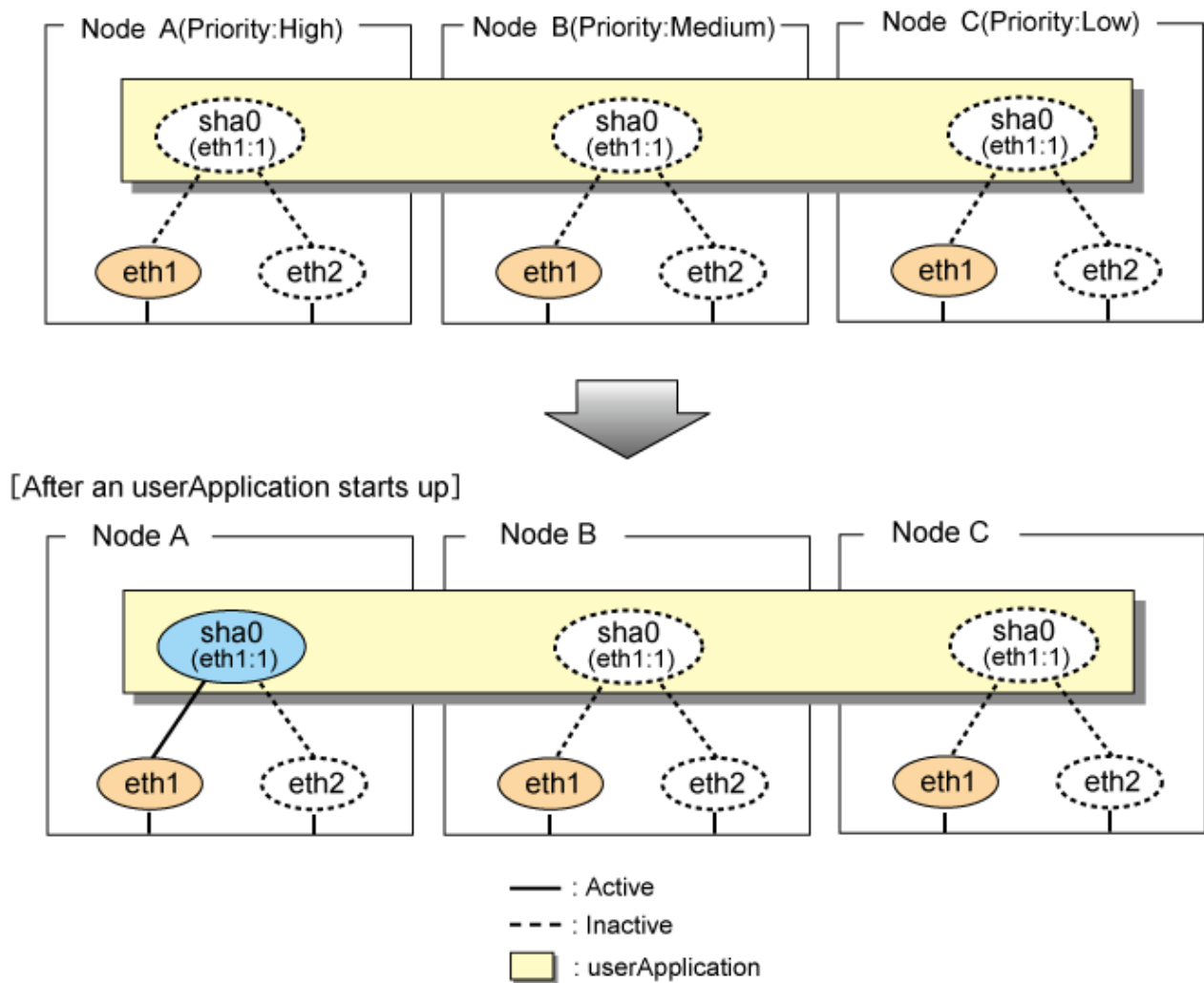
### 5.4.10.1 Starting

There are three types of IP takeover feature in NIC switching mode. For detail, refer to "5.4.2.1 Starting".

The physical interface (eth1) for each node becomes active when the redundant control function starts up for logical IP takeover. Once the userApplication starts up, takeover virtual interface (eth1:1) then becomes active on the operating node which has higher priority.

Figure 5.31 Start-up behavior of NIC switching mode (logical IP takeover) illustrates start-up behavior of logical IP takeover.

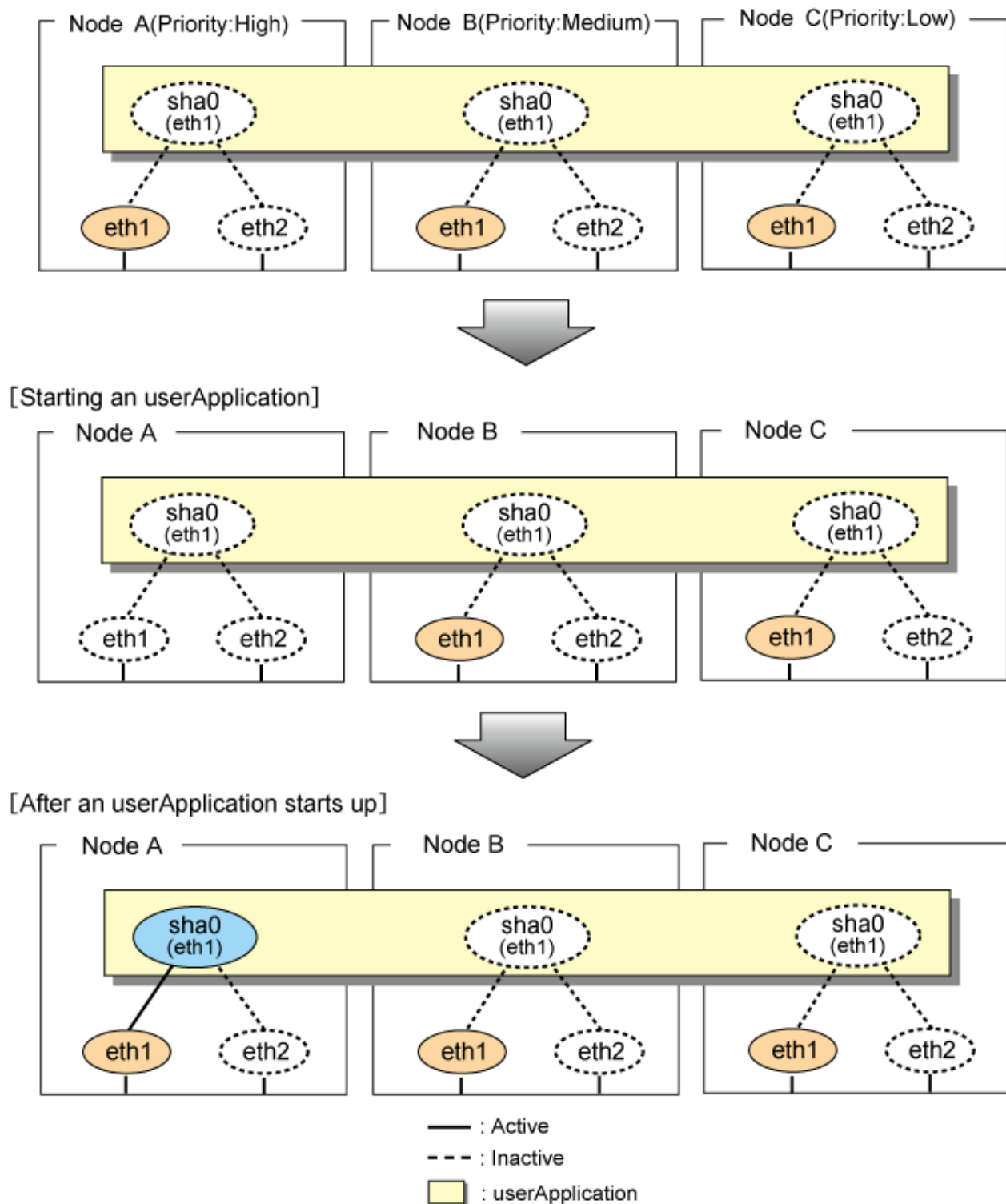
Figure 5.31 Start-up behavior of NIC switching mode (logical IP takeover)  
 [Before an userApplication starts up]



The physical interface (eth1) 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 (eth1) by allocating the takeover IP address to the physical interface (eth1) on the operating node, which has a higher priority. During this process, the physical interface (eth1) on the standby node maintains its state.

Figure 5.32 Start-up behavior of NIC switching mode (physical IP takeover I) illustrates start-up behavior of the physical IP takeover I.

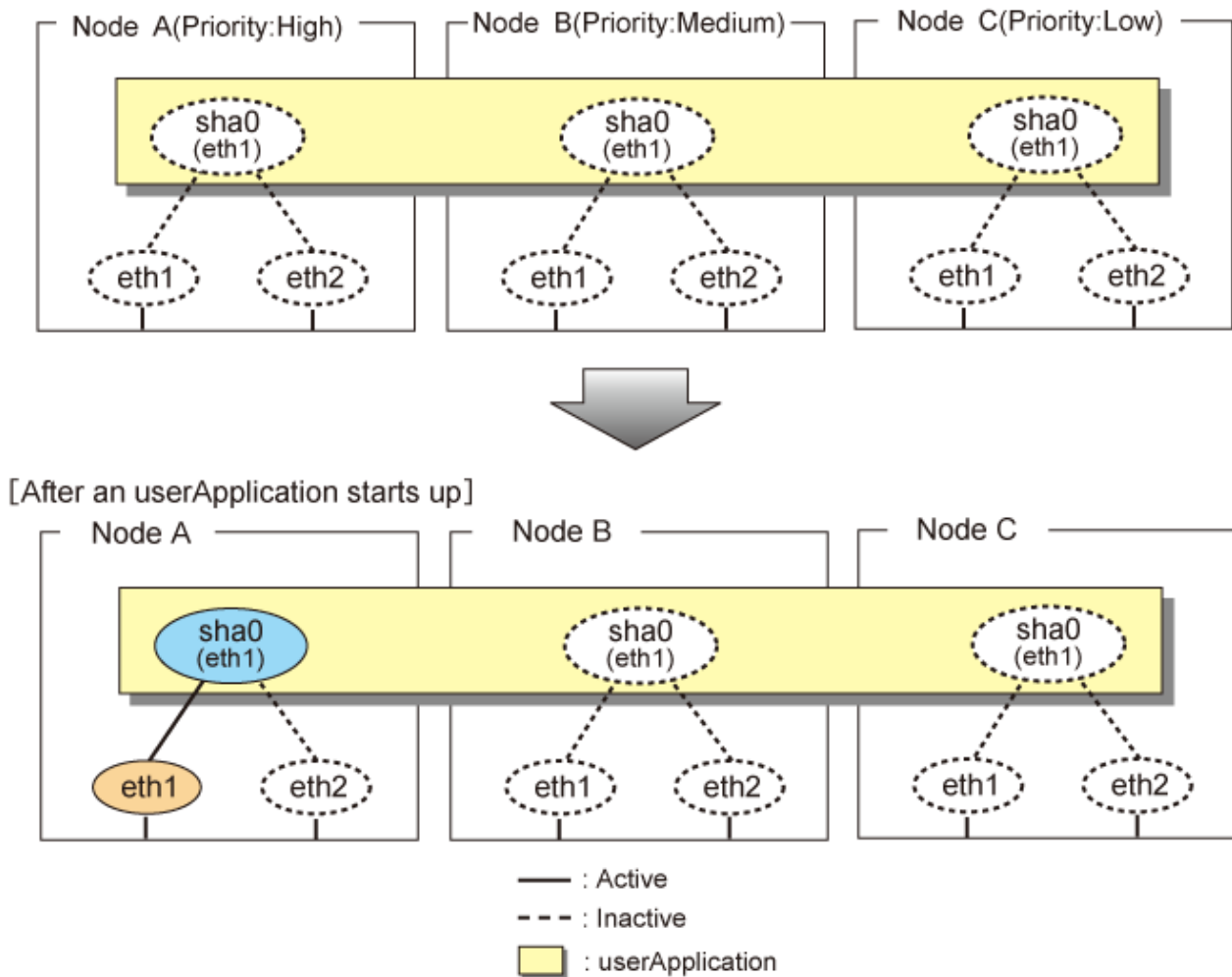
Figure 5.32 Start-up behavior of NIC switching mode (physical IP takeover I)  
[Before an userApplication starts up]



The physical interface (eth1) 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 (eth1) by allocating the takeover IP address to the physical interface (eth1) on the operating node, which has a higher priority. While this process takes place, the physical interface on the standby node remains inactive.

Figure 5.33 Start-up behavior of NIC switching mode (physical IP takeover II) illustrates start-up behavior of physical IP takeover II

Figure 5.33 Start-up behavior of NIC switching mode (physical IP takeover II)  
[Before an userApplication starts up]



#### 5.4.10.2 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.

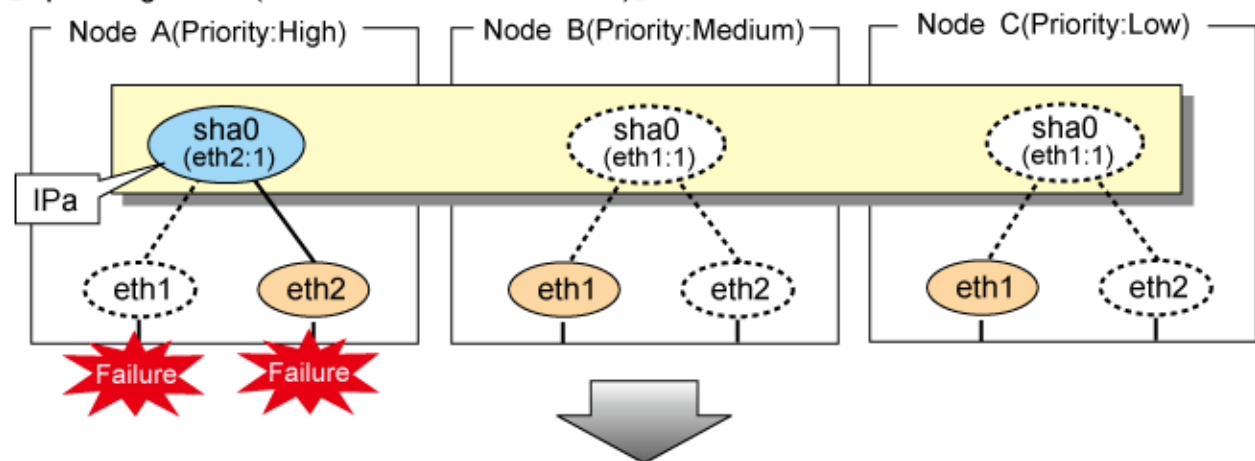
Figure 5.34 Switching operation of NIC switching mode (logical IP takeover) illustrates switching behavior of NIC switching mode (logical IP address takeover function).

In the following figure, the takeover virtual IP address (IPa) in the operating node A is allocated to the logical interface (eth2.1) for the secondary interface. Once IPa is allocated, the logical interface (eth2.1) for the secondary interface turns into activate state.

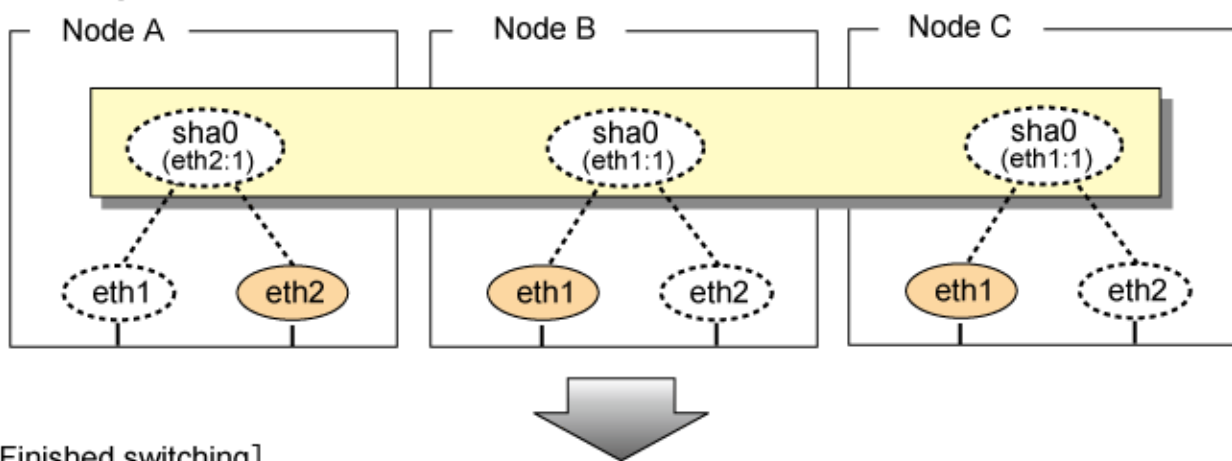
When switching the node due to failure in the transfer routes, NIC switching mode inactivates the logical virtual interface which has allocated the takeover IP address (IPa) in the operating node A. Then it allocates the takeover IP address to the primary interface (eth1) and finally activates the logical interface (eth1:1).

Figure 5.34 Switching operation of NIC switching mode (logical IP takeover)

[Operating Status(Failure occurred in node A)]



[Switching]



[Finished switching]

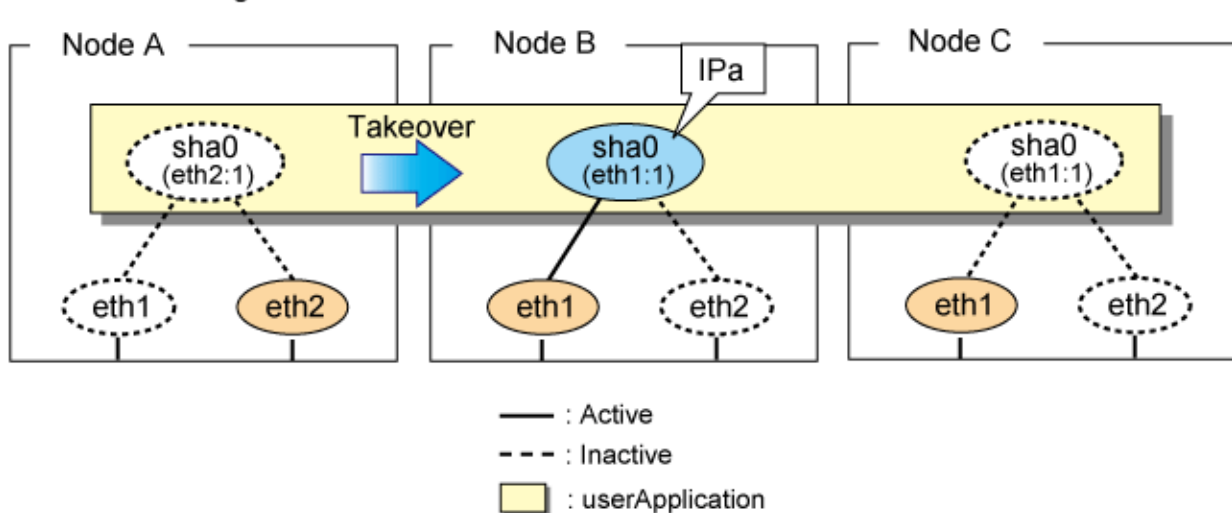


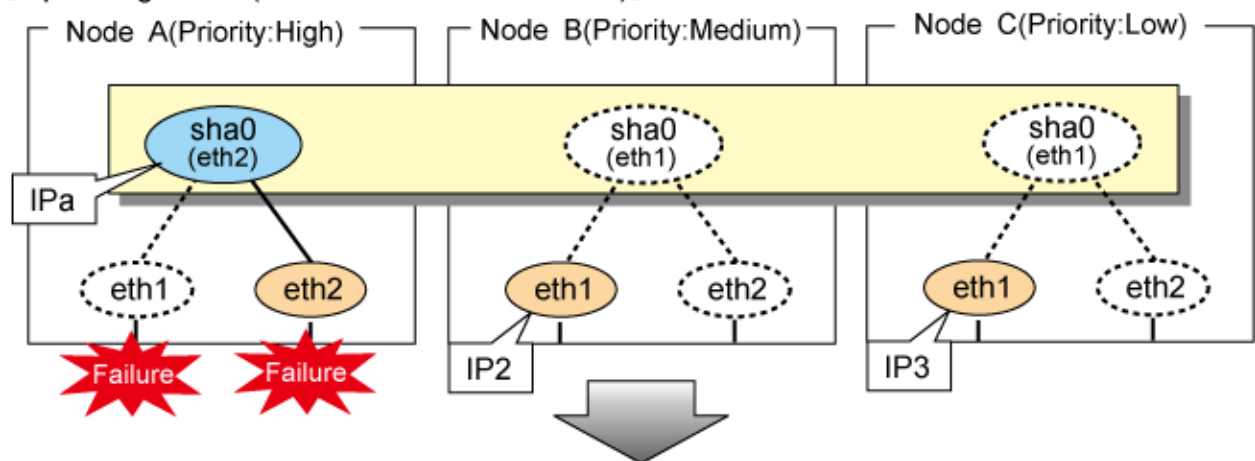
Figure 5.35 Switching operation of NIC switching mode (physical IP takeover I) (continues) and Figure 5.36 Switching operation of NIC switching mode (physical IP takeover I) (end) illustrate switching behavior of NIC switching mode (takeover physical IP address I).

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.

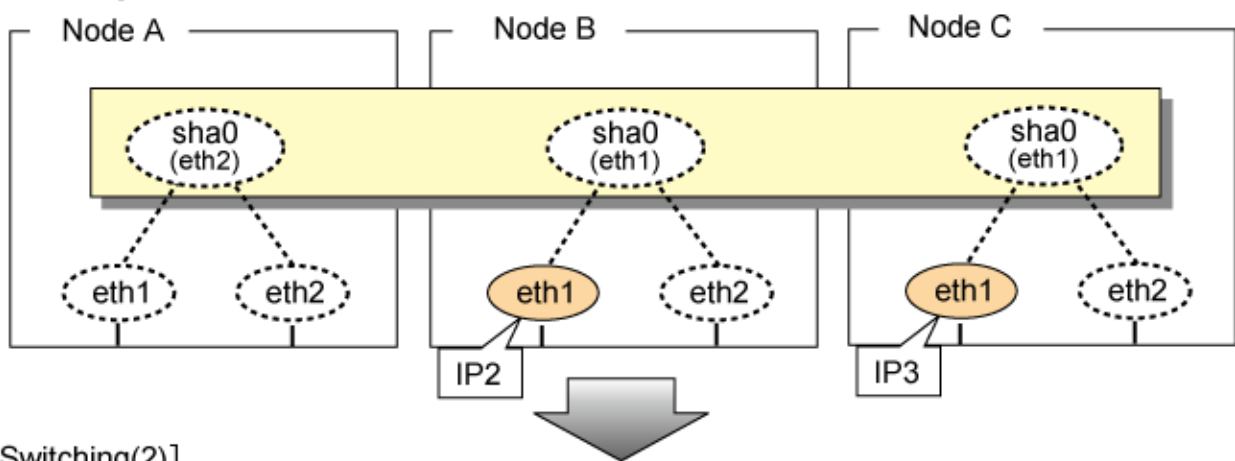
When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (eth1), which has been active in the standby node B. Then it allocates the takeover IP address (IPa) to activate the primary interface (eth1). Once the primary interface activates, different IP address is allocated to the secondary interface (eth2) by means of inactivating eth2.

Figure 5.35 Switching operation of NIC switching mode (physical IP takeover I) (continues)

[Operating Status(Failure occurred in node A)]



[Switching(1)]



[Switching(2)]

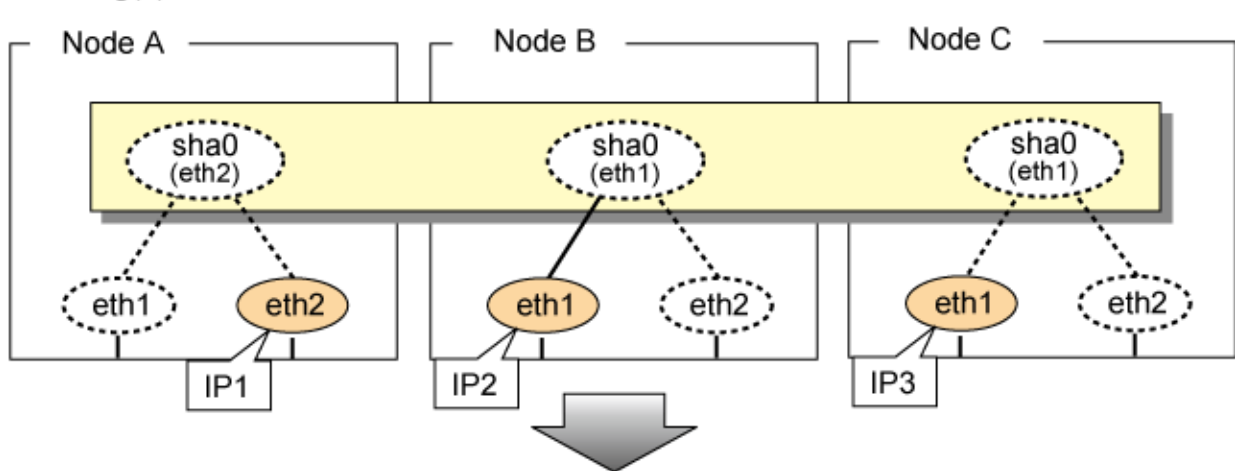


Figure 5.36 Switching operation of NIC switching mode (physical IP takeover I) (end)  
[Switching(3)]

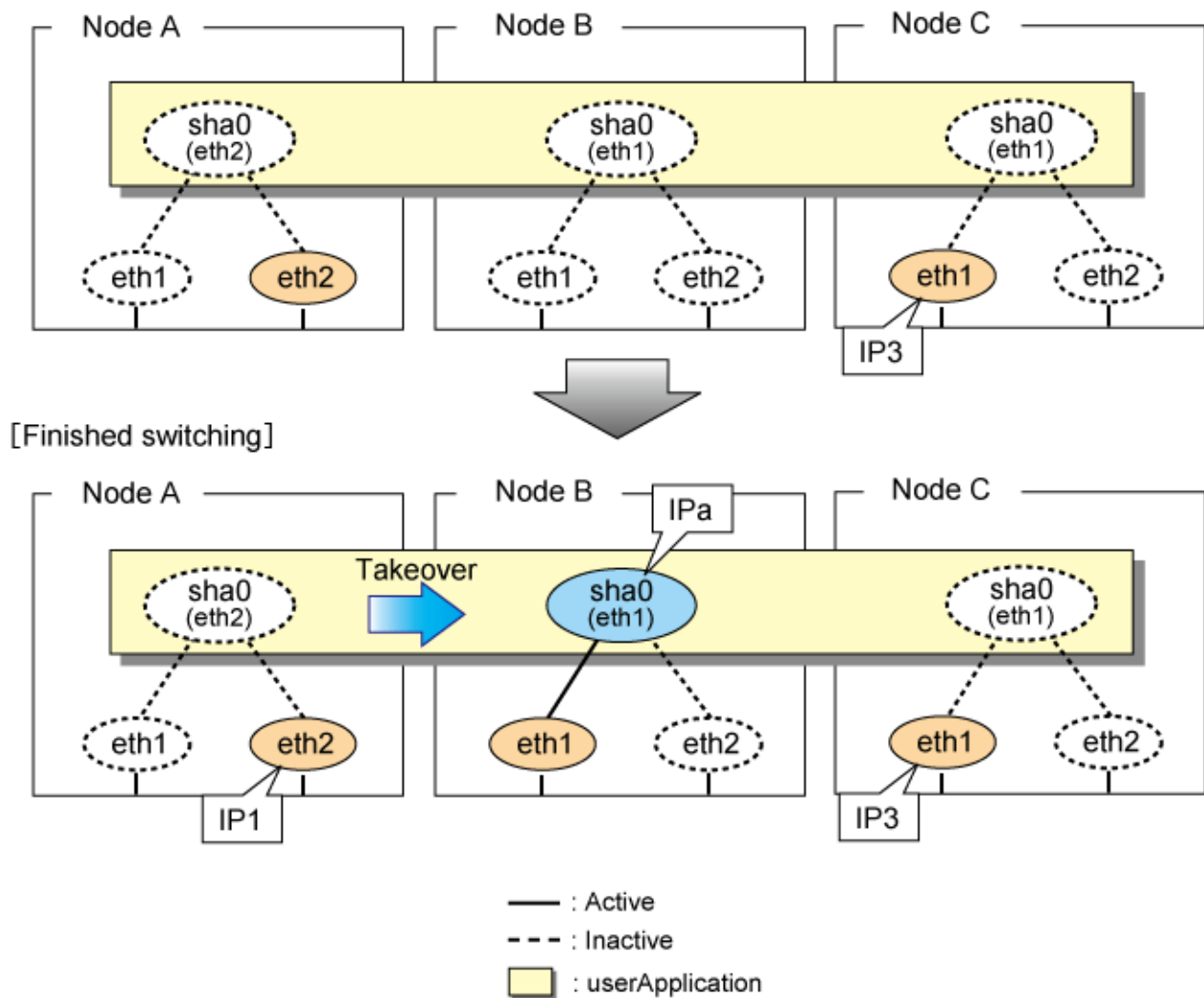


Figure 5.37 Switching operation of NIC switching mode (physical IP takeover II) illustrates switching behavior of NIC switching mode (takeover physical IP address I).

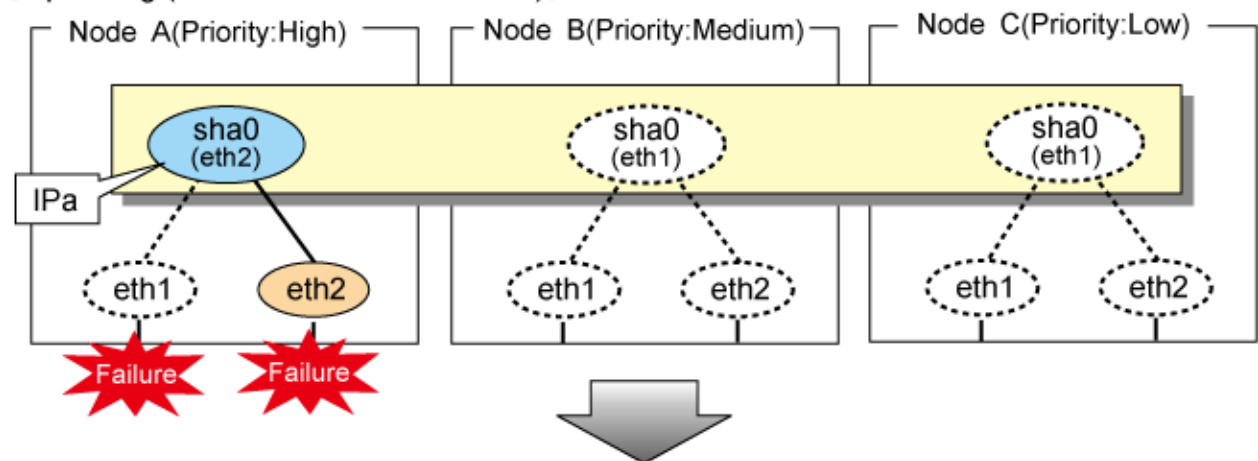
In the following figure, the takeover IP address (IPa) in the operating node A is allocated to the secondary interface. Once IPa is allocated it turns into activate state.

When switching the node because of a failure in the transfer path, activate the standby node B turns to be active by allocating the takeover IP address (IPa) to the primary interface (eth1). After the IP address is successfully passed over to the standby node B, becomes inactive the secondary interface (eth2), which previously owned the takeover IP address (IPa) in node A.

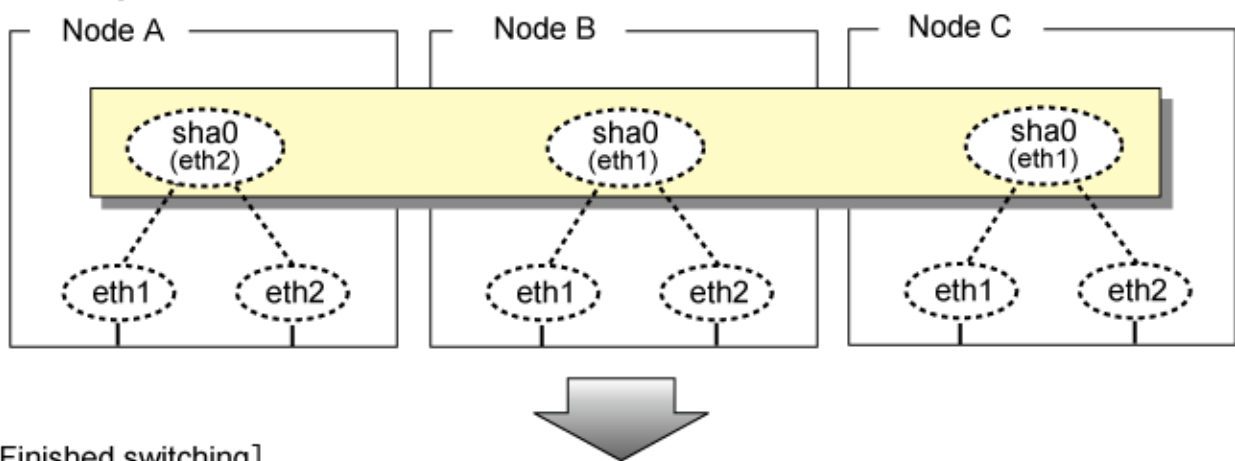


Figure 5.37 Switching operation of NIC switching mode (physical IP takeover II)

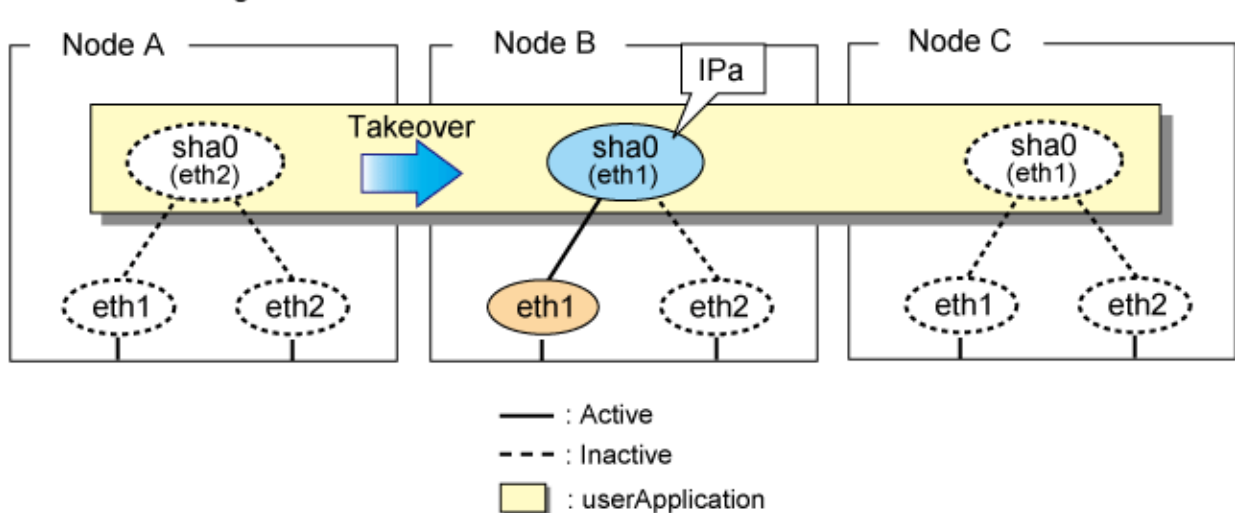
[Operating (Failure occurred in node A)]



[Switching]



[Finished switching]



### 5.4.10.3 Fail-back

The procedure for performing fail-back is the same as in Fast switching mode. For details, see "[5.4.9.3 Fail-back](#)".

### 5.4.10.4 Stopping

Figure 5.38 Stopping operation of NIC switching mode (logical IP takeover) illustrates stopping operation of a userApplication for logical IP takeover.

Figure 5.38 Stopping operation of NIC switching mode (logical IP takeover)  
 [Before an userApplication stops]

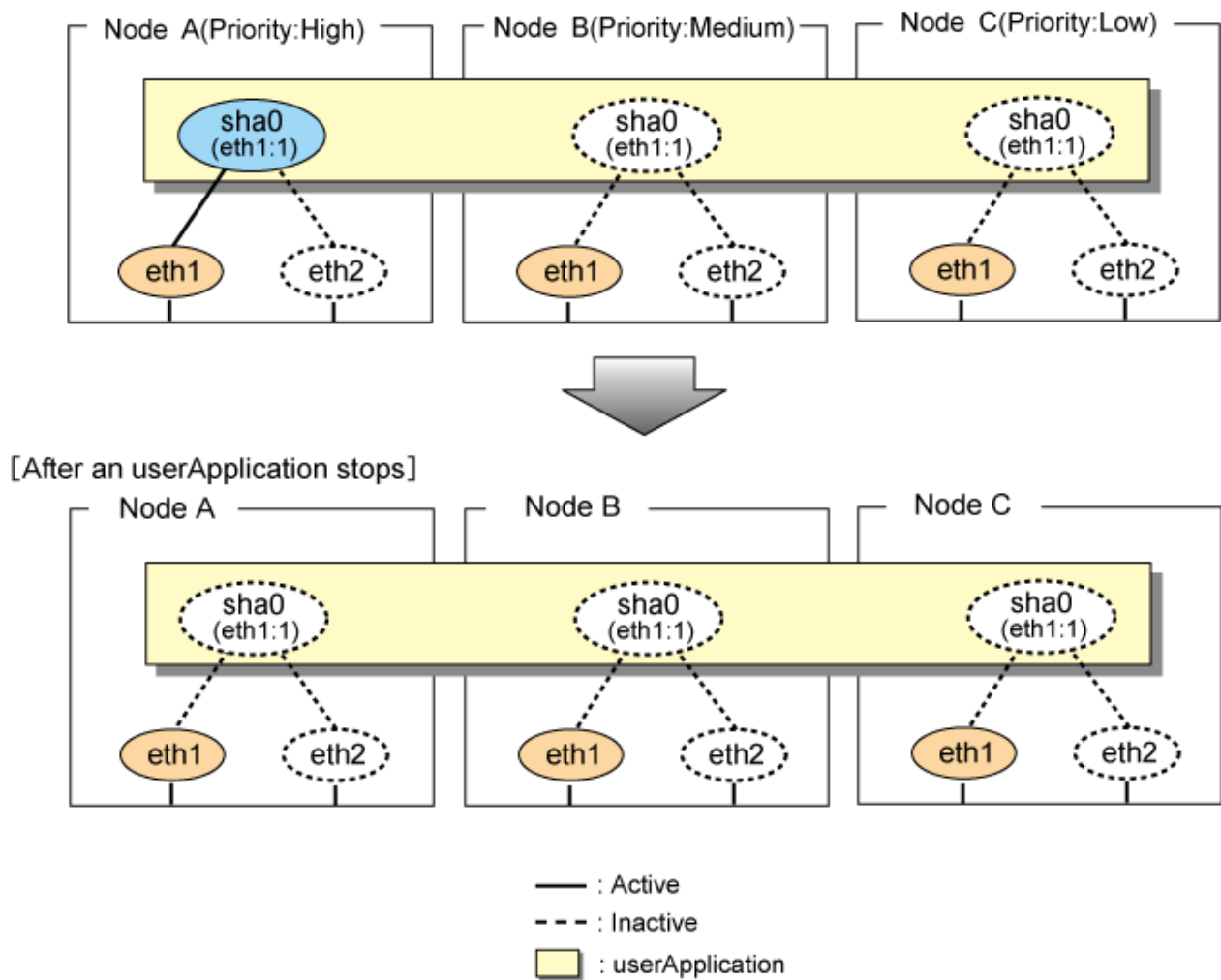


Figure 5.39 Stopping operation of NIC switching mode (physical IP takeover I) illustrates stopping operation of a userApplication for physical IP takeover I.

Figure 5.39 Stopping operation of NIC switching mode (physical IP takeover I)  
 [Before an userApplication stops]

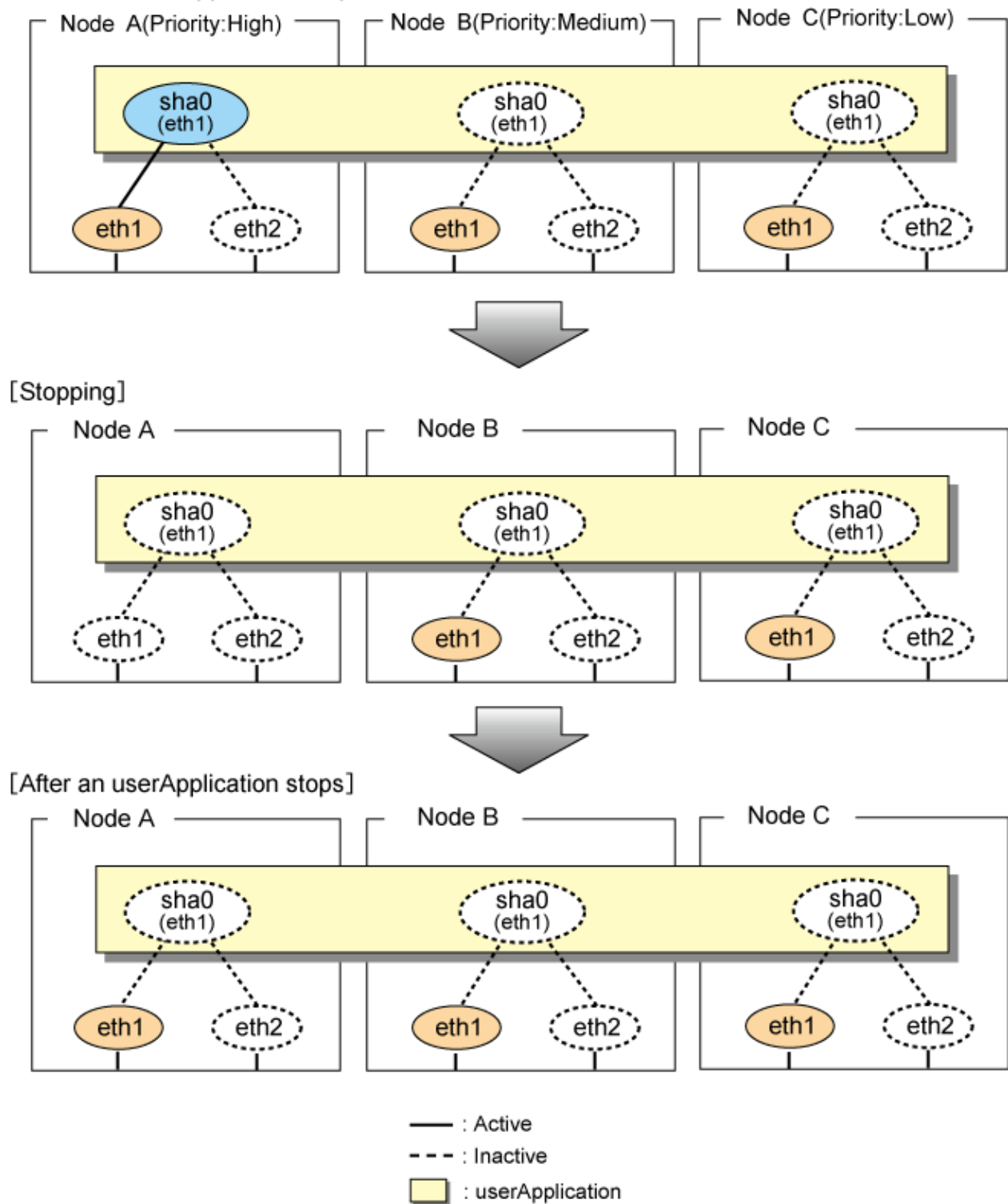
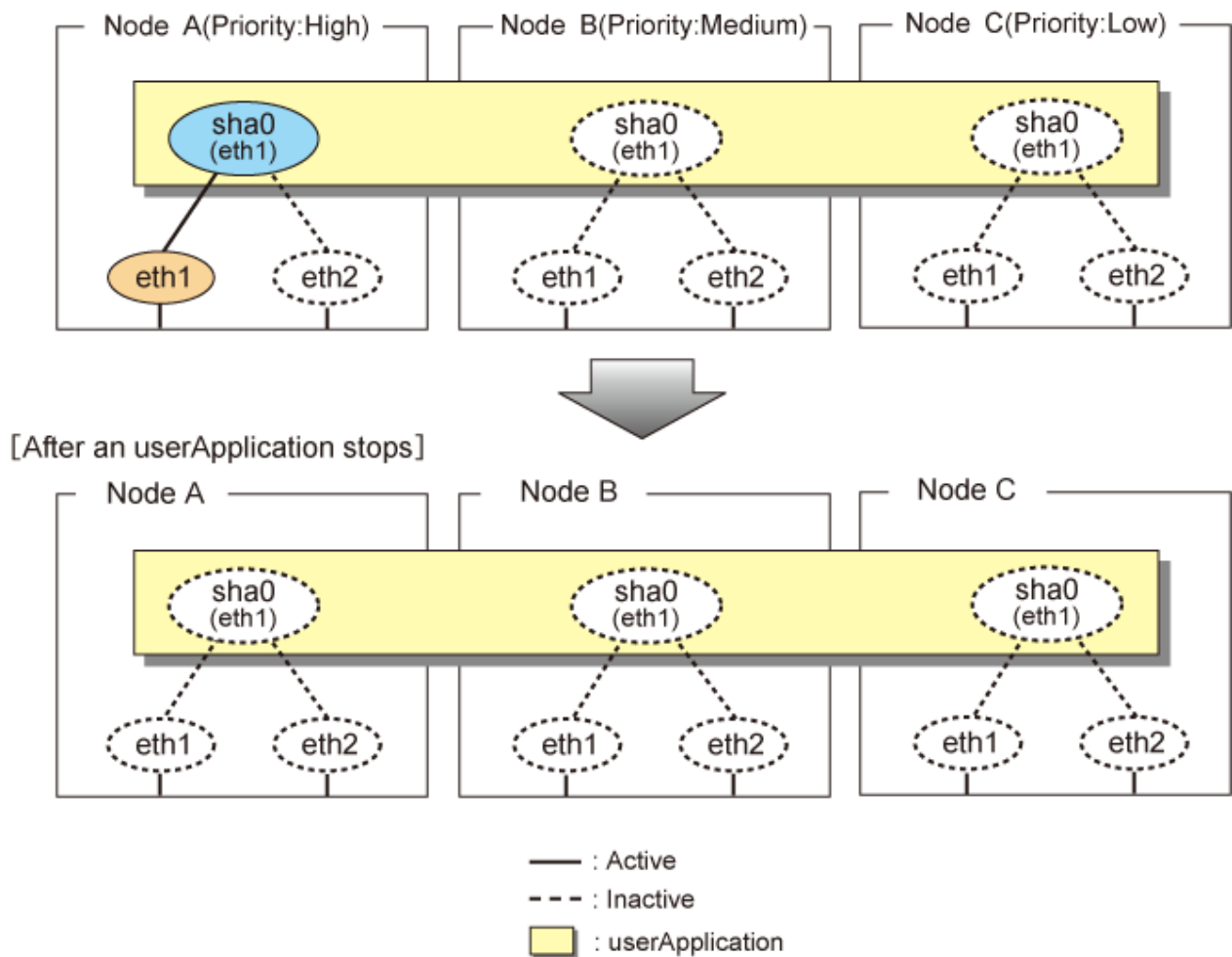


Figure 5.40 Stopping operation of NIC switching mode (physical IP takeover II) illustrates stopping operation of a userApplication for physical IP takeover II.

Figure 5.40 Stopping operation of NIC switching mode (physical IP takeover II)  
 [Before an userApplication stops]



## 5.4.11 Cascade (Virtual NIC mode)

### 5.4.11.1 Starting

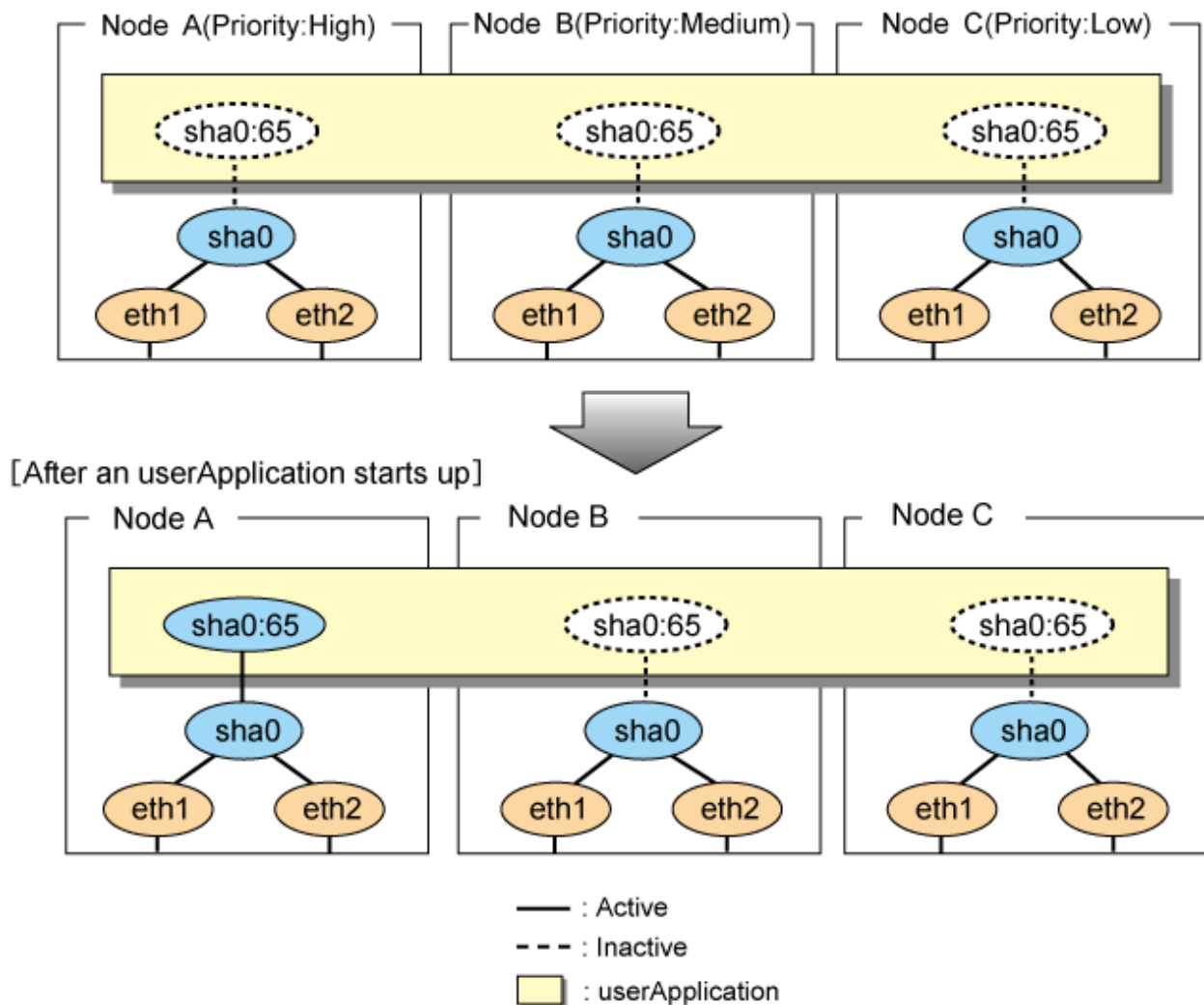
When the userApplication starts up, the takeover virtual interface (sha0:65) becomes active on the operating node, allows to hold communication using the takeover virtual IP address.

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 5.41 Startup behavior of Virtual NIC mode](#) illustrates start-up behavior of Virtual NIC mode.

Figure 5.41 Startup behavior of Virtual NIC mode  
[Before an userApplication starts up]



### 5.4.11.2 Switching

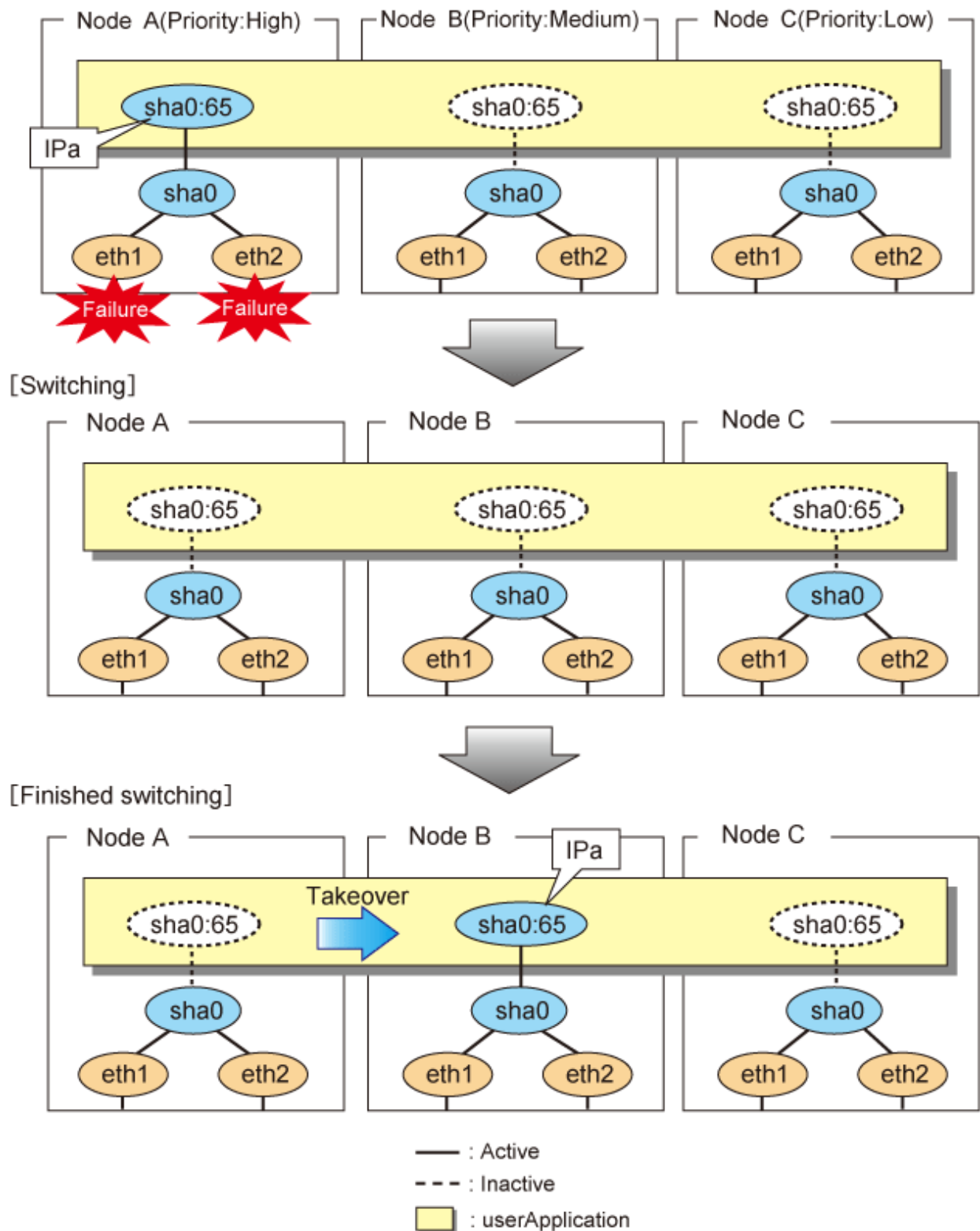
During normal operation, userApplication communicates with the remote system using the takeover virtual interface on the operating node.

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.

Figure 5.42 Switching behavior of Virtual NIC mode illustrates switching behavior of Virtual NIC mode.

In the following figure, the takeover 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 takeover IP address (IPa) becomes active. Note that the virtual interface (sha0) in node A stays unchanged.

Figure 5.42 Switching behavior of Virtual NIC mode  
 [Operating Status (Failure occurred in node A)]



### 5.4.11.3 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

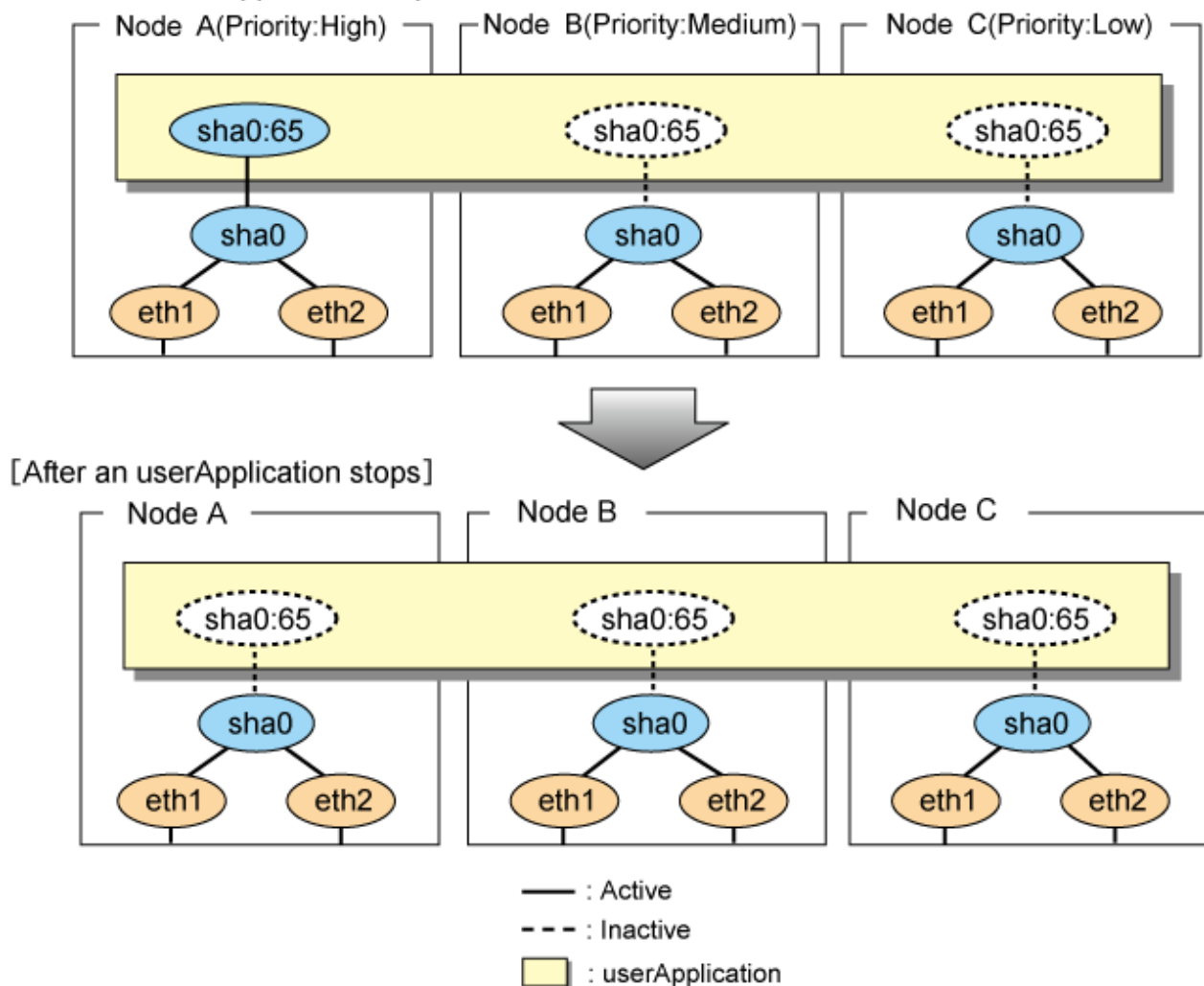
Fail-back the userApplication to an arbitrary node on standby using "Cluster Admin" of Web-Based Admin View.

### 5.4.11.4 Stopping

Figure 5.43 Stopping behavior of Virtual NIC mode illustrates stopping operation of a userApplication

Figure 5.43 Stopping behavior of Virtual NIC mode

[Before an userApplication stops]



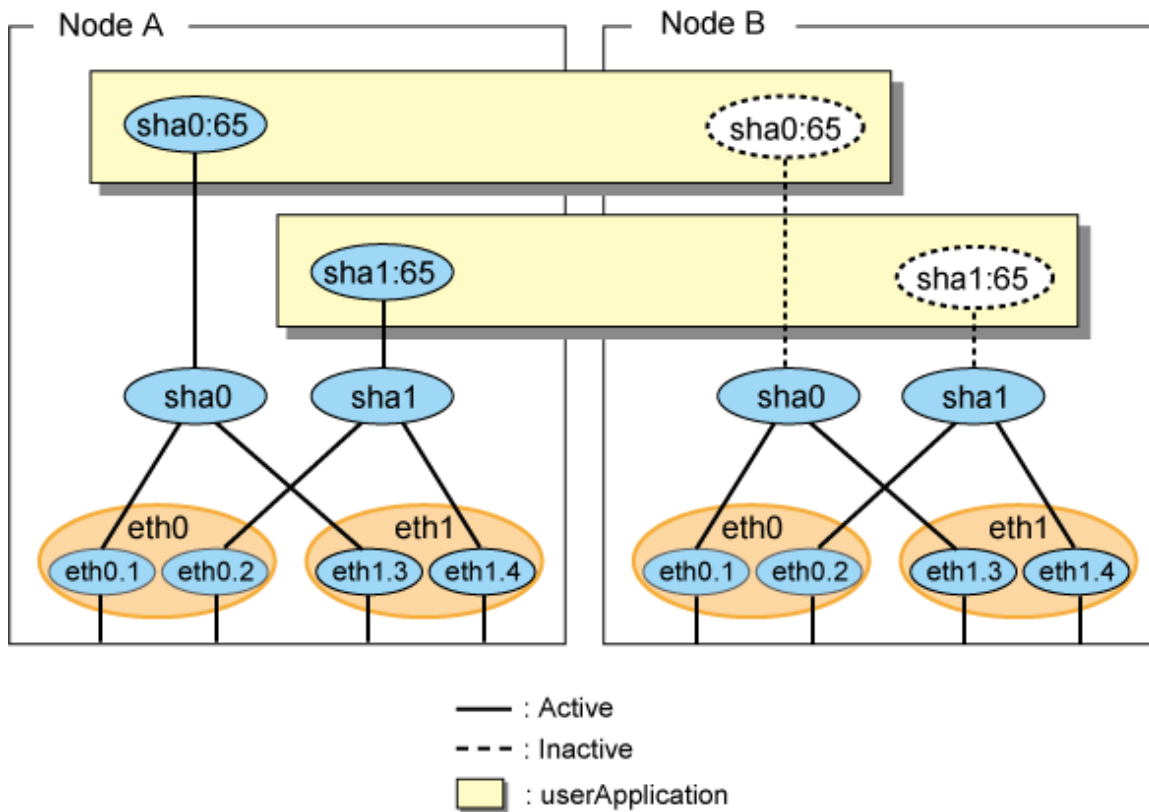
## 5.5 Tagged VLAN interface multiplexing on cluster system

This section explains the transfer route multiplexing using tagged VLAN interface that operates on a cluster system.

### 5.5.1 Active standby (Fast switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Active standby).

Figure 5.44 Tagged VLAN interface multiplexing on Fast switching mode (Active standby)

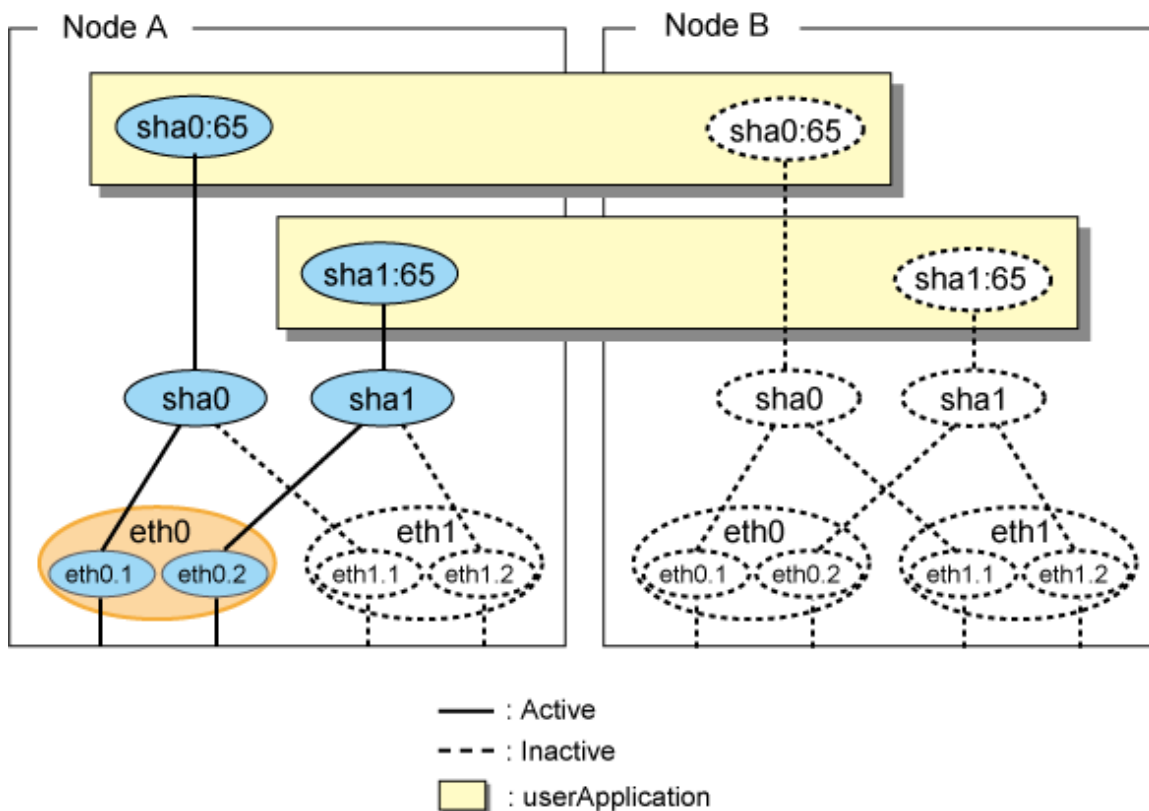


### 5.5.2 Active standby (NIC switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Active standby).



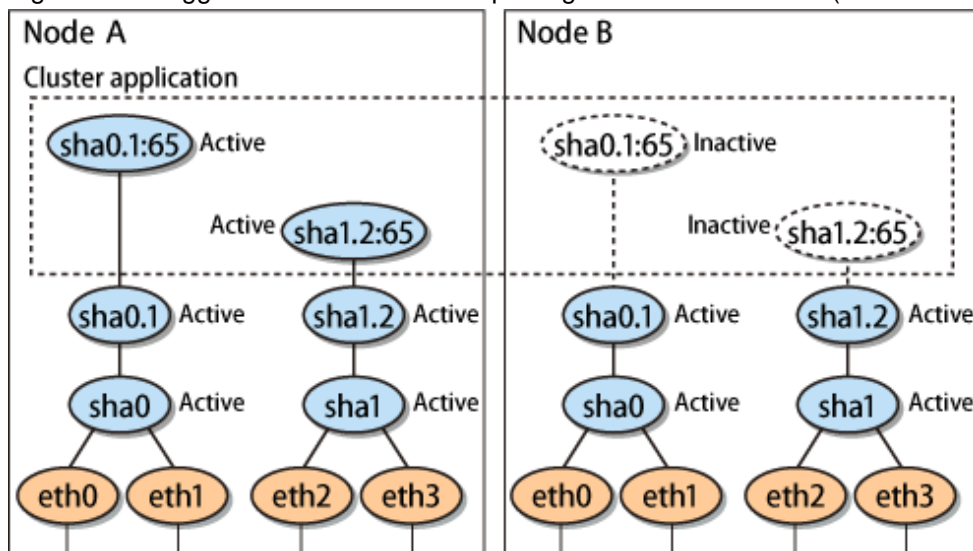
Figure 5.45 Tagged VLAN interface multiplexing on NIC switching mode (Active standby)



### 5.5.3 Active Standby (Virtual NIC mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Active standby).

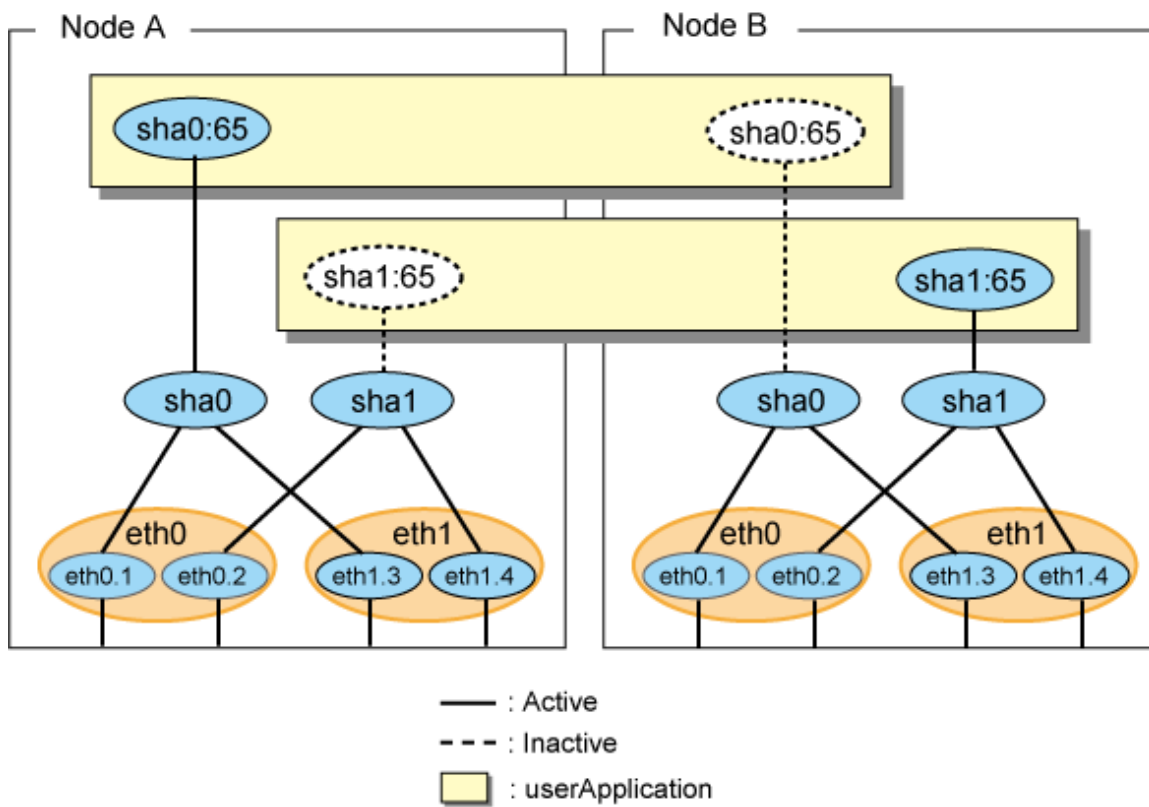
Figure 5.46 Tagged VLAN interface multiplexing on Virtual NIC mode (Active standby)



### 5.5.4 Mutual Standby (Fast switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

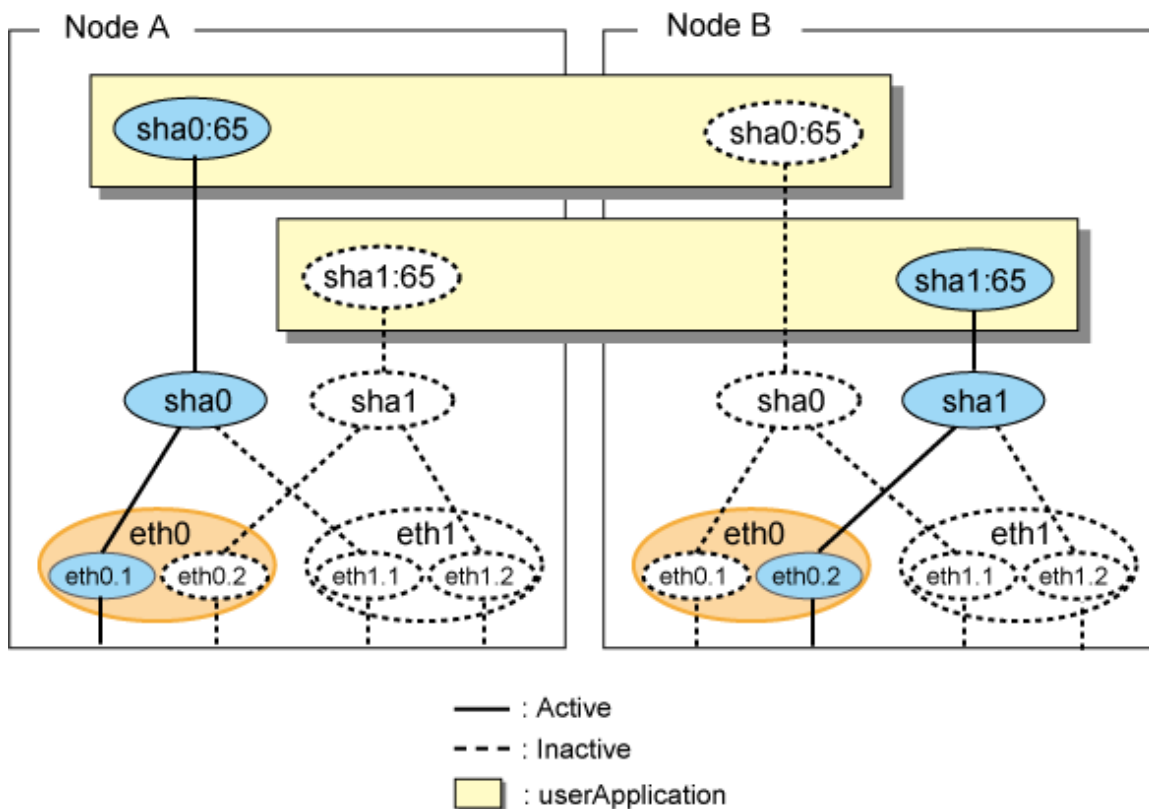
Figure 5.47 Tagged VLAN interface multiplexing on Fast switching mode (Mutual Standby)



### 5.5.5 Mutual Standby (NIC switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

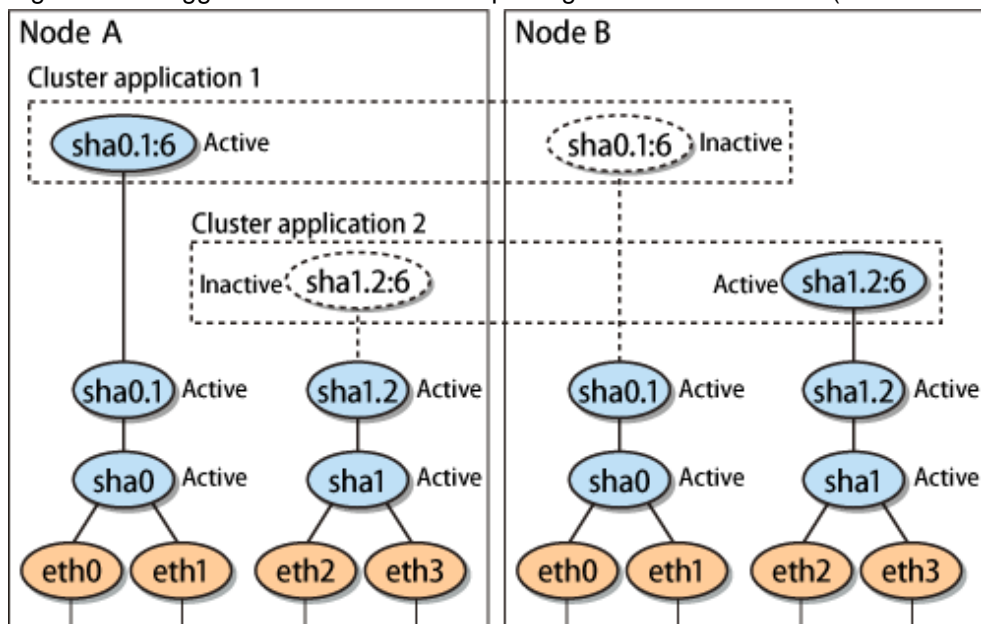
Figure 5.48 Tagged VLAN interface multiplexing on NIC switching mode (Mutual Standby)



### 5.5.6 Mutual Standby (Virtual NIC mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

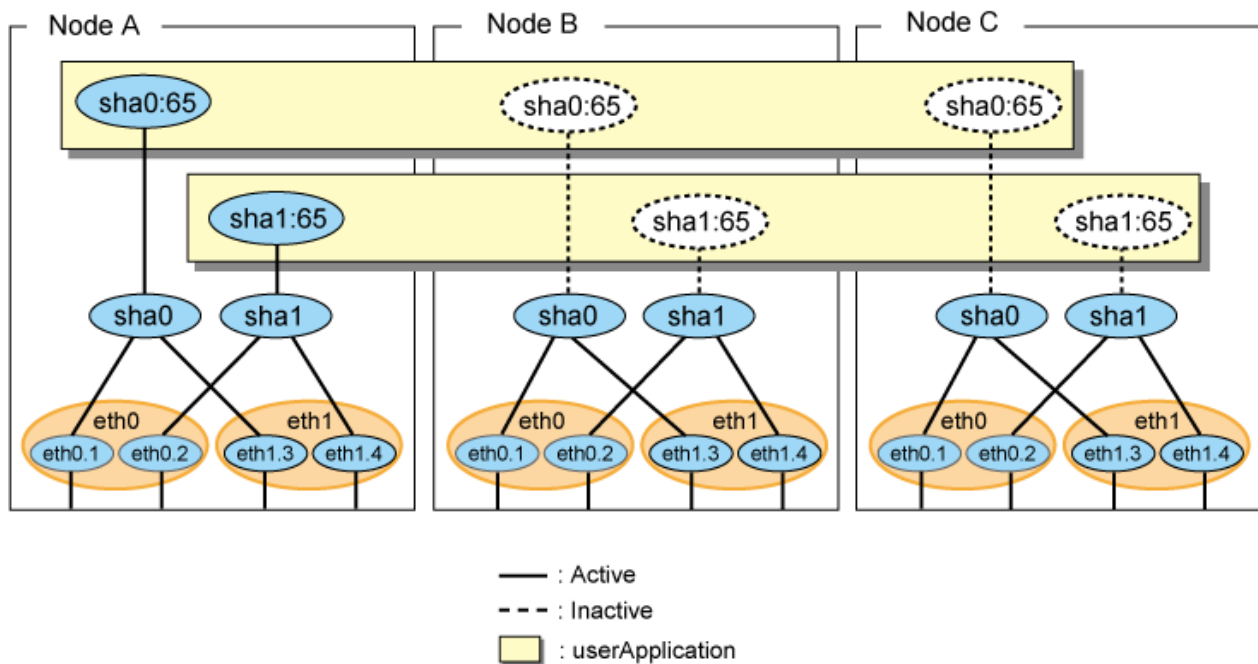
Figure 5.49 Tagged VLAN interface multiplexing on Virtual NIC mode (Mutual Standby)



### 5.5.7 Cascade (Fast switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

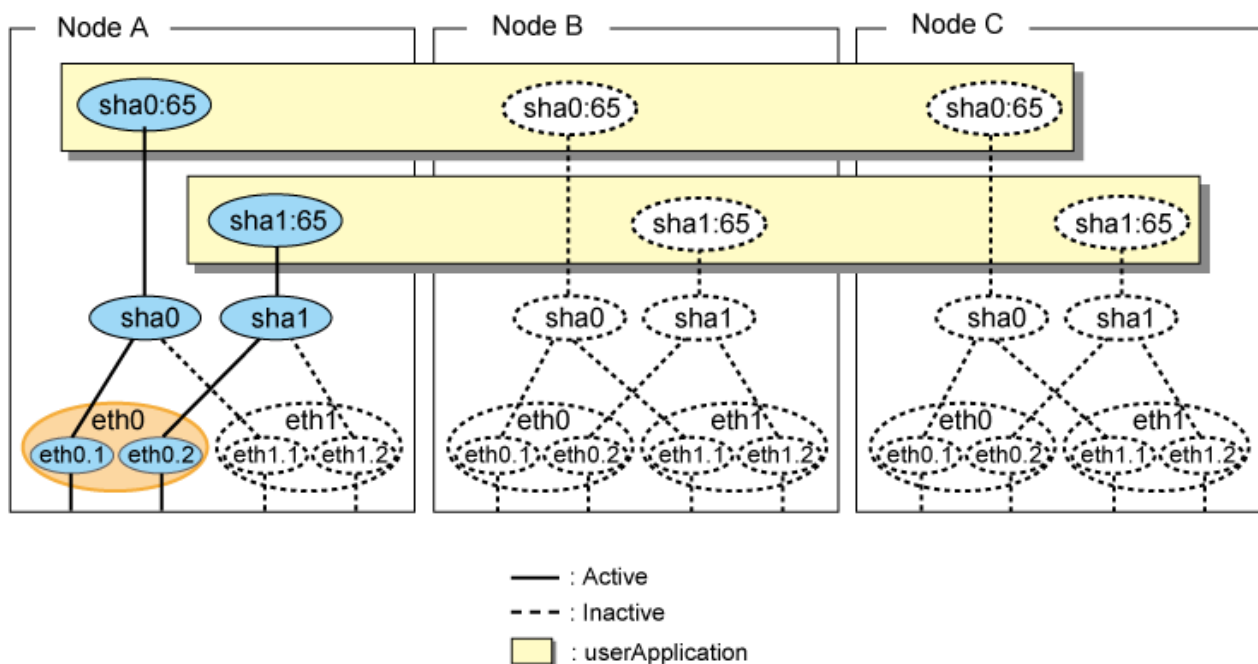
Figure 5.50 Tagged VLAN interface multiplexing on Fast switching mode (Cascade)



## 5.5.8 Cascade (NIC switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

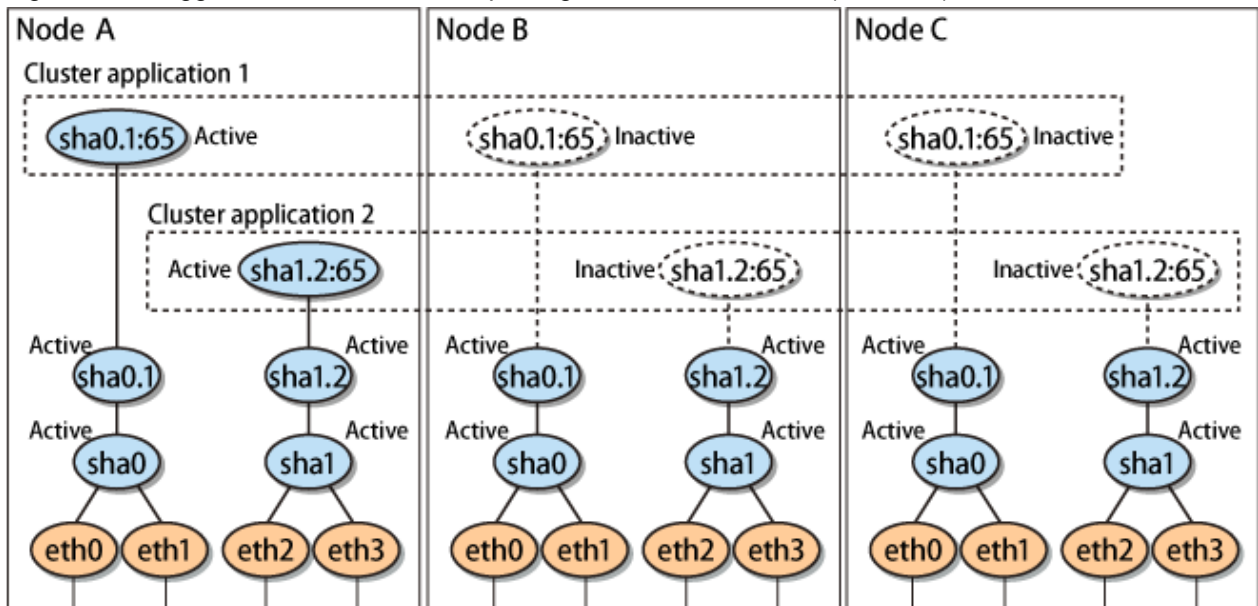
Figure 5.51 Tagged VLAN interface multiplexing on NIC switching mode (Cascade)



## 5.5.9 Cascade (Virtual NIC mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

Figure 5.52 Tagged VLAN interface multiplexing on Virtual NIC mode (Cascade)



## Chapter 6 Maintenance

This chapter focuses on a general approach to troubleshooting.

### 6.1 Redundant Line Control Function Troubleshooting Data to be Collected

In the event of a problem in Redundant Line Control Function operation, Redundant Line Control Function troubleshooting requires information about the problem to be collected.

When collecting examination materials of a Redundant Line Control Function all together, see "[6.1.1 Command to collect materials](#)".

In addition to the data collected by the material collection command, the following materials are necessary for troubleshooting a communication failure.

- Network configuration diagram (information for IP and MAC addresses)
- Examination materials for network devices (information for the ARP table, MAC learning table, STP, and routing table), which should be collected when a failure occurs.
- A packet trace (information collected by the tcpdump or tethereal command) for the NIC that the Redundant Line Control function uses, which should be collected when a failure occurs.

In addition, confirm that CLS and network devices are set correctly, referencing "[Appendix F Trouble shooting](#)".

#### 6.1.1 Command to collect materials

##### [Form]

```
/opt/FJSVhanet/usr/sbin/hanet_snap [-s] [save-directory]
```

##### [Detail of the function]

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:

Table 6.1 Collected information

Type	File name when collected	Collected information	Minimum examination materials
System information: OSInfo/	arp_n	arp -n	Y
	arptables_list	arptables --list	Y
	BASP/	/etc/basp baspcfg show	Y
	chkconfig	chkconfig --list	Y
	ctld_pinfo	/proc/XXX/cmdline /proc/XXX/maps /proc/XXX/fd /proc/XXX/stat /proc/XXX/statm /proc/XXX/status	N
	dmidecode_sysinfo	dmidecode -s system-manufacturer dmidecode -s system-product-name dmidecode -s system-version	Y
	etc/	/etc/fcoe /etc/gateways /etc/hosts /etc/iftab /etc/iscsi /etc/libvirt /etc/mactab /etc/modprobe.conf /etc/NetworkManager /etc/nsswitch.conf /etc/quagga/ /etc/radvd.conf /etc/rc.d/init.d /etc/rc.d/rc.local /etc/resolv.conf /etc/rsyslog.conf /etc/services /etc/sysconfig/arptables /etc/sysconfig/hwconf /etc/sysctl.conf /etc/syslog.conf /etc/udev /etc/xen /etc/udev/rules.d	Y
	etc/brctl	brctl show brctl showmacs brctl showstp	Y
	etc/class_net	ls -l /sys/class/net	Y
	etc/class_net_dev	/sys/class/net/*/carrier /sys/class/net/*/features /sys/class/net/*/flags /sys/class/net/*/iflink /sys/class/net/*/type	Y
	etc/rc_list	ls /etc/rc.d/*	Y

Type	File name when collected	Collected information	Minimum examination materials
	etc/selinux	/etc/selinux/config /usr/sbin/sestatus -v /usr/sbin/semodule -lv	Y
		/etc/selinux/targeted/contexts/files/ file_contexts /var/log/audit/audit.log /sbin/ausearch -m AVC	N
	etc/ virsh_dumpxml_<domain>	virsh dumpxml <domain> (domain information) * <domain>: domain ID	Y
	etc/virsh_list_all	virsh list --all	Y
	etc/virsh_nodeinfo	virsh nodeinfo	Y
	etc/virsh_version	virsh version	Y
	etc/xen_store_ls	xenstore-ls	Y
	etc/xm_dmesg.log	xm dmesg	N
	etc/xm_info	xm info	Y
	etc/xm_list_long	xm list --long	Y
	ethdev_info	ethtool ethX	Y
	free	free -bt	Y
	fstab	/etc/fstab	Y
	iANS/	/etc/ians ianscfg -s	Y
	ifconfig_a	ifconfig -a	Y
	include/	/lib/modules/^uname -r`/build/include/ linux/ kernel.h version.h module.h rhconfig.h autoconf.h /boot/kernel.h /etc/redhat-release	Y
	ipcs_a	ipcs -a ipcs -t ipcs -p ipcs -c ipcs -l ipcs -u	Y
	ip_info	ip link ip addr ip route ip rule ip neigh ip tunnel ip maddr ip mroute	Y



Type	File name when collected	Collected information	Minimum examination materials
	ip6tables-config	/etc/sysconfig/ip6tables-config	Y
	iptables-config	/etc/sysconfig/iptables-config	Y
	iptables_list	iptables --list	Y
	log/	/var/log/boot.log* /var/log/dmesg.log* /var/log/libvirt/* /var/log/messages* /var/log/xen/xend.log*	N
	lsmod	lsmod	Y
	lspci	lspci	Y
	netstat	netstat -na netstat -ni netstat -np netstat -nr netstat -na -A inet6 netstat -nr -A inet6 netstat -ng netstat -ns	Y
	proc_dev	/proc/devices	Y
	proc_net/	/proc/net/	N
	ps_ewfl	ps -ewfl	Y
	sel_pinfo	/proc/XXX/cmdline /proc/XXX/maps /proc/XXX/fd /proc/XXX/stat /proc/XXX/statm /proc/XXX/status	N
	sysconfig/	/etc/sysconfig/hwconf /etc/sysconfig/network /etc/sysconfig/netdump /etc/sysconfig/ntpd /etc/sysconfig/static-routes /etc/sysconfig/network-scripts/	Y
	sysctl_a	sysctl -a	N
	sys_info	/proc/cgroups /proc/cpuinfo /proc/interrupts /proc/meminfo /proc/iomem /proc/ioports /proc/slabinfo	Y
	uamlog	/var/opt/FJSVfupde/log/*	N
	uname_a	uname -a	Y
	uptime	uptime	Y
GLS information: hanetInfo/	config/	/etc/opt/FJSVhanet/config/	Y
	dev_sha	ls -l /dev/sha	Y

Type	File name when collected	Collected information	Minimum examination materials
	dsp_conf	dsphanet dsphanet -o dsphanet -v dsppathmon dspobserv dspobserv -ddd dsppoll	Y
	filelist_tmp	ls -la /var/opt/FJSVhanet/tmp/	Y
	log/	/var/opt/FJSVhanet/log/	Y
	modinfo	modinfo sha	Y
	print_conf	hanetconfig print hanetpathmon target hanetpathmon param hanetpoll print hanetpoll devparam hanetmask print hanetparam print hanetgw print hanetobserv print hanethvrsc print	Y
	rpminfo	rpm -qi FJSVhanet rpm -qi kmod-FJSVhanet-driv rpm -qi kmod-FJSVhanet-driv-xen rpm -qi kmod-FJSVhanet-driv-PAE	Y
	script/	/etc/opt/FJSVhanet/script/	Y
Cluster system information: RCInfo/	hvdsp_a	hvdsp -a	N
	log/	/var/opt/reliant/log/	N

[Meaning of the symbols] Y: It extracts. N: It does not extract.

### [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.gz.

Ex.) hostname040126093843.tar.gz

### [Using example]

- 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 /home/user1.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap -s /home/user1
```

## 6.1.2 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 / Virtual NIC]					
Name	Hostname	Mode	Physical	ipaddr	Interface List
sha0	192.168.1.110	t			eth0,eth1
sha1	192.168.10.110	d	192.160.10.10		eth2,eth3
sha12	-	p	-		sha1
sha2	192.168.100.110	c			eth4,eth5

2. Execute the `tethereal` command or `tcpdump` command to collect packet traces.

If a virtual interface bundles several physical interfaces, execute `tethereal(1)` command or `tcpdump(1)` command for all physical interfaces in the bundle.

Execution examples are shown below:

- sha0

```
# tethereal -i eth0 -w /tmp/packet_trace.eth0
# tethereal -i eth1 -w /tmp/packet_trace.eth1
```

- sha1 and sha12

```
# tethereal -i eth2 -w /tmp/packet_trace.eth2
# tethereal -I eth3 -w /tmp/packet_trace.eth3
```

- sha2

```
# tethereal -i eth4 -w /tmp/packet_trace.eth4
# tethereal -i eth5 -w /tmp/packet_trace.eth5
```



See

For `tethereal(1)` command or `tcpdump(1)` command, refer to the Linux manual.



Note

If you execute the `tethereal(1)` command or `tcpdump(1)` command for a virtual interface, you can only collect some packets. Execute the command for a physical interface to collect packet traces.

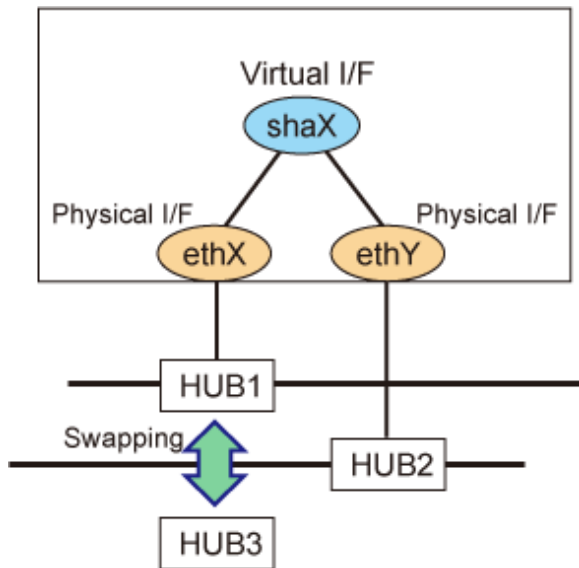
## 6.2 HUB maintenance

This section describes the procedure for swapping HUBs of the monitoring destination of GLS in the following three patterns.

- When HUBs are swapped in Fast switching mode/GS linkage mode
- When the monitoring destination IP address is changed by swapping HUBs in NIC switching mode
- When the monitoring destination IP address is not changed by swapping HUBs in NIC switching mode

### 6.2.1 Swapping HUB procedure (Fast switching mode / GS linkage mode)

The following describes the procedure for swapping HUBs in Fast switching mode and GS linkage mode.



1. Disconnect the route of the HUB to be swapped.

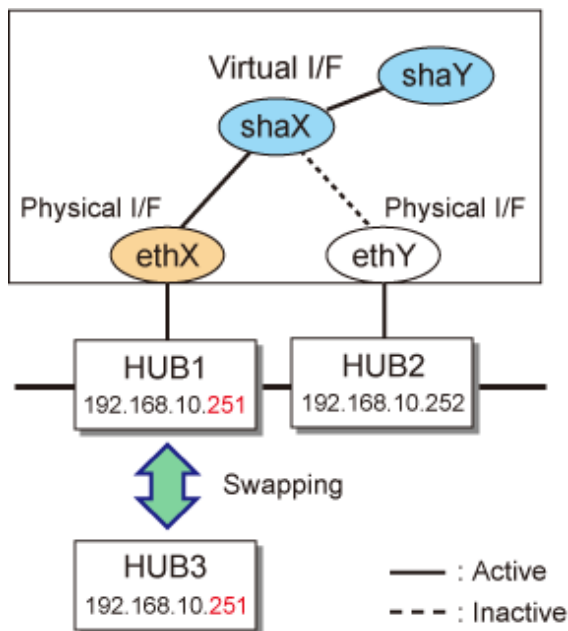
```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2. Swap the HUB
3. Check that HUB3 has been set correctly.
4. Reconnect the route of the HUB that was swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

## 6.2.2 Swapping HUB procedure (NIC switching mode / IP address remains unchanged)

The following shows the procedure in which the IP address remains unchanged even after swapping HUBs.



1. To maintain communications, switch the NIC so that the HUB to be swapped is on standby.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

2. Stop the standby patrol.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

3. Stop HUB monitoring or HUB-to-HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

4. Swap the HUB.

5. To make sure that HUB 3 has been set correctly, check whether you can ping HUB3 successfully. If there is no response, check the connections of the HUB itself and other devices.

```
# ping 192.168.10.251
```

6. Switch back to the NIC you want to use, if necessary.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

7. Start HUB monitoring or HUB-to-HUB monitoring.

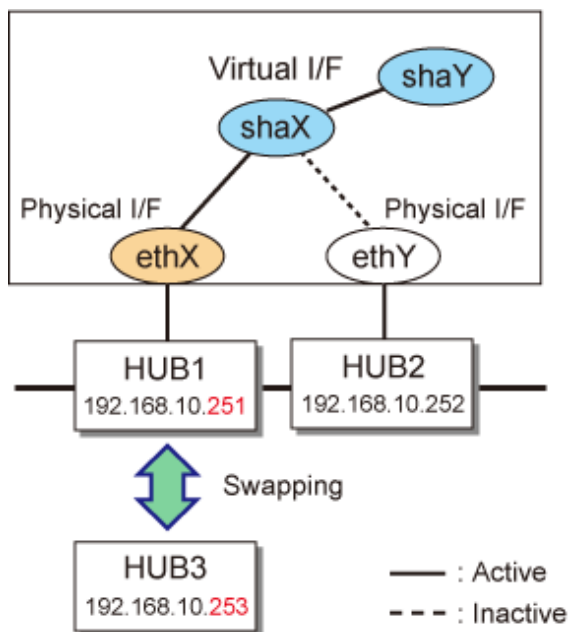
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8. Start standby patrol monitoring.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

## 6.2.3 Swapping HUB procedure (NIC switching mode / IP address is changed)

The following shows the procedure in which the IP address is changed after swapping HUBs.



1. Stop the GLS cluster application.

2. To maintain communications, switch the NIC so that the HUB to be swapped is on standby.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

3. Stop standby patrol monitoring.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

4. Stop HUB monitoring or HUB to HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

5. Swap the HUB. See the manual that comes with the HUB for how to set an IP address for a HUB.

6. Issue the ping command for HUB3 to check whether it has been set correctly. If there is no response, check the connections of the HUB and other devices.

```
# ping 192.168.10.253
```

7. Use the "hanetpoll modify" command to change the HUB monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n shaX -p  
192.168.10.253,192.168.10.252
```

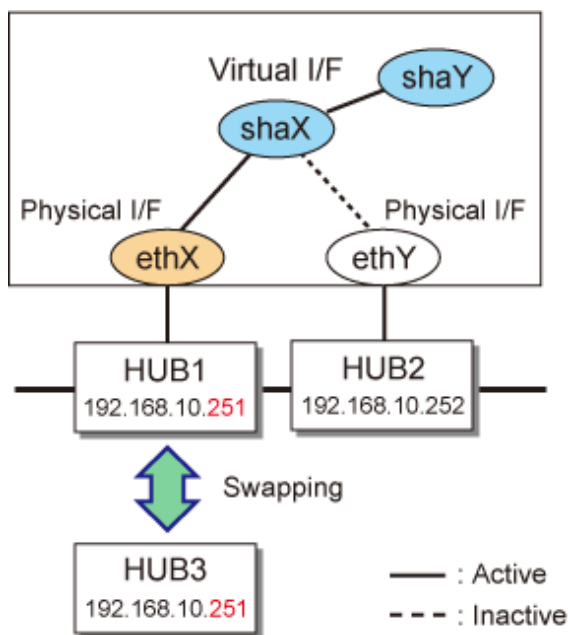
8. To enable the change of the monitoring destination, you need to reboot the GLS daemon. Reboot the system.

```
# shutdown -r now  
or  
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

9. Start the cluster application as needed. If you rebooted the system in (8), this procedure is not required.

## 6.2.4 Swapping HUB procedure (Virtual NIC mode / IP address remains unchanged)

The following shows the procedure in which the IP address remains unchanged even after swapping HUBs.



1. Stop network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon off -n shaX
```

2. To maintain communications, switch the NIC so that the HUB to be swapped is on standby.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethY
```

3. Swap the HUB.

4. To make sure that HUB 3 has been set correctly, check whether you can ping HUB3 successfully. If there is no response, check the connections of the HUB itself and other devices.

```
# ping 192.168.10.251
```

5. Switch back to the NIC you want to use, if necessary.

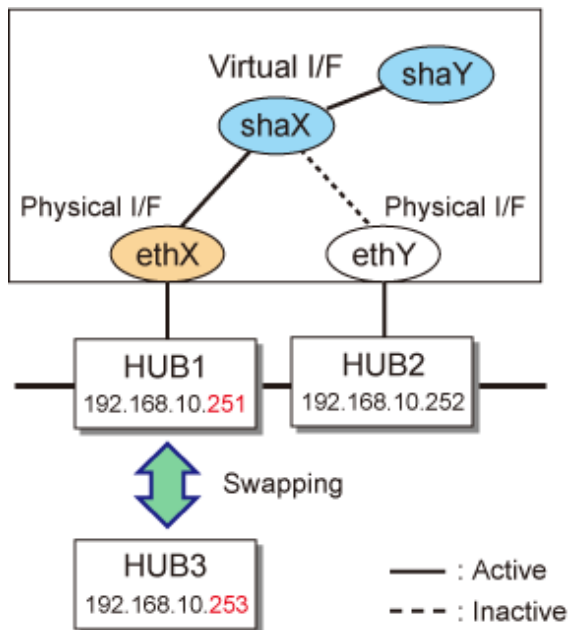
```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

6. Start network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon on -n shaX
```

## 6.2.5 Swapping HUB procedure (Virtual NIC mode / IP address is changed)

The following shows the procedure in which the IP address is changed after swapping HUBs.



1. Stop network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon off -n shaX
```

2. To maintain communications, switch the NIC so that the HUB to be swapped is on standby.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethY
```

3. Swap the HUB.

4. To make sure that HUB 3 has been set correctly, check whether you can ping HUB3 successfully. If there is no response, check the connections of the HUB itself and other devices.

```
# ping 192.168.10.251
```

5. Switch back to the NIC you want to use, if necessary.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

6. Change the monitoring target of network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target -n shaX -p  
192.168.10.253,192.168.10.252
```

7. Start network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon on -n shaX
```

## 6.3 NIC maintenance (for RHEL5)

---

This section describes NIC maintenance procedures. The following two types of procedures are available depending on the system state. Note that the active maintenance during system operation is possible only when PRIMEQUEST 1000 Series is used. For further details on swapping NICs, refer to the manual that is provided with the hardware.

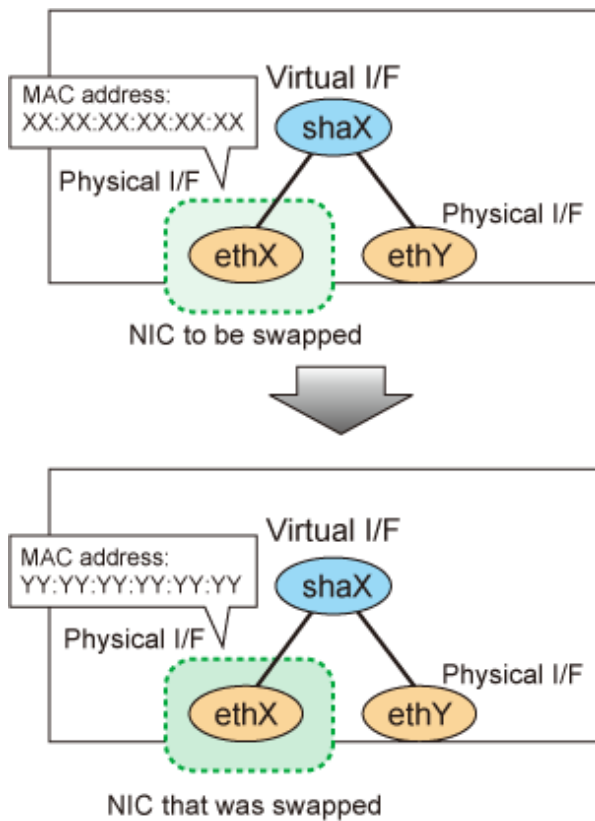
- Swapping NICs after stopping the system (shutdown maintenance)
- Swapping NICs while the system is in operation (active maintenance)

### 6.3.1 Shutdown maintenance of NIC

---

The following describes the procedure for swapping a NIC after stopping the system. The MAC address is changed after the NIC is swapped, so you need to modify the operating system configuration file.





1. Shut down the system.

```
# shutdown -h now
```

2. Swap the NIC.
3. Boot the system in single user mode.
4. Modify the operating system network configuration file. Change the HWADDR item according to the MAC address of the changed NIC.

[Fast switching mode, NIC switching mode, and GS linkage mode]

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethX
DEVICE=ethX
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet
```

[Virtual NIC mode]

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethX
DEVICE=ethX
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
```

```
ONBOOT=yes
DEVICETYPE=hanet
```

5. In RHEL5, collect the latest hardware information.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
# mv /etc/sysconfig/network-scripts/ifcfg-ethX \
/etc/sysconfig/network-scripts/ifcfg-ethX.bak
# /sbin/kudzu
# cp /etc/modprobe.conf.bak /etc/modprobe.conf
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak \
/etc/sysconfig/network-scripts/ifcfg-ethX
```

The backslash (\) at the end of line indicates no break.

6. Reboot the system. If the kudzu selection window is displayed at system startup, select Keep Configuration after Ignore.

```
# shutdown -r now
```

## 6.3.2 Active maintenance of NIC

This section describes how to set the PCI Hot Plug for redundant NIC.

For the procedure for setting up the PCI Hot Plug provided by PRIMEQUEST 1000 Series, see the following manual:

- PRIMEQUEST 1000 Series Administration Manual



### Note

Be sure to check the hot replacement procedure in the latest manual before performing hot maintenance for NIC.

The following table shows what active operation is enabled through PCI Hot Plug.

Table 6.2 Active maintenance with PCI Hot Plug in redundant line control function

Mode	System configuration	PCI Hot Plug		
		Add	Remove	Swap
Fast switching mode	Single system	A	A	A
	Cluster system	B (*1)	B (*2)	A
NIC switching mode	Single system	A	A	A
	Cluster system	B (*1)	B (*2)	A
Virtual NIC mode	Single system	A	A	A
	Cluster system	B (*1)	B (*2)	A
GS linkage mode	Single system	N	N	A
	Cluster system	N	N	A

[Meaning of the symbols]

A: Active maintenance is enabled when GLS is running

B: Active maintenance is enabled when GLS is stopped

N: Not supported

- \*1) Addition procedure for PCI Hot Plug in a cluster system

1. Add NIC.

For details, see the manuals for PRIMEQUEST 1000 Series.

2. Add the configuration for virtual interfaces.

For details, see "[5.2.1 Adding configuration](#)".

**\*2) Removal procedure for PCI Hot Plug in a cluster system**

1. Delete virtual interfaces.

For details, see "[5.2.3 Deleting configuration](#)".

2. Delete NIC.

For details, see the manuals for PRIMEQUEST 1000 Series.



**Note**

The hardware change detection tool (kudzu (1)) may be run when the system is rebooted after a NIC is added, removed, or swapped. In such cases, take appropriate action by following the steps below.

Operation	Action for Kudzu(8)
Add	Ignore
Remove	Keep Configuration
Swap	Keep Configuration, and then Ignore

**1) If a NIC has been added**

kudzu (8) displays a window for specifying whether to add device information for the added NIC to the system. From [Configure], [Ignore], and [Do Nothing], select [Ignore].

**2) If a NIC has been removed**

kudzu (8) displays a window for specifying whether to delete the device information for the removed NIC from the system. From [Remove Configuration], [Keep Configuration], and [Do Nothing], select [Keep Configuration].

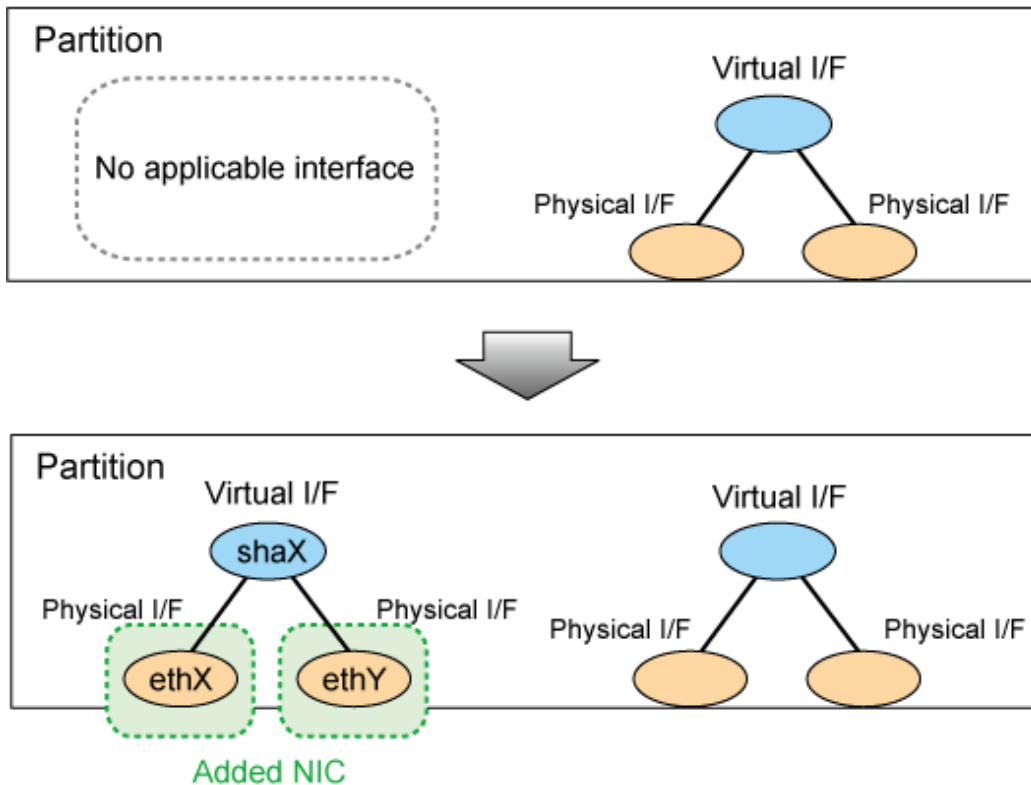
**3) If a NIC has been swapped**

kudzu (8) displays a window to specify whether to delete the device information for the removed NIC from the system . Keep the device information on the system for added NICs. From [Remove Configuration], [Keep Configuration], and [Do Nothing], select [Keep Configuration]. kudzu (8) then displays a window to specify whether to add the device information for the NIC added to the system. From [Configure], [Ignore], and [Do Nothing], select [Ignore].

### 6.3.2.1 Addition procedure

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

Figure 6.1 Addition of a virtual interface for making the added NICs (ethX,ethY) redundant



### For Fast switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Make sure that power to the target PCI slot is off.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# cat /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
0
```

3. Add a NIC to the PCI slot.
4. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

5. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 2 to 5.

6. Perform post-addition processing.

1) The added NICs must be activated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 5 for "HWADDR". Also specify "HOTPLUG=no".

ifcfg-ethX

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

ifcfg-ethY

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

2) Add the added NIC to the /etc/modprobe.conf file, which allows the NIC to be associated with the driver. The following is an example of /etc/modprobe.conf.

/etc/modprobe.conf

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

3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

4) Activate the added NICs.

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

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

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

6) Make the virtual interface settings to make the NICs redundant.

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

7) Activate the virtual interface.

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

## For NIC switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093 0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Make sure that power to the target PCI slot is off.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# cat /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
0
```

3. Add a NIC to the PCI slot.

4. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

5. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 2 to 5.

6. Perform post-addition processing.

1) The current NIC must be activated and the standby NIC must be deactivated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 5 for "HWADDR". Specify "HOTPLUG=no" for both NICs.

ifcfg-ethX (Active interface)

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

ifcfg-ethY (Standby interface)

```
DEVICE=ethY
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

2) Add the added NIC to the /etc/modprobe.conf file, which allows the NIC to be associated with the driver. The following is an example of /etc/modprobe.conf.

/etc/modprobe.conf

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

3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

4) Activate the added NICs.

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

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

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

6) Make the virtual interface settings to make the NICs redundant.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX -m d -i ipaddress1
-e ipaddress2 -t ethX,ethY
```

7) Specify hub monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n shaX -p ipaddr1,ipaddr2
```

8) If necessary, set the standby patrol function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaY -m p -t shaX
```

9) Restart GLS to enable the changed settings. This restart also activates the virtual interface and starts its monitoring.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

## For Virtual NIC mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Make sure that power to the target PCI slot is off.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# cat /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
0
```

3. Add a NIC to the PCI slot.

4. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```



5. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 2 to 5.

6. Perform post-addition processing.

1) The current NIC must be activated and the standby NIC must be deactivated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 5 for "HWADDR". Specify "HOTPLUG=no," "ONBOOT=yes," and "DEVICETYPE=hanet" for both NICs.

ifcfg-ethX (Active interface)

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

ifcfg-ethY (Standby interface)

```
DEVICE=ethY
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

2) Add the added NIC to the /etc/modprobe.conf file, which allows the NIC to be associated with the driver. The following is an example of /etc/modprobe.conf.

modprobe.conf

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

3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

4) Activate the added NICs.

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

5) Make the virtual interface settings to make the NICs redundant.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX -m v -t ethX,ethY
```

6) Set the IP address or the netmask and so on.

To make the virtual interface of GLS available, edit the network configuration file for the virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX) and configure IP addresses.

ifcfg-shaX

```
DEVICE=shaX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

7) If necessary, set the HUB monitoring destination for the network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target -n shaX -p ipaddr1,ipaddr2
```

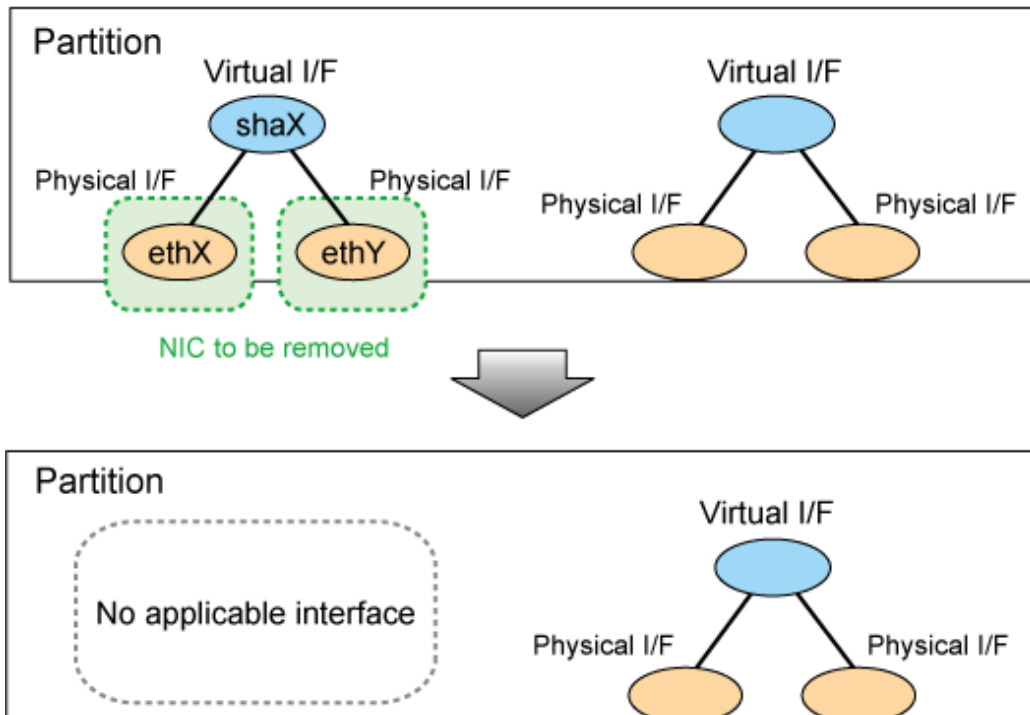
8) Activate the virtual interface.

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

### 6.3.2.2 Removal procedure

This section describes the procedure for removing NICs whose virtual interface makes them redundant.

Figure 6.2 Removing NICs whose virtual interface makes them redundant (ethX, ethY)



## For Fast switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for removing a card.

- 1) Deactivate the virtual interface.

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

- 2) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

- 3) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i network_address
```

- 4) Deactivate the target NIC.

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

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 4.

5. Perform post-removal processing.

- 1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

- 2) Delete the setting of a deleted interface from /etc/modprobe.conf.

/etc/modprobe.conf

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
```

```
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 # Remove
alias ethY e1000 # Remove
```

3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

## For NIC switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for removing a card.

- 1) Deactivate the virtual interface.

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

- 2) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

- 3) Stop hub monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

- 4) Delete the hub monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll delete -n shaX
```

- 5) Delete the standby patrol function. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaY
```

6) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

7) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i network_address
```

8) Deactivate the target NIC.

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

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 4.

5. Perform post-removal processing.

1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

2) Delete the setting of a deleted interface from /etc/modprobe.conf.

/etc/modprobe.conf

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

3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

4) Restart GLS to enable the changed settings.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

## For Virtual NIC mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for removing a card.

- 1) Deactivate the virtual interface.

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

- 2) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

- 3) Check the slot number of the PCI slot on which the NIC to be removed is installed.

For details, see the manuals for PRIMEQUEST 1000 Series.

- 4) Deactivate the interface of the NIC to be removed.

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

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 4.

5. Perform post-removal processing.

- 1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

- 2) Delete the setting of a deleted interface from /etc/modprobe.conf.

modprobe.conf

```
alias eth1 e1000
alias eth2 bcm5700
alias eth3 bcm5700
alias eth4 bcm5700
```

```
alias eth5 bcm5700
alias eth6 bcm5700
alias eth7 bcm5700
alias eth8 bcm5700
alias eth9 bcm5700
alias eth10 e100
alias eth11 e100
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias usb-controller ehci-hcd
alias usb-controller1 uhci-hcd
alias scsi_hostadapter2 lpfc
alias ethX e1000 # Remove
alias ethY e1000 # Remove
```

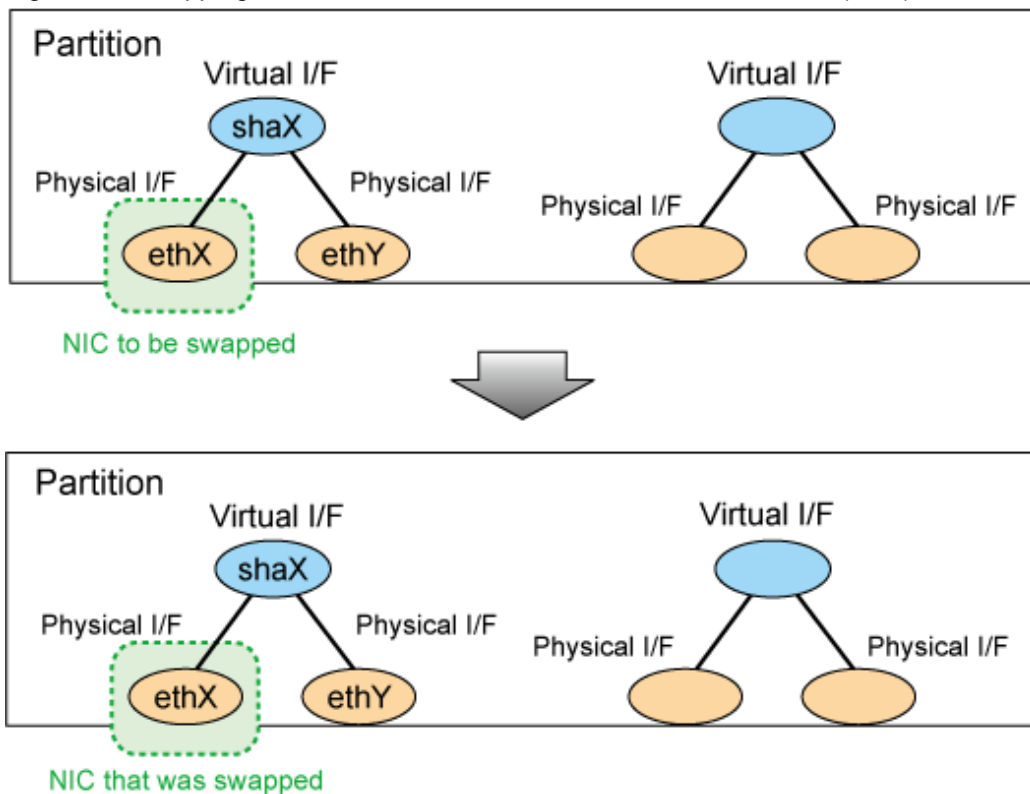
3) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

### 6.3.2.3 Swapping procedure

This section describes the procedure for swapping a NIC whose virtual interface makes it redundant.

Figure 6.3 Swapping a NIC whose virtual interface makes it redundant (ethX)



#### For Fast switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

#### Installation procedure

```
# /sbin/modprobe pciehp
```

#### 2. Prepare for swapping a card.

1) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
shaX      Active  t    OFF  ethX(CUT), ethY(ON)
```

3) Deactivate the NIC.

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

#### 3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

#### 4. Swap the NIC in the PCI slot.

#### 5. Backup setting files.

If you are using RHEL5 for the operating system, backup the following files.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
# mv /etc/sysconfig/network-scripts/ifcfg-ethX \
/etc/sysconfig/network-scripts/ifcfg-ethX.bak
```

#### 6. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

#### 7. Collect the current hardware information

When using RHEL5, take the following steps to collect hardware information. Also, restore the files backed up in Step 5. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# /sbin/kudzu
# cp /etc/modprobe.conf.bak /etc/modprobe.conf
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak \
/etc/sysconfig/network-scripts/ifcfg-ethX
```

#### 8. Check the hardware address.

An interface (ethX) is created for the swapped NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address of the swapped NIC (HWaddr).



9. Perform post-swap processing.

1) Change the specified value of "HWADDR" in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 8.

ifcfg-ethX (Swapped NIC)

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

2) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

3) Activate the swapped NIC.

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

4) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 2).

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

5) Enter the dsphanet command to confirm that the device status of the swapped NIC is "ON".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
  Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
shaX       Active   t    OFF   ethY(ON),ethX(ON)
```

## For NIC switching mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for swapping a card.

1) Stop hub monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

2) Stop standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

3) Enter the dsphanet command to check the status of the NIC to be swapped. The NIC must be in a different state from that of an active NIC (the NIC must be in the "OFF" or "STOP" state). If the NIC is active, follow Step 4 to switch its state to standby.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+---+---+-----+
shaX      Active   d   OFF  ethX(ON), ethY(OFF)
```

4) If the NIC is an active NIC, switch its state to standby. After the switch, enter the dsphanet command to confirm that the NIC is a standby NIC(OFF).

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+---+---+-----+
shaX      Active   d   OFF  ethX(OFF), ethY(ON)
```

5) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

6) Deactivate the NIC.

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

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Swap the NIC in the PCI slot.

5. Backup setting files.

If you are using RHEL5 for the operating system, backup the following files.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
# mv /etc/sysconfig/network-scripts/ifcfg-ethX \
/etc/sysconfig/network-scripts/ifcfg-ethX.bak
```

6. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

## 7. Collect the current hardware information

When using RHEL5, take the following steps to collect hardware information. Also, restore the files backed up in Step 5. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# /sbin/kudzu
# cp /etc/modprobe.conf.bak /etc/modprobe.conf
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak \
/etc/sysconfig/network-scripts/ifcfg-ethX
```

## 8. Check the hardware address.

An interface (ethX) is created for the swapped NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address of the swapped NIC (HWaddr).

## 9. Perform post-swap processing.

1) Change the specified value of "HWADDR" in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 8.

ifcfg-ethX (Swapped NIC)

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

2) Change the interface name of the swapped NIC to the name specified in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the same interface name and hardware address in the nameif (8) command as those in "DEVICE" and "HWADDR" in the ifcfg-ethX file that was set in 1) of step 9. When the nameif (8) command is executed, the specified interface must be deactivated.

```
# /sbin/nameif ethX ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
```

3) Set the state of the swapped NIC to that of a standby NIC of GLS. Confirm that an IPv4 address is not assigned and the "UP" and "NOARP" flags are set. If an IPv6 address is assigned to the virtual interface, this step is not necessary.

```
# /sbin/ifconfig ethX 0 -arp up
# /sbin/ifconfig ethX
ethX      Link encap:Ethernet  HWaddr ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
          inet6 addr: fe80::XXXXXXXXXXXXXXXX/64 Scope:Link
          UP BROADCAST NOARP MULTICAST  MTU:1500  Metric:1
```

4) If necessary, fail-back the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

5) Start standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/strptl -n shaY
```

6) Restart hub monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

7) Restart interface status monitoring.

```
# /bin/rm /var/opt/FJSVhanet/tmp/disable_watchif
```

8) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

## For Virtual NIC mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for swapping a card.

1) Stop network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon off
```

2) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

3) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+-----+
shaX      Active   v    OFF  ethX(CUT), ethY(ON)
```

4) Deactivate the NIC.

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

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Swap the NIC in the PCI slot.

5. Backup setting files.

If you are using RHEL5 for the operating system, backup the following files.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
# mv /etc/sysconfig/network-scripts/ifcfg-ethX \
/etc/sysconfig/network-scripts/ifcfg-ethX.bak
```

#### 6. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

#### 7. Collect the current hardware information

When using RHEL5, take the following steps to collect hardware information. Also, restore the files backed up in Step 5. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# /sbin/kudzu
# cp /etc/modprobe.conf.bak /etc/modprobe.conf
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak \
/etc/sysconfig/network-scripts/ifcfg-ethX
```

#### 8. Check the hardware address.

An interface (ethX) is created for the swapped NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address of the created interface (HWaddr). For details, see the manuals for PRIMEQUEST 1000 Series.

#### 9. Perform post-swap processing.

1) Change the specified value of "HWADDR" in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 8.

ifcfg-ethX (Swapped NIC)

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

2) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

#### 3) Activate the swapped NIC.

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

4) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 2).

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

5) Enter the dsphanet command to confirm that the device status of the swapped NIC is "OFF".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
shaX      Active  v    OFF  ethX(OFF),ethY(ON)
```

6) If necessary, fail-back the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

7) Restart network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon on
```

## For GS linkage mode

1. Confirm that the PCI Hot Plug driver is installed.

If the PCI Hot Plug driver is not installed, install it according to the manuals for PRIMEQUEST 1000 Series.

Confirmation procedure

```
# lsmod | grep pciehp
pciehp                75093  0
```

Installation procedure

```
# /sbin/modprobe pciehp
```

2. Prepare for swapping a card.

1) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
shaX      Active   c    OFF  ethX(CUT), ethY(ON)
```

3. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 0 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

4. Swap the NIC in the PCI slot.

5. Backup setting files.

If you are using RHEL5 for the operating system, backup the following files.

```
# cp /etc/modprobe.conf /etc/modprobe.conf.bak
# mv /etc/sysconfig/network-scripts/ifcfg-ethX \
/etc/sysconfig/network-scripts/ifcfg-ethX.bak
```

6. Turn on power to the PCI slot.

For details, see the manuals for PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<BUS-number_slot-number>"/power
```

## 7. Collect the current hardware information

When using RHEL5, take the following steps to collect hardware information. Also, restore the files backed up in Step 5. For details, see the manuals for PRIMEQUEST 1000 Series.

```
# /sbin/kudzu
# cp /etc/modprobe.conf.bak /etc/modprobe.conf
# mv /etc/sysconfig/network-scripts/ifcfg-ethX.bak \
/etc/sysconfig/network-scripts/ifcfg-ethX
```

## 8. Check the hardware address.

An interface (ethX) is created for the swapped NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address of the swapped NIC (HWaddr).

## 9. Perform post-swap processing.

1) Change the specified value of "HWADDR" in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>) to the hardware address of the swapped NIC that was checked in Step 8.

ifcfg-ethX (Swapped NIC)

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

2) Change the interface name of the swapped NIC to the name specified in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the same interface name and hardware address in the nameif (8) command as those in "DEVICE" and "HWADDR" in the ifcfg-ethX file that was set in 1) of step 9. When the nameif (8) command is executed, the specified interface must be deactivated.

```
# /sbin/nameif ethX ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
```

3) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 2).

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

4) Enter the dsphanet command to confirm that the device status of the swapped NIC is "ON".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+-----+
shaX      Active   c    OFF  ethY(ON),ethX(ON)
```

5) Restore the PCI Hot Plug driver. If you have installed the PCI Hot Plug driver according to 1., execute the following command to remove it.

```
# /sbin/modprobe -r pciehp
```

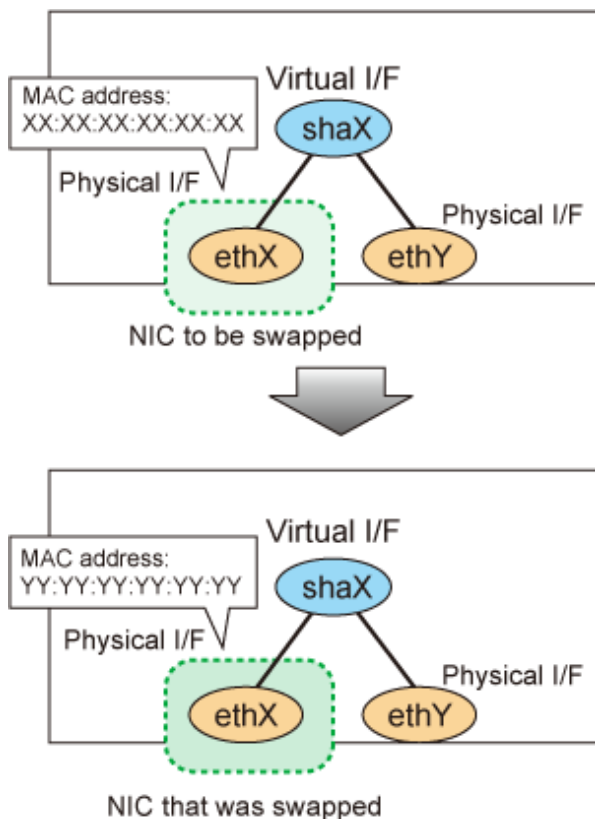
## 6.4 NIC maintenance (for RHEL6)

This section describes NIC maintenance procedures. The following two types of procedures are available depending on the system state. Note that the active maintenance during system operation is possible only when PRIMEQUEST is used. For further details on swapping NICs, refer to the manual that is provided with the hardware.

- Swapping NICs after stopping the system (shutdown maintenance)
- Swapping NICs while the system is in operation (active maintenance)

### 6.4.1 Shutdown maintenance for a NIC

The following describes the procedure for swapping a NIC after stopping the system on RHEL6. The MAC address is changed after the NIC is swapped, so you need to modify the operating system configuration file.



1. Delete the entry information related to the NIC before swap from the rule file `/etc/udev/rules.d/70-persistent-net.rules` for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

The backslash (\) at the end of line indicates no break.

2. Shut down the system.

```
# shutdown -h now
```

3. Swap the NIC.



4. Boot the system in single user mode.
5. Check that the entry information related to the NIC after swap is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="YY:YY:YY:YY:YY:YY", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

The backslash (\) at the end of line indicates no break.

6. If interface names are switched before and after swapping NICs, edit the interface name in the rule file of udev function.
7. Modify the operating system network configuration file. Change the HWADDR item according to the MAC address of the changed NIC.

[For Fast switching mode, NIC switching mode, and GS linkage mode]

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethX
DEVICE=ethX
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
BROADCAST=XXX.XXX.XXX.XXX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
NETWORK=XXX.XXX.XXX.XXX
ONBOOT=yes
TYPE=Ethernet
```

[For Virtual NIC mode]

```
# vi /etc/sysconfig/network-scripts/ifcfg-ethX
DEVICE=ethX
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

8. Reboot the system.

```
# shutdown -r now
```

## 6.4.2 Active maintenance of NIC

This section describes the PCI Hot Plug for redundant NIC by Redundant line control function.

For the outline and the procedure for setting up PCI Hot Plug provided by PRIMEQUEST, see the following manuals:

- PRIMEQUEST 1000 Series  
PRIMEQUEST 1000 Series Administration Manual
- PRIMEQUEST 2000 Series  
PRIMEQUEST 2000 Series Administration Manual



## Note

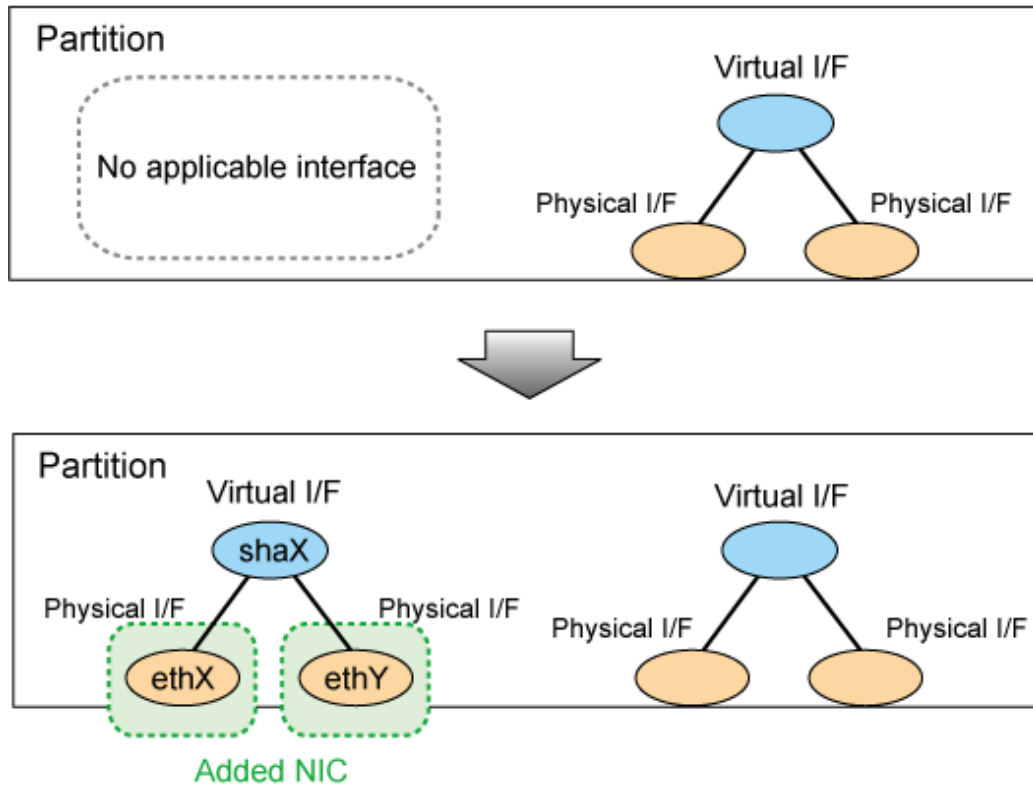
Make sure to check the procedure for the PCI Hot Plug in the latest manual before performing active maintenance for NIC.

For active maintenance with PCI Hot Plug in redundant line control function, see "[6.3.2 Active maintenance of NIC.](#)"

### 6.4.2.1 Addition procedure

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

Figure 6.4 Addition of a virtual interface for making the added NICs (ethX,ethY) redundant



#### For Fast switching mode

1. Make sure that power to the target PCI slot is off.

For details, see the following manuals:

- PRIMEQUEST 1000 Series

"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"

- PRIMEQUEST 2000 Series

"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# cat /sys/bus/pci/slots/"<slot-number>"/power
0
```

2. Add a NIC to the PCI slot.
3. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series

"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"

- PRIMEQUEST 2000 Series

"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

4. Check that the entry information related to the NIC after addition is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. If the interface (ethX) created by turning on the power for the added NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

6. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 1 to 6.

7. Perform post-addition processing.

1) The added NICs must be activated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 6 for "HWADDR". Specify "HOTPLUG=no" and "ONBOOT=yes" in the interface setting files of NICs for redundancy.

ifcfg-ethX

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

ifcfg-ethY

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

2) Activate the added NICs.

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

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

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

4) Make the virtual interface settings to make the NICs redundant.

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

5) Activate the virtual interface.

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

## For NIC switching mode

1. Make sure that power to the target PCI slot is off.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# cat /sys/bus/pci/slots/"<slot-number>"/power
0
```

2. Add a NIC to the PCI slot.

3. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

4. Check that the entry information related to the NIC after addition is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. If the interface (ethX) created by turning on the power for the added NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

6. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 1 to 6.

7. Perform post-addition processing.

1) The added NICs must be activated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 6 for "HWADDR". In addition, specify "HOTPLUG=no" and "ONBOOT=yes" in the interface setting files of NICs for redundancy.

ifcfg-ethX (Active interface)

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

ifcfg-ethY (Standby interface)

```
DEVICE=ethY
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- 2) Activate the added NICs.

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

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

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

- 4) Make the virtual interface settings to make the NICs redundant.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX -m d -i ipaddress1 -e ipaddress2 -t
ethX,ethY
```

- 5) Specify HUB monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll create -n shaX -p ipaddr1,ipaddr2
```

- 6) If necessary, set the standby patrol function.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaY -m p -t shaX
```

- 7) Restart GLS to enable the changed settings. This restart also activates the virtual interface and starts its monitoring.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

## For Virtual NIC mode

1. Make sure that power to the target PCI slot is off.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# cat /sys/bus/pci/slots/"<slot-number>"/power
0
```

2. Add a NIC to the PCI slot.

3. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

4. Check that the entry information related to the NIC after addition is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. If the interface (ethX) created by turning on the power for the added NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

6. Check the hardware address.

An interface (ethX) is created for the added NIC when power is turned on. Execute the ifconfig (8) command to check the hardware address (HWaddr) of the created interface. To add more NICs, repeat steps 1 to 6.

7. Perform post-addition processing.

1) The added NICs must be activated at system startup. For this purpose, make the settings shown below in each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>). Specify the hardware address that was checked in Step 6 for "HWADDR". Specify "HOTPLUG=no", "ONBOOT=yes", and "DEVICETYPE=hnet" in the interface setting files of NICs for redundancy.

ifcfg-ethX (Active interface)

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
DEVICETYPE=hanet
```

ifcfg-ethY (Standby interface)

```
DEVICE=ethY
BOOTPROTO=static
HWADDR=YY:YY:YY:YY:YY:YY
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

2) Activate the added NICs.

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

3) Make the virtual interface settings to make the NICs redundant.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n shaX -m v -t ethX,ethY
```

4) Set the IP address or the netmask and so on.

To make the virtual interface of GLS available, edit the network configuration file for the virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX) and configure IP addresses.

ifcfg-shaX

```
DEVICE=shaX
IPADDR=XXX.XXX.XXX.XXX
NETMASK=XXX.XXX.XXX.XXX
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

5) If necessary, specify HUB monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target -n shaX -p ipaddr1,ipaddr2
```

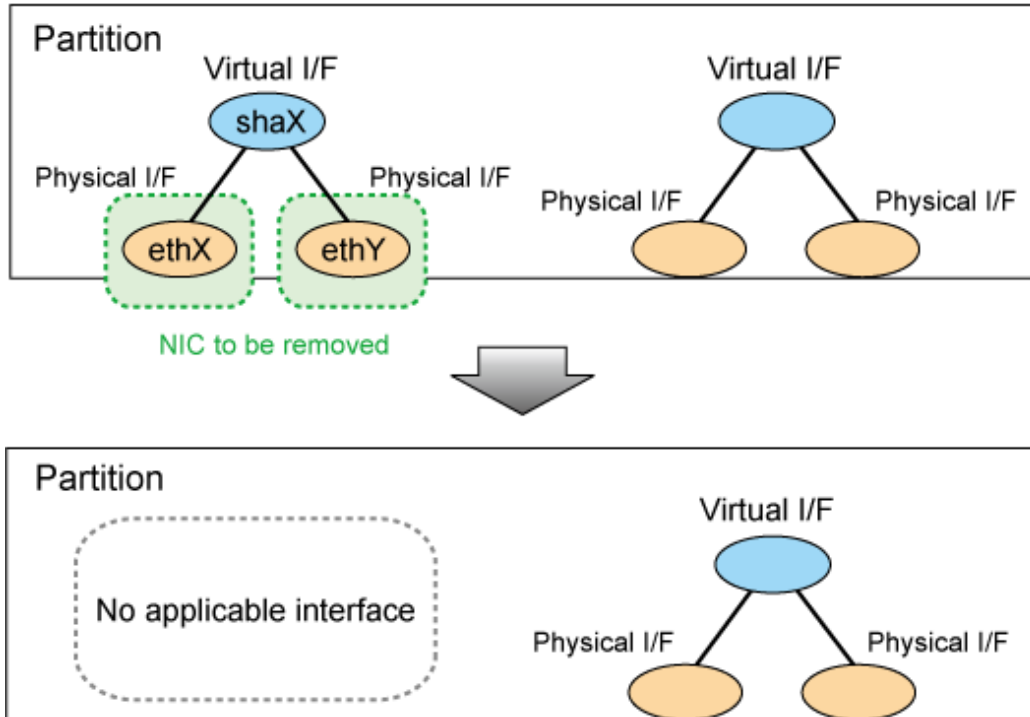
6) Activate the virtual interface.

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

## 6.4.2.2 Removal procedure

This section describes the procedure for removing NICs whose virtual interface makes them redundant.

Figure 6.5 Removing NICs whose virtual interface makes them redundant (ethX, ethY)



### For Fast switching mode

1. Prepare for removing a card.

- 1) Deactivate the virtual interface.

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

- 2) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

- 3) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i network_address
```

- 4) Check the slot number of the PCI slot on which the NIC to be removed is installed.

- 5) Deactivate the interface of the NIC to be removed.

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

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```



3. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 3.

4. Perform post-removal processing.

1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

2) Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*", \
ATTR{address}=="YY:YY:YY:YY:YY:YY", ATTR{type}=="1", KERNEL=="eth*", NAME="ethY"
```

3) Update udev with the edited rule.

When loading the rule defined in the rule file at startup, udevd holds it in the memory and the rule is not updated by only changing the rule file. Then update udev with the new rule.

```
# udevadm control --reload-rules
```

## For NIC switching mode

1. Prepare for removing a card.

1) Deactivate the virtual interface

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

2) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

3) Stop HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

4) Delete the HUB monitoring destination information.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll delete -n shaX
```

5) Delete the standby patrol function. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaY
```

6) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

7) If necessary, delete the subnet mask information about the virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i network_address
```

8) Check the slot number of the PCI slot on which the NIC to be removed is installed.

9) Deactivate the interface of the NIC to be removed.

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

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 3.

4. Perform post-removal processing.

1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

2) Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"

# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="YY:YY:YY:YY:YY:YY", ATTR{type}=="1", KERNEL=="eth*", NAME="ethY"
```

3) Update udev with the edited rule.

When loading the rule defined in the rule file at startup, udevd holds it in the memory and the rule is not updated by only changing the rule file. Then update udev with the new rule.

```
# udevadm control --reload-rules
```

4) Restart GLS to enable the changed settings.

```
# /opt/FJSVhanet/usr/sbin/resethanet -s
```

## For Virtual NIC mode

1. Prepare for removing a card.

1) Deactivate the virtual interface.

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

Stop monitoring by stphanet if it is running.

2) Delete the virtual interface configuration information.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n shaX
```

3) Check the slot number of the PCI slot on which the NIC to be removed is installed.

4) Deactivate the interface of the NIC to be removed.

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

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Remove the NIC from the PCI slot.

To remove more NICs, repeat steps 2 to 3.

4. Perform post-removal processing.

1) Delete each interface setting file (/etc/sysconfig/network-scripts/ifcfg-eth<x>).

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

2) Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"

# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="YY:YY:YY:YY:YY:YY", ATTR{type}=="1", KERNEL=="eth*", NAME="ethY"
```

3) Update udev with the edited rule.

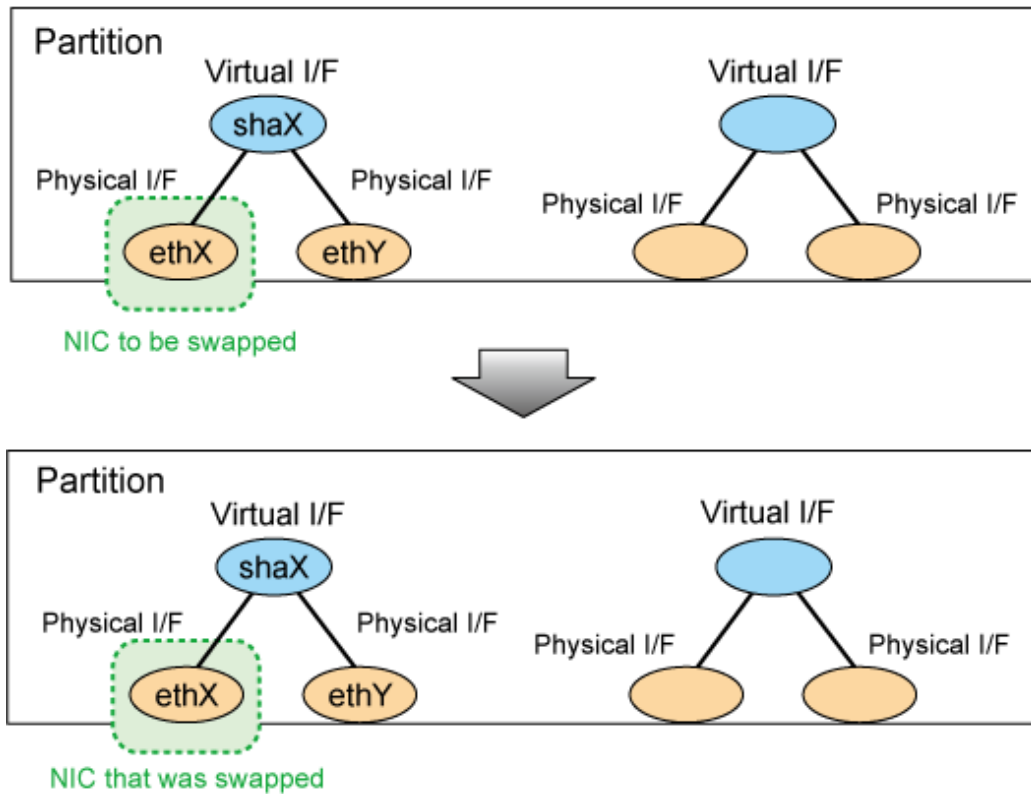
When loading the rule defined in the rule file at startup, udevd holds it in the memory and the rule is not updated by only changing the rule file. Then update udev with the new rule.

```
# udevadm control --reload-rules
```

### 6.4.2.3 Swapping procedure

This section describes the procedure for swapping a NIC whose virtual interface makes it redundant.

Figure 6.6 Swapping a NIC whose virtual interface makes it redundant (ethX)



### For Fast switching mode

1. Prepare for swapping a card.

1) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+-----+
shaX      Active   t    OFF  ethX(CUT),ethY(ON)
```

3) Deactivate the NIC.

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

4) Back up the network configuration file of the interface.

```
# cd /etc/sysconfig/network-scripts
# mkdir temp
# mv ifcfg-ethX temp
```

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series

- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Swap the NIC in the PCI slot.
4. Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

6. If the interface (ethX) created by turning on the power for the swapped NIC is activated, deactivate it..

```
# /sbin/ifconfig ethX down
```

7. Check that the entry information related to the NIC after swap is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="ZZ:ZZ:ZZ:ZZ:ZZ:ZZ", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

8. If interface names are switched before and after swapping NICs, turn off the power of the PCI slot. Then edit the interface name in the rule file for udev function and turn on the power of the PCI slot again. For details, see the following manuals:

- PRIMEQUEST 1000 Series  
"Network card replacement procedure" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series  
"Network card replacement procedure" in "PRIMEQUEST 2000 Series Administration Manual"

9. Check the hardware address.

Check that the hardware address (HWaddr) of the created interface on the swapped NIC from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

10. Perform post-swap processing.

1) Change the HWADDR in the interface setting file, which was backed up, to the hardware address of the swapped NIC that was checked in Step 9.

```
# cd /etc/sysconfig/network-scripts
# mv temp/ifcfg-ethX .
# rmdir temp
```

ifcfg-ethX (Swapped NIC)

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

2) Activate the swapped NIC.

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

3) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

4) Enter the dsphanet command to confirm that the device status of the swapped NIC is "ON".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+---+---+-----+
shaX      Active   t    OFF  ethY(ON),ethX(ON)
```

## For NIC switching mode

1. Prepare for swapping a card.

1) Stop HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

2) Stop standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

3) Enter the dsphanet command to check the status of the NIC to be swapped. The NIC must be in a different state from that of an active NIC (the NIC must be in the "OFF" or "STOP" state). If the NIC is active, follow Step 4) to switch its state to standby.

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+---+---+-----+
shaX      Active   d    OFF  ethX(ON),ethY(OFF)
```

4) If the NIC is an active NIC, switch its state to standby. After the switch, enter the dsphanet command to confirm that the NIC is a standby NIC(OFF).

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL   Device
+-----+-----+---+---+-----+
shaX      Active    d   OFF   ethX(OFF),ethY(ON)
```

5) Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

6) Deactivate the NIC.

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

7) Back up the network configuration file of the interface.

```
# cd /etc/sysconfig/network-scripts
# mkdir temp
# mv ifcfg-ethX temp
```

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Swap the NIC in the PCI slot.

4. Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series.

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

6. If the interface (ethX) created by turning on the power for the swapped NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

7. Check that the entry information related to the NIC after swap is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="ZZ:ZZ:ZZ:ZZ:ZZ:ZZ", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

8. If interface names are switched before and after swapping NICs, turn off the power of the PCI slot. Then edit the interface name in the rule file for udev function and turn on the power of the PCI slot again. For details, see the following manuals:

- PRIMEQUEST 1000 Series

"Network card replacement procedure" in "PRIMEQUEST 1000 Series Administration Manual"

- PRIMEQUEST 2000 Series

"Network card replacement procedure" in "PRIMEQUEST 2000 Series Administration Manual"

9. Check the hardware address.

Check that the hardware address (HWaddr) of the created interface on the swapped NIC from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

10. Perform post-swap processing.

- 1) Change the HWADDR in the interface setting file, which was backed up, to the hardware address of the swapped NIC that was checked in Step 9.

```
# cd /etc/sysconfig/network-scripts
# mv temp/ifcfg-ethX .
# rmdir temp
```

ifcfg-ethX (Swapped NIC)

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

- 2) Set the state of the swapped NIC to that of a standby NIC of GLS. Confirm that an IPv4 address is not assigned and the "UP" and "NOARP" flags are set. If an IPv6 address is assigned to the virtual interface, this step is not necessary.

```
# /sbin/ifconfig ethX 0 -arp up
```

```
# /sbin/ifconfig ethX
ethX      Link encap:Ethernet  HWaddr ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
          inet6 addr: fe80::XXXXXXXXXXXXXXXX/64 Scope:Link
          UP BROADCAST NOARP MULTICAST  MTU:1500  Metric:1
```

- 3) If necessary, fail-back the NIC.



```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

4) Start standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/strptl -n shaY
```

5) Restart HUB monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

6) Restart interface status monitoring.

```
# /bin/rm /var/opt/FJSVhanet/tmp/disable_watchif
```

## For Virtual NIC mode

1. Prepare for swapping a card.

1) Stop network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon off
```

2) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

3) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name          Status   Mode CL  Device
+-----+-----+-----+-----+-----+
shaX          Active    v    OFF  ethX(CUT),ethY(ON)
```

4) Deactivate the NIC.

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

5) Back up the network configuration file of the interface.

```
# cd /etc/sysconfig/network-scripts
# mkdir temp
# mv ifcfg-ethX temp
```

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Swap the NIC in the PCI slot.

4. Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
```

```
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series  
"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series  
"PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

6. If the interface (ethX) created by turning on the power for the swapped NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

7. Check that the entry information related to the NIC after swap is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="ZZ:ZZ:ZZ:ZZ:ZZ:ZZ", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

8. If interface names are switched before and after swapping NICs, turn off the power of the PCI slot. Then edit the interface name in the rule file for udev function and turn on the power of the PCI slot again. For details, see the following manuals:

- PRIMEQUEST 1000 Series  
"Network card replacement procedure" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series  
"Network card replacement procedure" in "PRIMEQUEST 2000 Series Administration Manual"

9. Check the hardware address.

Check that the hardware address (HWaddr) of the created interface on the swapped NIC from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

10. Perform post-swap processing.

1) Change the HWADDR in the interface setting file, which was backed up, to the hardware address of the swapped NIC that was checked in Step 9.

```
# cd /etc/sysconfig/network-scripts
# mv temp/ifcfg-ethX .
# rmdir temp
```

ifcfg-ethX (Swapped NIC)

```
DEVICE=ethX
BOOTPROTO=static
HWADDR=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ
```

```
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

2) Activate the swapped NIC.

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

3) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

4) Enter the dsphanet command to confirm that the device status of the swapped NIC is "OFF".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
shaX      Active   v    OFF  ethX(OFF),ethY(ON)
```

5) If necessary, fail-back the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

6) Restart network monitoring.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon on
```

## For GS linkage mode

1. Prepare for swapping a card.

1) From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped.

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2) Enter the dsphanet command to confirm that the device status of the NIC is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+
shaX      Active   c    OFF  ethX(CUT),ethY(ON)
```

3) Deactivate the NIC.

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

4) Back up the network configuration file of the interface.

```
# cd /etc/sysconfig/network-scripts
# mkdir temp
# mv ifcfg-ethX temp
```

2. Turn off power to the target PCI slot.

The interface (ethX) is deleted when power is turned off. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 0 > /sys/bus/pci/slots/"<slot-number>"/power
```

3. Swap the NIC in the PCI slot.

4. Delete the entry information of the deleted interface from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

5. Turn on power to the PCI slot.

For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "PCI Card Hot Maintenance in Red Hat Enterprise Linux 6" in "PRIMEQUEST 2000 Series Administration Manual"

For example: PRIMEQUEST 1000 Series

```
# echo 1 > /sys/bus/pci/slots/"<slot-number>"/power
```

6. If the interface (ethX) created by turning on the power for the swapped NIC is activated, deactivate it.

```
# /sbin/ifconfig ethX down
```

7. Check that the entry information related to the NIC after swap is added into the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

```
# cat /etc/udev/rules.d/70-persistent-net.rules
# This file was automatically generated by the /lib/udev/write_net_rules
# program, run by the persistent-net-generator.rules rules file.
...
...
# PCI device 0xXXXX:0xXXXX (e1000)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", \
ATTR{address}=="ZZ:ZZ:ZZ:ZZ:ZZ:ZZ", ATTR{type}=="1", KERNEL=="eth*", NAME="ethX"
```

8. If interface names are switched before and after swapping NICs, turn off the power of the PCI slot. Then edit the interface name in the rule file for udev function and turn on the power of the PCI slot again. For details, see the following manuals:

- PRIMEQUEST 1000 Series
- "Network card replacement procedure" in "PRIMEQUEST 1000 Series Administration Manual"
- PRIMEQUEST 2000 Series
- "Network card replacement procedure" in "PRIMEQUEST 2000 Series Administration Manual"

9. Check the hardware address.

Check that the hardware address (HWaddr) of the created interface on the swapped NIC from the rule file /etc/udev/rules.d/70-persistent-net.rules for the udev function of the operating system.

10. Perform post-swap processing.

1) Change the HWADDR in the interface setting file, which was backed up, to the hardware address of the swapped NIC that was checked in Step 9.

```
# cd /etc/sysconfig/network-scripts
# mv temp/ifcfg-ethX .
# rmdir temp
```

ifcfg-ethX (Swapped NIC)

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

2) Activate the swapped NIC.

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

3) Restore the NIC definition that was temporarily deleted prior to swapping in 1) of Step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

4) Enter the dsphanet command to confirm that the device status of the swapped NIC is "ON".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+---+---+-----+
shaX      Active   c   OFF  ethY(ON),ethX(ON)
```

# Chapter 7 Command references

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,...]
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}
-t interface
Virtual NIC mode:
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m v -t
interfacel[,interface2]
```

```
GS linkage mode:
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m c -i
ipaddress -t interface1[,interface2,...]
```

- 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
GS linkage mode
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -i
ipaddress
```

[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. Up to 64 names can be set. Specify the virtual interface name with a string of "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. Logical virtual interface can only be configured on operation mode "t" and "c".

-m t|d|e|p|q|v|c:

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. This mode creates a virtual interface used in Fast switching mode.

d: NIC switching mode (logical IP address takeover function)

Specify this parameter to use the Redundant Line Control Function in NIC switching mode. Communication is performed by activating a physical interface to be used and its logical interface and taking over the IP address attached to the logical interface.

e: NIC switching mode (physical IP address takeover function)

Specify this parameter to use the Redundant Line Control Function in NIC switching mode. Communication is performed by taking over the IP address attached to the physical interface without activating a logical interface.

p: Standby patrol function (automatic fail-back 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 fail-back occurs until the currently used NIC encounters a failure.

q: Standby patrol function (immediate automatic fail-back)

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 fail-back immediately occurs.

v: Virtual NIC mode

Specify this parameter to use the Redundant Line Control function in Virtual NIC mode. This mode creates a virtual interface used in Virtual NIC mode.

c: GS linkage mode

Specify this parameter to use the Redundant Line Control function in GS linkage mode.

This mode creates a virtual interface used in GS linkage mode. This mode creates a virtual interface used in GS linkage mode.

The following table lists options that can be specified in each operation mode.

Operation mode	Specifiable parameter				
	inet   inet6	-n	-i	-e	-t
't' (Fast switching mode)	Supported	O	O (*6)	X	O (*1)
'd' (NIC switching mode (logical IP address takeover function))	Supported	O	O	O (*4)	O (*2)
'e' (NIC switching mode (physical IP address takeover function))	Not supported	O	O	O (*5)	O (*2)
'p' (Standby patrol function (automatic fail-back if a failure occurs))	Not supported	O	X	X	O (*3)
'q' (Standby patrol function (immediate automatic fail-back))	Not supported	O	X	X	O (*3)
'v' (Virtual NIC mode)	Not supported	O	X	X	O (*2)
'c' (GS linkage mode)	Not supported	O	O	X	O (*1)

[Meaning of the symbols] O: Required, X: 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 a physical interface that is not specified in any other operation mode. One or two physical interface can be assigned.

\*3 Specify a virtual interface specified in the operation mode "d" or "e". Only one interface can be assigned.

\*4 It is not possible to specify this parameter when set inet6 to an address form.

\*5 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).

\*6 It can specify, only when creating logical virtual interface.

-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 specified IP address or host must be defined in an /etc/hosts file. 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/hosts 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/hosts file. 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"). In cluster operation, it is possible to omit this option if an interface of NIC switching mode (operation mode is "e") is not activated by a standby node.

**-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) for standby patrol function (operation mode "p" or "q").

Specify physical interface names (such as eth0) or tagged VLAN interface names (such as eth0.1 or eth1.2) for any other mode (operation mode "t", "d" "e" "v", or "c") than standby patrol function.

## (2) copy command

Use the copy command to create different configuration information while sharing a 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/FJSVhanet/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/FJSVhanet/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/FJSVhanet/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/FJSVhanet/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 string 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/FJSVhanet/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.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print  
[IPv4,Patrol / Virtual NIC]  
Name      Hostname      Mode Physical ipaddr      Interface List  
+-----+-----+-----+-----+-----+  
sha0      192.168.10.110  d   192.160.10.10   eth0,eth1  
sha1      -               p   -               sha0  
sha2      hostC           d   hostC1          eth2,eth3  
sha3      -               p   -               sha2  
sha4      -               v   -               eth4,eth5  
  
[IPv6]  
Name      Hostname/prefix      Mode Interface List  
+-----+-----+-----+-----+  
sha0      fec0:1::123/64       d   eth0,eth1
```

Display	Contents
[IPv4,Patrol / Virtual NIC]	The information of a virtual interface for IPv4 and standby patrol and a virtual interface in Virtual NIC mode
[IPv6]	The information of an IPv6 virtual interface
Name	A virtual interface name
Hostname	The host name or IP address of a virtual interface

Display	Contents
Hostname/prefix	The host name or IP address of a virtual interface, and the prefix value
Mode	The operation mode of a virtual interface (For details, see the "-m" option of the "create" command.)
Interface List	A virtual interface name in standby patrol function (operation mode "p" or "q"). Outputs a physical interface name (such as eth0) in other mode.

#### (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 {[-i
ipaddress1] [-t interface1[,interface2,...]]}
Fast switching mode (IPv6):
/opt/FJSVhanet/usr/sbin/hanetconfig modify inet6 -n devicename -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 {[-t
interface1]}
GS linkage mode
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename {[-i
ipaddress] [-t interface1[,interface2,...]]}
```

- 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
GS linkage mode
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n devicename -i
ipaddress
```

[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 whose configuration information should be modified. This parameter is required.

**-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/hosts file. 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/hosts file. 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 standby patrol function (operation mode "p" or "q").

Specify physical interface names (such as eth0) if the operation mode of a virtual interface to be modified is not 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.

## (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 2.14
```

## [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.
- An IP address or host name to be specified to create, copy, or modify configuration information must be defined in /etc/hosts file.
- 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") and GS linkage mode (the operation mode is "c"), be sure to define to use in TCP/IP before defining a virtual interface. (Check if or not there is /etc/sysconfig/network-scripts/ifcfg-ethX 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/hosts file. 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/hosts so that it does not contain any other characters. Also, the first and last character for the host name must be alphanumeric character.
- If tagged VLAN interfaces are created in physical interfaces bundled by GLS in Virtual NIC mode, they are not used during operation.
- In Virtual NIC mode, the interface setting file of the virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX) is created or deleted at the following timing:

For creation: when a virtual interface is set by using the "create" command.

For deletion: when a virtual interface is deleted by using the "delete" command.

- The logical virtual interfaces (shaX:2 to 64) of GS linkage mode are not available as IP addresses which are taken over between nodes in the cluster by default. To use them, it is necessary to set the parameter (logical\_vip\_takeover) beforehand. For details, see "[3.6.3 Multiple logical virtual interface definition](#)".
- Even though there is an error in the physical interface configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX) while creating configuration information, the configuration information is created, but at this time, the warning message (message number: 927) is output. Modify the configuration file according to "[3.2.2 Network configuration](#)".

## [Examples]

### (1) create command

The following shows an example of the setting command used in Fast switching mode to bundle two physical interfaces (eth0 and eth1) 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 eth0,eth1
```

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 eth0,eth1
# /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 (eth0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i hosti -t eth0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (eth0 and eth1) 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
eth0,eth1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

The following shows an example of the setting command used in NIC switching mode to set two physical interfaces (eth0 and eth1) 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 -e hostj -t
eth0,eth1
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -a 02:00:00:00:00:01 -
t sha0
```

The following is an example that set two physical interfaces (eth0 and eth1) 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 eth0,eth1
or
# /opt/FJSVhanet/usr/sbin/hanetconfig inet6 create -n sha0 -m d -i hostg/64 -t
eth0,eth1
```

The following is an example of configuring two physical interfaces (eth0 and eth1) and creating a virtual interface (sha0) using IPv6 address.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

The following shows an example of the setting command used in GS linkage mode to bundle two physical interfaces (eth1 and eth2) as the virtual interface host "hostf" to duplicate the virtual interface sha0.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i hostf -t eth1,eth2
```

The following shows an example of the setting command used in NIC switching mode to set two tagged VLAN interfaces (eth0.1 and eth1.1) 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  
eth0.1,eth1.1  
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

The following shows an example of setting the virtual interface (sha0) by bundling two physical interfaces (eth0 and eth1) in Virtual NIC mode.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

The following shows an example of setting when the virtual interface (sha0) bundles one physical interface (eth0).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0
```

## (2) modify command

The following is an example of modifying bundled physical interfaces (eth0 and eth1) in the virtual interface (sha0) to different physical interfaces (eth2 and eth3).

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -t eth2,eth3
```

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
```

## (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
```

The following is an example of deleting the virtual interface (sha0) in Virtual NIC mode.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig delete -n sha0
```

## 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"), GS linkage mode("c"). This command cannot be specified for virtual interfaces in Standby patrol function (operation mode "p" or "q").
- A standby patrol function ("p" or "q") is automatically activated when activated a virtual interface of the corresponding NIC switching mode ("d" or "e").
- 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.
- If you want to activate a virtual interface using Fast switching mode or GS linkage mode, wait at least 1 minute to execute the command to activate after deactivating it.
- If tagged VLAN interfaces are created in physical interfaces bundled by GLS in Virtual NIC mode, they are not used during operation.
- Since the MAC address of bundled interfaces are rewritten in the Virtual NIC mode, when the strhanet command is executed for the virtual interface, a message which indicates the MAC address is different from the settings of the ifcfg-ethX in a system log may be output. Ignore this message.

```
/etc/sysconfig/network-scripts/ifup-eth: Device ethX has different MAC address than expected,  
ignoring.
```

- VLAN interface and the virtual bridge connected to the virtual interface of the Virtual NIC mode cannot be activated with the strhanet command. When activating it, activate them individually after executing the strhanet command. For the activation of a VLAN interface or a virtual bridge, refer to "Linux documentation".

- In Virtual NIC mode, when SHAMACADDR is set to the setting file of the virtual interface (ifcfg-shaX), the physical interface will become the promiscuous mode. While the virtual interface is being activated, the following message which indicates the promiscuous mode is output to a system log.

```
kernel: device ethX entered promiscuous mode
```

### [Examples]

The following is an example in which all virtual interfaces defined in the configuration information for Redundant Line Control Function are activated.

```
# /opt/FJSVhanet/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/FJSVhanet/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/FJSVhanet/usr/sbin/strhanet inet6
```

## 7.3 stphanet Command

---

### [Name]

stphanet - Inactivation of virtual interfaces

### [Synopsis]

```
/opt/FJSVhanet/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"), GS linkage mode("c"). It is not possible to specify to a virtual interface of a standby patrol function ("p" or "q"). A Standby patrol function ("p" or "q") is automatically deactivated when deactivated a virtual interface of the corresponding NIC switching mode ("d" or "e").
- Be sure to use a stphanet 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 stpctl command to deactivate.
- When a virtual interface of NIC switching mode is deactivated and only a virtual interface of standby patrol is activated, use stpctl command to deactivate the virtual interface of standby patrol.
- When deactivating a virtual interface, if stacked physical interfaces are not used at all, deactivate them as well.
- When using Fast switching mode on IPv6 environment, it takes maximum 30 seconds to complete stphanet command. The following message might be output to /var/log/messages, but it is not an error.  
"kernel: unregister\_netdevice: waiting for shaX to become free."
- If you want to inactivate a virtual interface using Fast switching mode or GS linkage mode, wait at least 1 minute to execute the command to activate after deactivating it.
- 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.
- If a virtual bridge is connected to a virtual interface used in Virtual NIC mode, the virtual interface cannot be deactivated. Execute this command after disconnecting the virtual bridge.

## [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 deactivate 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]
```

### [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.

### [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 / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active  d    OFF  eth0(ON),eth1(OFF)
sha1      Active  p    OFF  sha0(ON)
sha2      Active  c    OFF  eth2(ON),eth3(ON)
sha3      Active  t    OFF  eth4(OFF),eth5(OFF)
sha4      Active  v    OFF  eth6(ON),eth7(OFF)
[IPv6]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active  d    OFF  eth0(ON),eth1(OFF)
sha3      Active  t    OFF  eth4(ON),eth5(ON)
```

Display	Contents
[IPv4,Patrol / Virtual NIC]	The information of a virtual interface for IPv4 and standby patrol and a virtual interface in Virtual NIC mode
[IPv6]	Virtual interface information of an IPv6 address form.
Name	A virtual interface name. Even if the virtual interface is changed, the original name is displayed.

Display		Contents
Status	Active	The status of a virtual interface is active status.
	Inactive	The status of a virtual interface is inactive status.
Mode	t	Fast switching mode
	d	NIC switching mode (logical IP address takeover function)
	e	NIC switching mode (physical IP address takeover function)
	p	Standby patrol function (automatic fail-back if a failure occurs)
	q	Standby patrol function (immediate automatic fail-back)
	v	Virtual NIC mode
	c	GS linkage mode
CL	ON	Cluster resource
	OFF	None cluster resource
Device	(ON)	Enabled. 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. The status if the virtual interface in disabled. For Fast switching mode and GS linkage mode, 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.  If the virtual interface is in the active state in Virtual NIC mode, this shows the status of interfaces in standby.
	(STOP)	Ready for use. 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. Displays the status when an interface detects a link down in Virtual NIC mode.
	(CUT)	Unused. Displays the status if temporally dispatched by hanetnic delete command, or no NIC is provided on startup of the operating system.

The following shows the display format used when the -o option is specified.

```

# /opt/FJSSVhanet/usr/sbin/dsphanet -o
NIC      Destination Host Status
+-----+-----+-----+
eth0     habostA      Active
          habostB      Active
          habostC      Inactive
eth1     habostA      Active
          habostB      Active
          habostC      Inactive

```

Display	Contents
NIC	A physical interface name.
Destination Host	The host name of the communication target. (If the target host does not exist, it will display "none".)

Display		Contents
Status	Active	The status of the communication target is active status.
	Inactive	The status of the communication target is inactive status.

### [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
```

## 7.5 hanetmask Command

### [Name]

hanetmask - Sets, modifies, deletes, and prints a subnet mask.

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetmask command [args]
```

### [Feature description]

This hanetmask command sets/modifies/deletes/prints a subnet mask value to specify when activating a virtual IP address. For virtual IP addresses used in Virtual NIC mode, use ifcfg-shaX to set the subnet mask value instead of this command.

Command	Process outline	Authority
create	Sets a subnet mask.	Super user
print	Prints a subnet mask.	General user
modify	Modifies a subnet mask.	Super user
delete	Deletes a subnet mask.	Super user

### (1) create command

Sets a subnet mask value to a virtual IP address defined by a hanetconfig command. A form of a create command is as follows:

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

-i network\_address:

Specifies a network address of a virtual IP to set a subnet mask value in decimal dotted notation.

-m netmask:

Specifies a subnet mask value to a network address specified by -i in decimal dotted notation.

## (2) print command

It is possible to print current information of a subnet mask by a print command. A form of a print command is as follows:

```
/opt/FJSSVhanet/usr/sbin/hanetmask print [-i  
network_address1[,network_address2.....]]
```

-i network\_address1[,network\_address2.....]:

It is possible to specify a network address to print dividing by a comma (","), Here it specifies a network address specified by -i of a create command.

When not specified a -i option, all subnet mask information set at present is printed. An example of printing subnet mask information is as follows:

```
# /opt/FJSSVhanet/usr/sbin/hanetmask print  
network-address netmask  
+-----+-----+  
10.34.151.0      255.255.255.0
```

Display	Contents
network-address	A network address of a virtual IP.
netmask	A subnet mask value to set to a network address.

## (3) modify command

When modifying a subnet mask value created by a create command, use a modify command. A form of a modify command is as follows:

```
# /opt/FJSSVhanet/usr/sbin/hanetmask modify -i network_address -m  
netmask
```

-i network\_address:

Specifies a network address of subnet mask information to modify in decimal dotted notation.

-m netmask:

Specifies a modified subnet mask value to a network address specified by -i in decimal dotted notation.

## (4) delete command

When deleting a subnet mask value created by a create command, use a delete command. A form of a delete command is as follows:

```
/opt/FJSSVhanet/usr/sbin/hanetmask delete -i  
{network_address1[,network_address2.....] | all}
```

**-i network\_address1[,network\_address2.....]:**

It is possible to specify a network address to delete dividing by a comma (","). Here it specifies a network address specified by -i of a create command.

**-i all:**

Deletes all subnet mask information set at present.

### [Notes]

- When dividing a network, which a virtual interface belongs to, into a subnet, set a subnet mask value by this command without fail. If not set, it is not possible to communicate with other systems. It is not necessary to execute this command if not divide into a subnet.
- Set the same subnet mask value without fail in a system connected to the same network.
- In NIC switching mode, set the same subnet mask value as that set to a physical IP address (a value set in /etc/sysconfig/network-scripts/ifcfg-ethX file) to a network address of a virtual IP.
- The setting by this command is required in the following cases: when NIC switching mode, Fast switching mode, or GS linkage mode is used in the IPv4 configuration, when NIC switching mode or Fast switching mode is used in the dual configuration, or when the cluster takeover IP of IPv4 is used in Virtual NIC mode.
- This configuration is not required for IPv6 configuration. The configured subnet mask assigned to a physical interface is subject to the address of the virtual interface of Fast switching mode, logical virtual interface, virtual interface of NIC switching mode and physical interface.

### [Examples]

#### (1) create command

An example to define a subnet mask 255.255.255.0 to a network address 10.34.151.0 is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanetmask create -i 10.34.151.0 -m
255.255.255.0
```

#### (2) print command

Prints a list of subnet mask information.

```
# /opt/FJSVhanet/usr/sbin/hanetmask print
```

#### (3) modify command

An example to modify a subnet mask, set to an already defined network address 10.34.0.0, to 255.255.0.0 is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanetmask modify -i 10.34.0.0 -m
255.255.0.0
```

#### (4) delete command

Deletes all subnet mask information.

```
# /opt/FJSVhanet/usr/sbin/hanetmask delete -i all
```



## 7.6 hanetparam Command

---

### [Name]

hanetparam - Setting up the monitoring function for each redundant line switching mode

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetparam {-w sec | -m times | -l times | -p sec | -o times | -c {on | off}  
| -s {on | off} | -h {yes|no} | -e {yes|no} | -q sec | -r sec | -g sec}  
/opt/FJSVhanet/usr/sbin/hanetparam print
```

### [Feature description]

The hanetparam command sets up the monitoring function.

### [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. 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 how many times 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 switching, specify the number of repeatedly monitoring within the range between 1-100 for monitoring Cluster switching. The default is set to 5 (switch the Cluster if failure was detected on the entire transfer routes). This option is only available for Cluster operation on Fast switching mode.

##### -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.

< Valid options in Virtual NIC mode >

-q value

Specify the standby time in seconds from when the link status monitoring function detects a failure of the link status (link down) in a physical interface to when the transfer path is switched. A value from 0 to 60 can be specified.

If the network links up again within the time specified by this parameter after a link down is detected, the transfer path is not switched.

Note that a failure may be detected by the network monitoring function.

The default value is 0 (second).

-r value

Specify the time in seconds from when the link status monitoring function detects a recovery of the link (link up) in a physical interface to when it can be used as a standby NIC. A value from 0 to 60 can be specified.

By using this parameter to check the time specified by this parameter and continuation of the link up status, usage of a transfer path in the unstable state is suppressed.

The default value is 1 (second).

-g value

Specify the standby time in seconds from when a virtual interface is activated to when the link status monitoring function is started. A value from 1 to 300 can be specified.

If the value of this parameter is shorter than the time to link up a physical interface, the secondary path may be used on activation of a virtual interface.

The default value is 5 (seconds).

< Valid options in all modes >

-h value

If the host name is set using the virtual IP address, physical IP address, or monitored IP address, the host name should be changed to an IP address to use GLS. This process may take a long time because the process is performed using the DNS server or the /etc/hosts file based on the OS setting (nsswitch.conf). Enabling this option allows you to immediately change the host name for GLS just by referencing the /etc/hosts file without depending on the OS setting.

## -e value

Periodically monitors the status of the GLS control daemon and the virtual driver, which enables the output of a message in the event of an error. Also, by enabling this option, monitoring is performed when GLS starts (when the system starts or "resethanet -s" is executed).

No(no monitoring) is set by default.

## print:

Outputs a list of settings.

The following shows the output format:

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
[Fast switching]
  Line monitor interval(w)           :5
  Line monitor message output (m)    :0
  Cluster failover (l)               :5
  Cluster failover in unnormality (c):OFF
  Line status message output (s)     :OFF

[NIC switching]
  Standby patrol interval(p)         :15
  Standby patrol message output(o)   :3

[Virtual NIC]
  LinkDown detection time (q)        :0
  LinkUp detection time (r)          :1
  Link monitor starting delay (g)    :5

[Common Setting]
  Hostname resolution by file(h)     :NO
  Self-checking function(e)         :NO
```

Display		Contents
Line monitor interval (w)		The setting for the transmission line monitoring interval.
Line monitor message output (m)		The monitoring retry count before message output when a line failure occurs.
Cluster failover (l)		The consecutive monitoring failure count before execution of cluster failover.
Cluster failover in unnormality (c)		Operation when an error occurred in all transfer routes at activating a userApplication.
Line status message output (s)	ON	A message is output.
	OFF	A message is not output.
Standby patrol interval (p)		The monitoring interval of the standby patrol.
Standby patrol message output (o)		The consecutive monitoring failure count before output of a message when a standby patrol failure occurs.
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.
LinkDown detection standby time (q)		Standby time for link down detection
LinkUp detection standby time (r)		Standby time for link up detection

Display		Contents
Link status watch starting delay time (g)		Standby time for startup of link status monitoring
Line status message output (s)	ON	A message is output.
	OFF	A message is not output.
Hostname resolution by file(h)	YES	Change the host name by using only the /etc/hosts file.
	NO	Change the host name based on the OS setting.
Self-checking function(e)	YES	Enable the self-checking function when GLS starts.
	NO	Do not enable the self-checking function when GLS starts.

## [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"), standby patrol function (operation mode "p" or "q"), and Virtual NIC mode (operation mode "v").
- The setting by this command is valid in the whole system. It is not possible to change in a unit of virtual interface.

## [Examples]

< Example of Fast switching mode >

### (1) Example of setting line failure monitoring 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
```

< Example of Virtual NIC mode >

**(1) Example of setting the standby time for link down detection**

The following shows an example of using this command to detect link down when the link down status continues for 3 seconds from occurrence of link down.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -q 3
```

**(2) Example of setting the standby time for link up detection**

The following shows an example of using this command to detect link up when the link up status continues for 5 seconds from occurrence of link up.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -r 5
```

**(3) Example of setting the standby time for startup of link status monitoring**

The following shows an example of using this command to prevent detecting link down at least 10 seconds from activation of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -g 10
```

< Example common to all modes >

**(1) Example of the setting for changing the host name**

The following shows an example of changing the host name by using only the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -h yes
```

### (2) Example of the setting for self-checking function

The following shows an example of changing self-checking function.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -e yes
```

### (3) 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	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
devparam	Displays monitoring destination information for each virtual interface	General user
	Creates/deletes monitoring destination information for each virtual interface	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 a monitor-to host name or IP address. Specify a monitor-to host name or IP address to "polladdress1" when activating a Primary interface. Specify a monitor-to host name or IP address to "polladdress2" when activating a Secondary interface. When Primary and Secondary interfaces monitor the same thing, or when a Secondary interface is not defined (a single case), omit "polladdress2". In NIC switching mode, specify a host name or an IP address of the connected HUB. It is also possible to set IPv4 or IPv6 addresses as an address form. When setting an IPv6 address, do not specify a prefix value. When specifying a host name, do not use the same name that exists in IPv4 and IPv6. If the same name exists, it is dealt with as an IPv6 host.

**-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 the copy command to create copy monitoring destination information on a virtual interface in NIC switching mode. 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
```



.....  
When the tagged VLAN interface is used, the "copy" command is used to set a synchronous switching in the virtual interface.  
.....

**-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
Polling Status      = OFF
    interval(idle) =  5( 60) sec
    times           =  5 times
    repair_time     =  5 sec
    link detection  = NO
FAILOVER Status     = YES
Name    HUB Poll Hostname
+-----+-----+-----+
sha0    OFF  hostA,192.168.10.10
```

Display		Contents
Polling Status		The current status of the monitoring function.
Polling Status	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
interval(idle)	interval	The monitoring interval in the stationary status.
	idle	In seconds the wait time that elapses after monitoring starts and before the HUB links up.
times		The monitoring count.
repair_time		The recovery monitoring interval in seconds.
link detection	YES	NIC switching is performed when the NIC link down is detected.
	NO	NIC switching is not performed even if the NIC link down is detected until ping monitoring fails.
FAILOVER Status		With or without cluster switching when an error occurred in all transfer routes.
FAILOVER Status	YES	Node switching is performed when the virtual interface is registered in the cluster resource.
	NO	No node switching is performed.
Name		The name of a virtual interface to be monitored.
HUB Poll		The HUB-to-HUB monitoring status.
HUB Poll	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
	---	The monitoring function is not used.
Hostname		The host name or IP address to be monitored, in the order of the primary and secondary monitoring destinations. In the example, "hostA" is the primary monitoring destination and "192.168.10.10" is the secondary monitoring destination.



#### (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. Specify a virtual interface whose monitoring destination information is currently defined.

**-p polladdress1[,polladdress2]**

Specify the host names or IP addresses of the monitoring destinations to be modified. In RIP mode, specify the host names or IP addresses of neighboring routers as the monitoring destinations. In NIC switching mode, specify the host names or IP addresses of the primary and secondary HUBs.

**-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. This parameter cannot be specified for the monitoring destination information in RIP mode.

on: Monitors communication between two HUBs.

off: Does not monitor communication between two HUBs.



#### Note

Changing the number of monitoring targets 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, use the on command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll on [-s sec] [-c times] [-b sec] [-f {yes |  
no}] [-p sec] [-l {yes | no}]
```

-s sec:

Specify the monitoring time in seconds. A value from 1 to 300 can be specified (note that the product of sec and time must be 300 or less). 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 time must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified.

-b sec:

When detected an error in HUB-to-HUB monitoring of NIC switching mode, specify an interval to monitor recovery. The range possible to set is zero to 300. If not specified this option, the values set the last time become valid. 5 (seconds) is set as the initial set value.

-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 when a takeover virtual interface is set for 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.



#### Note

Setting "no" restricts switching caused by an error occurred in transfer routes. This does not restrict node switching caused by other errors such as an activation failure for virtual interfaces.

-p sec:

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in NIC switching 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 the monitoring interval multiplied by the monitoring count, the system ignores the specified link-up time and adopts the time obtained by multiplying the monitoring interval by the monitoring count.

-l yes | no:

Specify the task to be performed when the link of a running NIC in NIC switching mode is down. If you do not specify this option, the previous value will be used. The default value is "no".

yes: NIC switching is immediately performed if HUB monitoring fails even once when the link of a running NIC is down.

no : NIC switching is not performed until HUB monitoring fails when the link of a running NIC is down.



#### Note

- In an environment where GLS is used on the host OS of the virtual machine function, 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 OS 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.
- Link down is detected just after a failure by ping with the HUB monitoring function is detected. As with the HUB monitoring function, monitoring is started after the waiting time for linkup specified by the -p option elapses.

## (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
```

## (8) devparam command

### Display

Use the "devparam" command to display the HUB monitoring parameters set for each virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam
[ Standard Polling Parameter ]
Polling Status      = ON
    interval(idle) = 5( 60) sec
    time           = 5 times
    repair_time    = 5 sec
    link detection  = NO
FAILOVER Status     = YES

[ Polling Parameter of each interface ]
Name  intvl idle time repara link Fover
+-----+-----+-----+-----+-----+-----+-----+
sha0   2    60    5    5    NO    NO
sha1   3    60    5    5    NO    YES
sha2   ---    ---    ---    ---    ---    ---
```

Display		Contents
[ Standard Polling Parameter ]		The current status of the monitoring function.
[ Polling Parameter of each interface ]		Common monitoring information. For information on each displayed item, see "(3) print command".
[ Polling Parameter of each interface ]		Monitoring information that has been set for each individual virtual interface. If no setting has been made, '-' is displayed. Common monitoring information is used.
Name		The name of a virtual interface to be monitored.
intvl		The monitoring interval in the stationary status.
idle		In seconds the wait time that elapses after monitoring starts and before the HUB links up.
time		The monitoring count.
repara		The recovery monitoring interval in seconds.
link	YES	NIC switching is performed when the NIC link down is detected.
	NO	NIC switching is not performed even if the NIC link down is detected until ping monitoring fails.
Fover	YES	Node switching is performed when the virtual interface is registered in the cluster resource.
	NO	No node switching is performed.

## Settings

To set the HUB monitoring parameters for each individual virtual interface, specify the virtual interface name by using the "-n" option, and then the desired monitoring parameters by using options such as "-s". The parameters you do not specify will be set to common monitoring defaults. If NICs are shared, the settings of virtual interface parameter that you made first will be used. To enable the settings, restart monitoring (execute the "hanetpoll off" command and then the "hanetpoll on" command).

```
/opt/FJSVhanet/usr/sbin/hanetpoll devparam -n devicename [-s sec] [-c times]
[-b sec] [-f {yes | no}] [-p sec] [-l {yes | no}]
```

### -n devicename:

Specify the virtual interface name for which individual monitoring parameters are to be set.

### -s sec:

Specify the monitoring time in seconds. For details about this option, see '(6) on command'.

### -c times:

Specify the monitoring count. For details about this option, see '(6) on command'.

### -b sec:

When detected an error in HUB-to-HUB monitoring of NIC switching mode, specify an interval to monitor recovery. For details about this option, see '(6) on command'.

### -f yes | no:

Specify the operation used when node switching occurs due to a line failure during cluster operation. For details about this option, see '(6) on command'.

### -p sec:

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in NIC switching mode. For details about this option, see '(6) on command'.

### -l yes | no:

Specify the task to be performed when the link of a running NIC in NIC switching mode is down. For details about this option, see '(6) on command'.

## Deleting

To delete the HUB monitoring parameters that have been set for each virtual interface, specify the virtual interface name with the "-n" option and specify the "-d" option.

```
/opt/FJSVhanet/usr/sbin/hanetpoll devparam -n devicename -d
```

### -n devicename:

Specify the virtual interface name for which individual monitoring parameters are to be set.

-d:

Delete the individual parameter settings of the specified virtual interface.

## [Notes]

- Be sure to specify address information for neighboring hubs (hubs in the subnet to which physical interfaces bundled by the specified virtual interface belong) as the hub monitoring destination. If any other address information is specified, the HUB monitoring function may not operate properly.
- 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").
- After modifying monitoring destination information, disable the HUB monitoring function (hanetpoll off) and then enable it again (hanetpoll on). If the HUB monitoring function is enabled while it has already been enabled (duplicated activation of hanetpoll on), no monitoring destination information is reflected after modification.
- 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.
- If a virtual interface to be monitored is set to Fast switching mode, an error message is output to indicate this fact and the line 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 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/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, not a create command, for setting the second and after. If used a create command, occasionally the state is not displayed properly by a dspoll command.
- 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/hosts file. 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/hosts 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 reconfigure.
- Do not specify a multicast address as a monitor-to address.
- 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/hosts 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/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 hubs hubA and hubB to hubA and hubC on virtual interface sha2. The host name is assumed to be associated with the virtual IP address in the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha2 -p hubA,hubC
```

## (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
```

## (7) off command

The following shows an example of stopping the HUB monitoring function.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll off
```

## (8) devparam command

The following shows an example of setting monitoring parameters for each virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam -n sha0 -s 2
```

## 7.8 dsppoll Command

### [Name]

dsppoll - Displaying the monitoring status

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/dsppoll
```

### [Feature description]

The dsppoll command displays the current monitoring status of monitoring information created using the hanetpoll command.

### [Display format]

The following shows the display format used when no option is specified.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = OFF
    interval(idle) =  5( 60) sec
    times           =  5 times
    repair_time     =  5 sec
    link detection  = NO
FAILOVER Status     = YES
Name   HUB Poll Hostname
+-----+-----+-----+-----+-----+-----+
sha0    OFF  hostA,192.168.10.10
```

Display		Contents
Polling Status	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
interval (idle)	interval	In seconds the monitoring interval in the stationary status.
	(idle)	In seconds the wait time that elapses after monitoring starts and before the HUB links up.
times		The monitoring count.
repair_time		The recovery monitoring interval in seconds.
link detection	YES	The link detection function is enabled.
	NO	The link detection function is disabled.
FAILOVER Status	YES	Node switching is performed when the virtual interface is registered in the cluster resource.
	NO	No node switching is performed.
Status	ON	Monitoring is in progress.
	OFF	Monitoring is stopped.
Name		: 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/ Secondary Target		Monitoring status in Primary/Secondary monitor-to IP address or a host name and parenthesis.

Display		Contents
	(ON)	Monitoring is in progress.
	(WAIT)	Waiting is in progress.
	(FAIL)	Monitoring failed (monitoring is stopped).
	(STOP)	Unused.
HUB-HUB	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.

#### [Related commands]

hanetpoll

#### [Notes]

If no option is specified, this command can be specified for a virtual interface in NIC switching mode (operation mode "d" or "e").

#### [Examples]

The following shows an example of displaying all the monitoring statuses properly defined using the hanetpoll command.

```
# /opt/FJSVhanet/usr/sbin/dspoll
```

## 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.



## (1) add command

This command adds physical interfaces bundled by a virtual interface in Fast switching mode, Virtual NIC mode, or GS linkage mode dynamically. (Real interfaces are added while the virtual interface is active.) However, only physical interfaces specified in configuration information can be specified. 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, Virtual NIC mode, or GS linkage mode 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)".

### -f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic addition.)

Note that this option cannot be configured when operating in GS linkage mode.

## (2) delete command

This command deletes physical interfaces bundled by a virtual interface in Fast switching mode, Virtual NIC mode, or GS linkage mode dynamically (Real interfaces are deleted while the virtual interface is active). However, only physical interfaces specified in configuration information can be specified. The following is the format of the delete command. When a virtual interface bundles only one physical interface, this command cannot be executed.

```
/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, Virtual NIC mode, or and GS linkage mode.

### -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.

### -f:

Specifies when changes the configuration information of a virtual interface at the same time. (Permanent dynamic deletion.)

Note that this option cannot be configured when operating in GS linkage mode.

### (3) change command

This command switches physical interfaces used in a virtual interface in NIC switching mode or Virtual NIC mode to those of the standby system. The following is the format of the change command. If there is no standby interface, which means that an interface is temporarily cut off by the "delete" command or it is linked down, this command cannot be executed.

#### NIC switching mode:

```
/opt/FJSVhanet/usr/sbin/hanetnic change -n devicename
```

#### Virtual NIC mode:

```
/opt/FJSVhanet/usr/sbin/hanetnic change -n devicename -i interface
```

#### -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") or Virtual NIC mode (operation mode "v") specified.

#### -i interface

Specify the physical interface name of the communication destination. Only Virtual NIC mode can be specified for the operation mode of the virtual interface.

### [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/sysconfig/network-scripts/ifcfg-ethX file. If not, create it. Then execute "/sbin/ifup ethX " command, and activate the interface.)
- In GS linkage mode, only temporary dynamic addition/deletion is possible.
- If you want to execute this command for a virtual interface of NIC switching mode on the host OS of virtual machine function repeatedly, wait at least 1 minute.
- You can check whether there are physical interfaces in the OFF state by using the "dsphanet" command for physical interfaces in the standby state.
- You cannot execute the "hanetnic change" command when virtual interfaces are in the inactive state.
- To dynamically add or delete physical interfaces used by virtual interfaces in Virtual NIC mode by using this command with "-f" option, change monitoring destinations according to the connection status between physical interfaces and switch/HUB.

### [Examples]

#### (1) add command

The following example adds eth0 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"), Virtual NIC mode (operation mode "v"), or GS linkage mode (operation mode "c"), and eth0 has been deleted by using the "hanetnic delete" command.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n sha0 -i eth0
```

#### (2) delete command

The following example deletes eth1 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"), Virtual NIC mode (operation mode "v"), or GS linkage mode (operation mode "c").

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n sha0 -i eth1
```

### (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
```

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 Virtual NIC mode (operation mode "v"). In addition, the standby physical interface is defined as eth2.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n sha0 -i eth2
```

## 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]

stpptl

### [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/FJSVhanet/usr/sbin/strptl -n sha4
```

## 7.11 stpptl Command

---

### [Name]

stpctl - Stopping the standby patrol

### [Synopsis]

```
/opt/FJSVhanet/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]

strctl

### [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/FJSVhanet/usr/sbin/stpctl -n sha4
```

## 7.12 hanetpathmon Command

---

### [Name]

hanetpathmon - Enabling and disabling the network monitoring function, modifying and displaying the monitoring destination information, modifying monitoring parameters, and starting and stopping monitoring

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetpathmon command [args]
```

### [Feature description]

The hanetpathmon command serves to enable and disable the network monitoring function, to modify and display monitoring destination information, to modify monitoring parameters, and to start and stop network monitoring.

Command	Process outline	Authority
target	Changes and displays monitoring destination information.	Change: Super user Display: General user
param	Changes and displays monitoring parameters.	Change: Super user Display: General user
on	Starts network monitoring.	Super user

Command	Process outline	Authority
off	Stops network monitoring.	Super user

## (1) target command

Use the target command to modify or display the setting of monitoring destination. The following is the format of the target command.

```
Setting:
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n devicename [-v vlanid] [-p
ipaddress1[,ipaddress2]]
Displaying:
/opt/FJSVhanet/usr/sbin/hanetpathmon target [-n devicename]
Deleting:
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n devicename -d
```

### Setting

**-n devicename**

Specify the names of virtual interfaces whose monitoring destination information should be set.

**-v vlanid**

Specify the VLAN ID of a VLAN interface when the monitoring destination is the network of a tagged VLAN. When this parameter is not specified, the network without tag is monitored.

**-p ipaddress1[,ipaddress2]**

Specify a monitor-to host name or IP address. Specify a monitor-to host name or IP address to "ipaddress1" when activating a Primary interface. Specify a monitor-to host name or IP address to "ipaddress2" when activating a Secondary interface. When Primary and Secondary interfaces monitor the same thing, or when a Secondary interface is not defined (a single case), omit "ipaddress2".

In Virtual NIC mode, specify an IP address of the connected HUB. It is also possible to set IPv4 or IPv6 addresses as an address form. When specifying an IPv6 address, do not specify a prefix value.

Without specifying these parameters, HUB monitoring will not work. Only the standby patrol function will be enabled.



### Note

To specify an IPv4 address for the target IP of HUB monitoring, specify the same network address as IPv4 set in the setting file for a virtual interface or the setting file of a tagged VLAN for a virtual interface.

### Deleting

**-n devicename**

Specify the names of virtual interfaces whose monitoring destination information should be deleted.

**-d**

Specify this option to delete the monitoring destination IP and VLAN ID, and to initialize the monitoring destination information.

### Displaying

**-n devicename**

Specify each name of a virtual interface whose monitoring destination information should be displayed. When this parameter is omitted, all monitoring destination information currently set is displayed.

```
# /opt/FJSSVhanet/usr/sbin/hanetpathmon target
[Target List]
Name      VID      Target
+-----+-----+-----+
sha0      -        192.13.90.251,192.13.90.252
sha1      -        192.13.100.251
sha2      6        -
```

Display	Contents
Name	<p>Virtual interface name</p> <p>When monitoring a tagged VLAN interface, the name of the virtual interface from which the tagged VLAN interface is originally generated is displayed.</p>
VID	<p>When monitoring a virtual interface, a hyphen ("-") is displayed.</p> <p>When monitoring a tagged VLAN interface, the tag ID is displayed.</p>
Target	<p>Target IP addresses in HUB monitoring are displayed in the order of primary and secondary monitoring targets.</p> <p>If no monitoring target is specified, a hyphen ("-") is displayed.</p>



### Note

When network monitoring is started, you cannot change the settings of monitoring destination information. Stop network monitoring before executing this command.

## (2) param command

Use the `param` command to modify the settings of monitoring parameters.

```
Setting:
/opt/FJSVhanet/usr/sbin/hanetpathmon param -n devicename [-a {yes | no}] [-s sec] [-c times]
[-r times] [-p sec] [-q {yes | no}] [-f {yes | no}]
Displaying:
/opt/FJSVhanet/usr/sbin/hanetpathmon param [-n devicename]
```

## Setting

**-n devicename**

Specify the name of the virtual interface for which the monitoring parameters are to be modified.

-a yes/no

Set whether or not to start the network monitoring function in conjunction with startup of the virtual interface. If you do not specify this option, the previous value will be used. The default value is "yes".

yes: Network monitoring starts in conjunction with startup of the virtual interface.

no : Network monitoring does not start in conjunction with startup of the virtual interface.

#### **-s sec**

Specify the monitoring interval in seconds. The values which can be specified are from 1 to 300. If you do not specify this option, the previous value will be used. The default value is 3 (seconds).

#### **-c times**

Specify the monitoring count. The values which can be specified are from 1 to 300. If you do not specify this option, the previous value will be used. The default value is 5 (times).

#### **-r times**

Specify the number of succeed counts to go back to the normal monitoring after recovery of a monitoring target is detected in the recovery monitoring by the standby patrol of the network monitoring function. The values which can be specified are from 1 to 300. If you do not specify this option, the previous value will be used. The default value is 2 (times). (The monitoring target is considered as recovered if the standby patrol succeeds twice.)

#### **-p sec**

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in network monitoring. The values which can be specified are from 1 to 300. If you do not specify this option, the previous value will be used. The default value is 45 (seconds). If the value is less than the product of monitoring period and monitoring times (monitoring period X monitoring times), then the value is ignored and ends up using the value of the product of monitoring period and monitoring times.

#### **-q yes | no**

Specify whether to perform the automatic fail-back when recovery of transfer paths between active NICs and standby NICs is detected by using the standby patrol function. The default value is "no".

yes: Performs the automatic fail-back.

no : Does not perform the automatic fail-back.

#### **-f yes | no**

Specify the operation used when node switching occurs due to a line failure during cluster operation. If you do not specify this option, the previous value will be used. The default value is "yes". This parameter is valid only in 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.

### **Displaying**

#### **-n devicename**

Specify each name of a virtual interface whose monitoring parameter information should be displayed. When this parameter is omitted, all monitoring parameter information currently set is displayed.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon param
[Parameter List]
Name      Monitoring Parameter
+-----+-----+
sha0      auto_startup      =      YES
          interval        =      3 sec
          times            =      5 times
          repair_times     =      2 times
          idle             =      45 sec
          Auto fail-back   =      NO
          FAILOVER Status  =      YES
```





#### (4) off command

Use the off command to stop network monitoring. Execute this command for every virtual interface.

Normally, network monitoring is stopped along with the inactivation of a virtual interface, but this command is used to suspend the network when changing monitoring destination information by the target command or changing monitoring parameters by the param command.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon off [-n devicename]
```

-n devicename

Specify the names of virtual interfaces (such as sha0 and sha1) for which network monitoring is to be stopped. When this parameter is omitted, monitoring all virtual interfaces for which monitoring is enabled is stopped.

#### [Examples]

##### (1) target command

The following shows an example of setting IP addresses "192.13.90.251" and "192.13.90.252", which are monitoring destinations for the virtual interface sha0, as monitoring targets.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.13.90.251,192.13.90.252
```

The following shows an example of setting IP address "192.13.90.251", which is the monitoring destination for the virtual interface sha0, as monitoring target.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.13.90.251
```

The following shows an example of setting IP addresses "192.13.80.251" and "192.13.80.252", which are monitoring destinations for the virtual interface of the tagged VLAN interface sha0.2, as monitoring targets.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.13.80.251,192.13.80.252 -v 2
```

The following shows an example of initializing the monitoring destination information of the virtual interface sha0.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -d
```

##### (2) param command

The following shows an example when the monitoring interval is set to 10 seconds and when switching between nodes is not performed in the event of transfer path failure in cluster operation.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon param -n sha0 -s 10 -f no
```

##### (3) on command

The following shows an example of starting monitoring for all virtual interfaces.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon on
```

##### (4) off command

The following shows an example of stopping monitoring for all virtual interfaces.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon off
```

## 7.13 dsppathmon Command

### [Name]

dsppathmon - Displaying the monitoring status of the network monitoring function

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/dsppathmon
```

### [Feature description]

The dsppathmon command displays the current monitoring status of monitoring information created using the hanetpathmon command.

### [Display format]

The following shows the display format of the monitoring status.

```
# /opt/FJSVhanet/usr/sbin/dsppathmon

Status Name      VLAN Primary Target/Secondary Target      Patrol
+-----+-----+-----+-----+-----+
  OFF  sha1    u/t   192.168.100.15(STOP)                STOP
  ON   sha3    u/t   192.168.120.30(ON)/192.168.120.31(CUT)  STOP
  ON   sha4    u/t   ----/----                    ACTIVE
```

For IPv6 address

```
# /opt/FJSVhanet/usr/sbin/dsppathmon

Status Name      VLAN Primary Target/Secondary Target      Patrol
+-----+-----+-----+-----+-----+
  ON   sha1    u/t   fec0:1::100(ON)/fec0:1::101(WAIT)  ACTIVE
```

Display		Contents
Status	OFF	The monitoring function is stopped.
	ON	The monitoring function is running.
Name	shaX	Virtual interface name This name can be identified in the definition and will be displayed in the definition in the same way even after renaming the virtual interface.
VLAN		Items of "u/t" are displayed.
Primary Target	Displays the IP address or host name of the primary monitoring destination. Displays the status of the primary monitoring destination in parenthesis.	
	ON	Displayed when HUB monitoring is normal.
	WAIT	Displayed when HUB monitoring is waiting to be executed.
	FAIL	Displayed when an error has been detected in HUB monitoring but not yet recovered.
	STOP	Displayed when HUB monitoring is suspended.
	CUT	Displayed when the NIC has been disconnected. This is displayed after a temporary disconnection by the "hanetnic delete" command.

Display	Contents	
	----	Displayed when HUB monitoring is not running.
Secondary Target	Displays the IP address or host name of the secondary monitoring destination. Displays the status of the secondary monitoring destination in parenthesis.	
	ON	Displayed when HUB monitoring is normal.
	WAIT	Displayed when HUB monitoring is waiting to be executed.
	FAIL	Displayed when an error has been detected in HUB monitoring but not yet recovered.
	STOP	Displayed when HUB monitoring is suspended.
	CUT	Displayed when the NIC has been disconnected.  This is displayed after a temporary disconnection by the "hanetnic delete" command.
	----	Displayed when HUB monitoring is not running.
Patrol	Displays the monitoring status by the standby patrol.	
	ACTIVE	Displayed when standby patrol is normal.
	FAIL	Displayed when standby patrol is detecting an error.
	STOP	Displayed when standby patrol is suspended.

## 7.14 hanetgw Command

### [Name]

hanetgw - Setting, deleting, and displaying a virtual gateway configuration definition of GS linkage mode.

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/hanetgw command [args]
```

### [Feature description]

The hanetgw command sets/deletes/displays the virtual gateway required for operating in GS linkage mode.

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 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 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 devicename:

Specify the name of the virtual interface whose information you want to delete.

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.

## [Related commands]

hanetconfig  
hanetobserv

## [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 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 linkage mode.
- To enable the virtual gateway function, the host route to the virtual IP address of the communication target must be registered in the routing table. When you use GS linkage mode, be sure to add the route information in the /etc/sysconfig/network-scripts/route-"interface name" file.

## [Examples]

Shown below is an example of setting the virtual gateway information.

```
# /opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.70.254
```

Shown below is an example of deleting the virtual gateway information.

```
# /opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0
```

## 7.15 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 linkage mode.

Command	Process outline	Authority
create	Sets a monitoring destination information	Super user
delete	Deletes monitoring destination information	Super user
print	Displays monitoring destination information	General user
param	Modifies the monitoring destination information.	Super user

### (1) create command

The operation in GS 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
/opt/FJSVhanet/usr/sbin/hanetobserv create -n node -i ipaddress -t
nicaddress1[,nicaddress2,...]
```

**-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. Up to 128 can be set. This host name must correspond to an IP address in a network database such as the /etc/hosts 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 [routeraddress1+]nicaddress1[, [routeraddress2+]nicaddress2,...]:

For setting a communication target

Specify the IP addresses of physical interfaces bundled by a virtual interface held by the communication target, using a comma (",") to separate those IP addresses. Up to 32 IP addresses can be set.

In addition, if you perform remote network communication via router to connect to the communication target, specify the IP addresses in the format of "IP address of a neighboring router + IP address of a physical interface."

For setting the destination cluster node

Specify the IP addresses of physical interfaces bundled by a virtual interface of a destination cluster node and the IP addresses of neighboring switches, using a comma (",") to separate those IP addresses.

Note that, you can also specify the switches with the host names instead of IP addresses.

nicaddressX:

Specify the host name or IP address of a physical interface bundled by a virtual interface.

routeraddress:

Specify the IP address or host name of the router for the local system. This option can be omitted if you do not perform remote network communication via router to connect to GS.

## (2) delete command

The following is the format of the delete command used to delete the monitoring destination information created using the create command:

```
To delete all the monitoring destination information:
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n all

To delete the monitoring destination information by specifying the name of
the monitoring destination node:
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n node1[,node2,...]

To delete the monitoring destination information by specifying the virtual
IP address of the monitoring destination:
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n node -i
ipaddress1[,ipaddress2,...]

To delete the monitoring destination information by specifying the
physical IP address and router IP address of the monitoring destination:
/opt/FJSVhanet/usr/sbin/hanetobserv delete -n node -i ipaddress -t
[routeraddress1+]nicaddress1[, [routeraddress2+]nicaddress2]
```

-n all | node1[,node2,...]:

Specify the name of the remote host. You can specify more than one name by delimiting them with a comma.

all:

If all is specified, all monitoring destination information is deleted.

node1[, node2, ...]:

Specify a remote node name that is set in the monitoring destination information and should be deleted. You can specify more than one remote node name by listing them delimited with a comma.

**-i ipaddress1[,ipaddress2,...]:**

Specify the name of the remote host you want to delete that is set in the monitoring destination information.

**ipaddress:**

Specify the virtual IP address or host name of the virtual interface on the remote host. The definition information of the remote host is also deleted if only one virtual interface is defined on the remote host.

**-t [routeraddress1+]nicaddress1[, [routeraddress2+]nicaddress2,...]:**

Specify the IP addresses or host names to be deleted. You can use the print command of hanetobserv to confirm the combination of the IP addresses or host names to be deleted.

**nicaddressX:**

Specify the IP addresses or host names of the physical interfaces assigned to the virtual interface.

**routeraddressX:**

Specify the IP address or host name of the router for the local system.

### (3) 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
```

The following shows an example of displaying monitoring destination information:

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
repair_retry(r)  = 0 times
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+-----+
hostA          192.168.91.1          192.168.70.254+192.168.80.2,
                                     192.168.71.254+192.168.81.2
hostB          ipaddress3           ipaddress4,ipaddress5
```

Item		Explanation
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.
repair_time		Displays the recovery monitoring interval in seconds.
repair_retry		Displays the retry count of the recovery monitoring.
fail over mode	YES	If the virtual interface is registered in the cluster resource, node switching is performed when all the transfer routes fail. (default)

Item		Explanation
	NO	If the virtual interface is registered in the cluster resource, node switching is not performed when all the transfer routes fail.
Destination Host		Outputs the host name of the communication target.
Virtual Address		Displays the host name or IP address set for the virtual interface of the communication target.
(Router addr+)NIC Address		Displays the host name or IP address of the physical interfaces assigned to the virtual interface of the communication target, and the host name or IP address of a local router.

#### (4) param command

Use this command to modify each parameter value for the remote host monitoring function. The command format is as follows.

```
/opt/FJSVhanet/usr/sbin/hanetobserv param [-s sec] [-c times] [-p sec]
[-b sec] [-r times] [-f {yes | no}]
```

##### -s sec:

Specify the monitoring time in seconds. A value from 1 to 300 can be specified (note that the product of sec and time must be 300 or less). 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 time must be 300 or less). If this option is not specified, the previous setting is enabled. Initially, 5 (times) is specified.

##### -p sec:

Specify in seconds the wait time that should elapse after monitoring starts and before the HUB links up in GS 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 the monitoring interval multiplied by the monitoring count, the system ignores the specified link-up time and adopts the time obtained by multiplying the monitoring interval by the monitoring count.

##### -b sec:

When detected an error in communication target monitoring, specify an interval to monitor recovery. The range possible to set is zero to 300. If not specified this option, the values set the last time become valid. 5 (seconds) is set as the initial set value.

##### -r times

Specify the retry count to return to the regular monitoring if recovery monitoring has been consecutively successful after detecting an error in recovery monitoring by remote host monitoring. A value from 0 to 300 can be specified. The default value is 0 (times). (The monitoring target is considered as recovered if the ping monitoring succeeds once and no retry occurs.)

##### -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 when a takeover virtual interface is set for 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.





- Setting "no" restricts switching caused by an error occurred in transfer routes. This does not restrict node switching caused by other errors such as an activation failure for virtual interfaces.
- If the cluster application is switched when all the transfer paths for the virtual interface are failed, resources will fail even if "no" is set.
- To use "no" for maintenance purpose of nodes in the cluster, see "[G.6.5 Maintenance procedure performed when the communication target stopped](#)" and perform the procedure.

## [Notes]

- To change the monitoring destination, delete it first, and then re-create it.
- To add, delete, or change a monitoring destination, the virtual interface in GS linkage mode (operation mode "c") must be inactivated.
- An IP address or host name to be specified when the communication target monitoring function is set or changed must be defined in /etc/hosts.
- 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/hosts 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/hosts 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 host hahostA has virtual IP address "vip1", which bundles two physical IP addresses ipaddress1 and ipaddress2. The host name is assumed to be associated with the IP address in the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip1 -t  
ipaddress1,ipaddress2
```

The following shows a setting example in which monitoring is performed while the monitoring information for the virtual IP address "vip1" of the communication target host hahostA is specified and then the two physical IP addresses ipaddress3, and ipaddress4 for the virtual IP address vip1 are added. The host name is assumed to be associated with the IP address in the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip1 -t  
ipaddress3,ipaddress4
```

The following example shows the settings in which there exist routers rt1 and rt2 for the local system, there exists the virtual IP address "vip1" on the communication target host hahostA, and the "vip1" is assigned to the physical IP addresses ipaddress1 and ipaddress2. The host name is assumed to be associated with the IP address in the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n hahostA -i vip1 -t  
rt1+ipaddress1,rt2+ipaddress2
```

The following is an example for setting destination cluster node monitoring information and switches monitoring information.

It shows when the destination node name is cl\_node, a take-over IP address is cl\_vip, the physical IP addresses of the destination node are cl\_ipaddress1 and cl\_ipaddress2, and the IP addresses of neighboring switches are sw1 and sw2. The host name is assumed to be associated with the IP address in the /etc/hosts file.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n cl_node -i cl_vip -t  
cl_ipaddress1,cl_ipaddress2,sw1,sw2
```

## (2) 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 physical IP addresses (ipaddress1, ipaddress2) under the virtual IP address "vip1".

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -i vip1 -t  
ipaddress1,ipaddress2
```

The following shows an example of specifying and deleting the physical IP and router information in the virtual IP address "vip1" that the monitoring destination remote host hahostA has.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n hahostA -i vip1 -t  
rt1+ipaddress1,rt2+ipaddress2
```

## (3) print command

The following shows an example of displaying the configuration information list of a virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
```

## (4) param command

The following shows an example of setting the monitoring interval and monitoring count for the remote host monitoring function to 3 seconds and 2 times respectively.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv param -s 3 -c 2
```

The following shows an example of setting the remote host monitoring function to perform node switching when all the transfer routes fail. (when you set the node switching task to default)

```
# /opt/FJSVhanet/usr/sbin/hanetobserv param -f yes
```

## 7.16 dspobserv Command

---

### [Name]

dsphanet - Displaying the operation status of communication target monitoring

### [Synopsis]

```
/opt/FJSVhanet/usr/sbin/dspobserv [-d]
```

### [Feature description]

The dspobserv command displays the current operation status of communication target monitoring.

### [Option]

You can specify the following option.

#### [-d]

An asterisk (\*) is displayed at the end of a physical IP address of the active node that GLS recognizes as a communication target.

### [Display format]

The following shows the display formats of monitoring status:

- The option is not specified:

```
# /opt/FJSVhanet/usr/sbin/dspobserv
observ status      = ON
interval          = 5 sec
times             = 5 times
idle              = 60 sec
repair_time       = 5 sec
fail over mode    = YES

  Node          VIP          NIC          Status
+-----+-----+-----+-----+
host1          192.168.100.10  192.168.10.10  ACTIVE
                                   192.168.20.10  ACTIVE
                                   192.168.10.20  ACTIVE
                                   192.168.20.20  ACTIVE
```

- The option is specified:

```
# /opt/FJSVhanet/usr/sbin/dspobserv -d
observ status      = ON
interval          = 5 sec
times             = 5 times
idle              = 60 sec
repair_time       = 5 sec
fail over mode    = YES

  Node          VIP          NIC          Status
+-----+-----+-----+-----+
host1          192.168.100.10  192.168.10.10*  ACTIVE
                                   192.168.20.10*  ACTIVE
                                   192.168.10.20  ACTIVE
                                   192.168.20.20  ACTIVE
```

Display		Contents
observ status	ON	The monitoring function is enabled.
	OFF	The monitoring function is disabled.
interval		In seconds the monitoring interval in the stationary status.
times		The monitoring count.
idle		Displays in seconds the wait time that elapses after monitoring starts and before the HUB links up.
repair_time		Displays the recovery monitoring interval in seconds.
fail over mode	YES	If the virtual interface is registered in the cluster resource, node switching is performed when all the transfer routes fail. (default)
	NO	If the virtual interface is registered in the cluster resource, node switching is not performed when all the transfer routes fail.
VIP		Displays the name of a virtual interface held by the monitored node.
NIC		Displays the hostname or IP address of a real interface to be monitored. When the -d option is specified, an asterisk (*) is displayed at the end of the physical IP address of the active node in a communication target.
Status	Active	Monitoring is in progress.
	FAIL	Monitoring failed (recover monitoring in progress).
	----	The monitoring function is disabled.

#### [Related commands]

hanetobserv

#### [Examples]

The following shows an example of displaying the status of communication target monitoring in GS linkage mode.

```
# /opt/FJSVhanet/usr/sbin/dspobserv
```

## 7.17 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 takeover virtual interface and a takeover IP address. It is possible to create up to 64 takeover virtual interfaces. A logical number of a takeover virtual interface (a number to add after ":") is automatically numbered from 65.

- When creating the information of a virtual interface:

```
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
Virtual NIC mode:
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename [-i {takeover-
ipv4 | takeover-ipv6/prefix | takeover-ipv4,takeover-ipv6/prefix}] [-v
vlan_id]
GS linkage mode
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n devicename [-e
nicaddress1[,nicaddress2,...]]
```

### -n devicename:

Specify a name of the virtual interface for Fast switching, NIC switching mode, Virtual NIC mode, and GS linkage mode created with hanetconfig command.

A multiple takeover IP can be applied to a single virtual interface name for Fast switching mode or Virtual NIC mode.

For NIC switching mode and GS linkage mode, one takeover IP can be applied against one virtual interface name.



### Note

When the virtual interface of the Virtual NIC mode is registered in the cluster resource, it is activated regardless of ONBOOT setting in the setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) of the virtual interface.

### -i takeover-ipv4[,takeover-ipv6/prefix]:

Specify a host name or an IP address of a takeover IP.

Specify this option when a virtual interface to specify by -n option is Fast switching mode and Virtual NIC mode.

In Virtual NIC mode, when you do not need to take over a virtual IP address between clusters, specifying the -i option is unnecessary.

In addition, when you set a takeover IP address for a tagged VLAN interface (shaX.Y) in Virtual NIC mode, specify the takeover IP address with the -i option and VLAN ID (Y) with the -v option. This option is not necessary for NIC switching mode or GS linkage mode. In NIC switching mode and GS linkage mode, a value specified by -i option of hanetconfig create command is automatically set as a takeover IP.



### Note

- When you specify a takeover IP address with the -i option in Virtual NIC mode, set a subnet mask by using the hanetmask command in advance. For example, when specifying the IP address "192.168.1.1", set the subnet mask for "192.168.1.0."  
For details on the hanetmask command, see "[7.5 hanetmask Command](#)."  
Ensure that the subnet mask specified with the hanetmask command is the same subnet mask described in the setting file of the virtual interface (ifcfg-shaX).
- For the configuration that a virtual bridge has been connected to the virtual interface, the takeover IP address is set to the virtual bridge.

-v vlan\_id

Specify the VLAN ID of a tagged VLAN interface for Virtual NIC mode.

In Virtual NIC mode, specify VLAN ID (Y) by -v option when you register a tagged VLAN interface (shaX.Y) for Virtual NIC mode to a cluster resource.



### Note

In Virtual NIC mode, if you register a tagged VLAN interface for Virtual NIC mode to a cluster resource, you need to configure the setting file (/etc/sysconfig/network-scripts/ifcfg-shaX.Y) for a tagged VLAN interface for Virtual NIC mode beforehand.

-e nicaddress1[,nicaddress2,...]:

Specify the host name or IP address to be used as the gateway address for the takeover virtual interface in GS linkage mode. This host name or IP address is assigned as the logical interface to the physical interface that you make redundant. The specification of the host name or IP address is possible only in GS linkage mode. Be sure to specify the host names or IP addresses corresponding to the number of physical interfaces that the takeover virtual interface in GS linkage mode bundles.



### Point

You need to set the IP address to be configured by using the '-e' option under the following condition.

Communication type	Adapter type used by GS	
	LANC, ONA	LANC2, LR
Same network communication (local)	No setting required.	Setting required.
Remote network communication (remote)	Setting required.	Setting required.

You need to set the IP address by using the '-e' option when routers (including LANC2) are connected between the local nodes and GS host. In addition, if you specified the IP address with the '-e' option, you need to set the IP address specified with the '-e' option as the gateway to the local node's virtual IP address to the static route information for the routers for the local node.



### Note

When you specify the IP address with the '-e' option, set the subnet mask beforehand with the hanetmask command. For example, when you specify the IP addresses "192.168.70.12" and "192.168.71.12" by using the '-e' option, set the subnet masks for "192.168.70.0" and "192.168.71.0". For details on the hanetmask command, see "7.5 hanetmask Command".

## (2) delete command

Deletes the information of a virtual interface from the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n devicename
```

-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.



The virtual interface name specified by the "delete" command is the name which is assigned by the virtual interface name specified by the "create" command at the timing of setting.

### (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
```

An example of a display is as follows:

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4    takeover-ipv6    vlan-id/logical ip address list
+-----+-----+-----+-----+
sha0:65     takeovertip1        -                -
sha1:65     -                  takeovertip2/64  -
sha2:65     192.168.50.1       fec0:1::123/64   -
sha3:65     192.168.80.1       -                192.168.70.12,192.168.71.12
sha4:65     sha0-65            -                -
sha4:66     192.168.11.10      -                -
sha4:67     -                  fec0:1::69/64    5
```

Display	Contents
ifname	A name of a logical virtual interface to register in the cluster resources.
takeover-ipv4	A host name or an IP address of a takeover IP (IPv4) to add to a logical virtual interface.
takeover-ipv6	A host name or an IP address of a takeover IP (IPv6) to add to a logical virtual interface.
logical ip address list	A host name or an IP address of a logical IP (IPv4) to be added to a physical interface used as a gateway address for a takeover virtual interface.
vlan-id/logical ip address list	In Virtual NIC mode, VLAN ID of a tagged VLAN interface to which a takeover IP is set or a hyphen is displayed.
'-'(hyphen)	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/hosts file. 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 register 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 takeover 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 takeover 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 takeover IP address (10.1.1.1) and IPv6 takeover 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 using create command when setting Virtual NIC mode:

An example of using create command when registering a virtual interface sha0 with adding a takeover IP address (10.1.1.1) of IPv4 in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 10.1.1.1
```

An example of using create command when setting Virtual NIC mode:

An example of using create command when registering a virtual interface sha0 without a takeover IP address in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

An example of using create command when setting Virtual NIC mode:

An example of using create command when registering a virtual interface sha0 with adding a takeover IP address (fec0:1::69/64) of IPv6 to a tagged VLAN interface sha0.5 on a virtual interface sha0 in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::69/64  
-v 5
```

An example of using create command when setting GS linkage mode:

An example of using create command when registering a virtual interface sha2 in the cluster resources.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha2 -e  
192.168.70.12,192.168.71.12
```

## (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
```



## 7.18 hanetbackup Command

---

### [Name]

hanetbackup - Backing up the environment definition files

### [Synopsis]

```
/opt/FJSVhanet/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/FJSVhanet/usr/sbin/hanetbackup
```

## 7.19 hanetrestore Command

---

### [Name]

hanetrestore - Restoring the environment definition files

### [Synopsis]

```
/opt/FJSVhanet/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 "[7.20 resethanet Command](#)" for the detail of a resethanet command.
- Recovery can be made exclusively on the same system configuration where the configuration file is backed up.

### [Examples]

The following shows an example of restoring a file (/tmp/hanet20041231.bk) created using the backup command.

```
# /opt/FJSVhanet/usr/sbin/hanetrestore -f /tmp/hanet20041231.bk
```

## 7.20 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 subnet mask information (the definition information set by hanetmask command)
- 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 information of virtual gateway configuration (the definition information set by hanetgw command)
- The setting information of the network monitoring function (the definition information set by hanetpathmon command)

The parameters set by hanetpoll on command, hanetparam command, hanetobserv param 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. If even one virtual interface is registered as cluster resources in the corresponding system, it is not possible to initialize.

-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. If RMS is activated at PRIMECLUSTER operation in a corresponding system, it is not possible to reactivate. If you restart on the host OS when the virtual machine function is used, the standby patrol and the interface of Fast switching mode are not activated. Activate them executing the strptl command or the strhanet command.

### [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.
- When you execute this command, please stop RMS beforehand.
- If you execute the resethanet -s command during operation, all virtual interfaces are re-activated, which may cut off communication between user applications.
- If a virtual bridge is connected to a virtual interface used in Virtual NIC mode, disconnect the bridge before executing this command.
- The virtual interface on the Virtual NIC mode in the single system configuration cannot be restarted. When changing the setting of the activated virtual interface, deactivate it with the stphanet command and then activate it with the strhanet command.

### [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
```

# 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:	EEEE	FFFF
(1)	(3)	(4)	(5)	(6)

2. A format for console output messages:

hanet:	AAAAA:	BBBCC	DDDDD:	EEEE	FFFF
(1)	(2)	(3)	(4)	(5)	(6)

### (1) Component name

Always begins with "hanet".

### (2) Error Kind

Included in the console messages. AAAAA provides the following information:

ERROR:

Error message

WARNING:

Warning message

INFO:

Information message. It is only output when the system log ("[3.2.3 Setting up the system log](#)") is set.

### (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 700)

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.	An unauthorized user performed the operation.	Only a user with super-user privilege can perform this operation.
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.
113	polling already active.	The HUB monitoring function has already been activated.	No action is required.
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 within the range for each value, and execute the command again.
117	polling already stopped.	The HUB monitoring function has already been deactivated.	No action is required.

Message number	Message	Meaning	Action
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.
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.

Message number	Message	Meaning	Action
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.
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 transmission line monitoring of the specified operation set was operating.	Stop the transmission line monitoring, and execute the command again.
152	logicalIP is inactive.	The specified processing could not be performed because the transmission line monitoring of the specified operation set was stopped.	Start the transmission line 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	Specify correct operation set information.

Message number	Message	Meaning	Action
		in the operation set information is invalid.	
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 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.
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/hosts 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/hosts file. If the host



Message number	Message	Meaning	Action
			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-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 Fast switching mode or GS linkage mode, make sure that the setting of the physical interface is correct and activated. 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 Fast switching 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.
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.

Message number	Message	Meaning	Action
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 128).	The number of virtual interfaces of the communication target exceeded the maximum number (maximum 128).	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 reached the maximum number possible to bundle. Therefore, it is not possible to add an actual interface dynamically.	Review the number of the physical interfaces that configures a virtual interface, 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.

Message number	Message	Meaning	Action
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/sysconfig/network-scripts/ifcfg-ethX file.
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.
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 takeover IP address incompatible.	The specified address form of a takeover IP address (an address family) is not compatible with that of a setting virtual interface.	Make an address form of a takeover IP address compatible with that of a setting virtual interface and execute again.
199	invalid takeover IP address.	The specified takeover IP address is invalid.	Check a value of the specified takeover 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.

Message number	Message	Meaning	Action
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 virtual interface for the specified address family is not defined.	Match the specifying address family with the address family of the virtual interface defined in the configuration then retry.
210	invalid address family.	The specified address family does not match the address family of the virtual interface.	Match the specifying address family with the address family of the virtual interface defined in the configuration then retry.
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 (VLAN-ID). 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 (VLAN-ID). 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 (VLAN-ID). Then, retry the operation.
216	When polling address is one, HUB-HUB polling flag must be OFF.	When polling address is one, HUB-to-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/sysconfig/network-scripts/ifcfg-interface) for the physical interface exists or the setting is correct. Modify the incorrect setting and then reboot the system. Execute the command again.
218	bundled interface does not exist.	A virtual interface bundling physical interface or tagged VLAN interface does not exist.	Ensure virtual interface bundling physical interface or 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.

Message number	Message	Meaning	Action
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.

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 been defined in the configuration information.	Specify a virtual interface so that it does not conflict with the 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.

Message number	Message	Meaning	Action
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.
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.

Message number	Message	Meaning	Action
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.
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 transmission line 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	observ information is not defined.	Monitoring destination information is not defined.	Define the monitoring destination information with the hanetobserv command.
352	routed is not started.	Not yet activated a routing daemon (routed).	Change a system definition (check if or not there is /etc/defaultrouter file, change a name

Message number	Message	Meaning	Action
			or delete it if exists) to activate a routing daemon (routed) and reboot the system.
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 on the specified virtual interface.	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 field engineers with the reported error message.
357	different network addresses are inappropriate.	Network addresses set for the NICs to be used are different.	Set the same network addresses for the NICs to be used. Review the assigned IP address (hostname) and netmask (prefix length).
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.
359	virtual gateway information is not defined.	A virtual gateway is not defined.	Define the virtual gateway information with the hanetgw command.
360	takeover ip address is not defined.	A takeover IP address is not set.	Review the setting of a Redundant Line Control Function and a cluster system.
361	virtual interface is not defined.	A virtual interface is not set.	Review the setting of a Redundant Line Control Function and a cluster system.
367	could not delete file. file=ifcfg-shaX	A file cannot be deleted.	Check the operation status of the "ifcfg-shaX" file, which is to be deleted, under /etc/sysconfig/network-scripts/. After confirming that there is no problem with "ifcfg-shaX" file, delete it.
368	file already exists. file=ifcfg-shaX	The file has already existed.	Check the operation status of the "ifcfg-shaX" file under /etc/sysconfig/network-scripts/. If there is no problem, no action is required.
369	file not found. file=/XXXX/YYYY	A file cannot be found.	Check whether the corresponding file exists or not and its authority. After confirming that there is no problem, with "hanetconfig delete", delete the virtual interface setting of the GLS most recently created with "hanetconfig create". Then create the virtual interface setting of the GLS with "hanetconfig create" again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.
370	path not found. path= /XXXX/YYYY	A path cannot be found.	Check that the appropriate path exists. After confirming that there is no problem, with "hanetconfig delete", delete the virtual



Message number	Message	Meaning	Action
			interface setting of the GLS most recently created with "hanetconfig create". Then create the virtual interface setting of the GLS with "hanetconfig create" again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.
371	invalid configuration parameter. file=/XXXX/YYYY	A parameter is invalid.	Check whether the corresponding file exists or not and its contents of the setting. After confirming that there is no problem, inactivate the virtual interface with "stphanet", and then activate it with "strhanet".
372	could not set vlan load balance.	Setting of VLAN load balance is failed.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
373	file not found. file=/XXXX/YYYY	A file cannot be found.	Check that the appropriate path exists. After confirming that there is no problem, with "hanetconfig delete", delete the virtual interface setting of the GLS most recently created with "hanetconfig create". Then create the virtual interface setting of the GLS with "hanetconfig create" again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.

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 a Redundant Line Control Function and a 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 a 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 a Redundant Line Control Function and a 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 a 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.

Message number	Message	Meaning	Action
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 a 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 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 a 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 a 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 a 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 a 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..
519	ioctl(SHAIOCPLUMB) fail.	An error was found in the internal system call.	Check that there is no mistake in the setting of a Redundant Line Control Function. After checked there is no mistake, execute a command again. If the same phenomenon occurs, Collect materials for examination

Message number	Message	Meaning	Action
			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 a 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 a 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 a 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 a 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..
541	ioctl(SHAIOCSAP) fail.	An unexpected system call error occurred.	Check that there is no mistake in the setting of a 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 a 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 a 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 a 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
545	ioctl(SHAIOCMESAGE) fail.	An unexpected system call error occurred.	Check that there is no mistake in the setting of a 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..
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 a 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 a 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 a 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..
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 dettach 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.	No action is required because recovery is automatically made. However, the message is output repeatedly, follow the procedure described below. The following system resources are required for a

Message number	Message	Meaning	Action
			<p>Redundant Line Control Function:</p> <p>* semsys:seminfo_semmni (The maximum number of the semaphore identifiers) : One or greater</p> <p>* semsys:seminfo_semmns (The maximum number of the semaphores in a system) : One or greater</p> <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(0xde.....) has already been used by another application. Verify if the same identifier is used in the system using ipcs command.</p> <p>If the problem still remains even after the identifier has been changed, collect examination materials of a Redundant Line Control Function and contact field engineers.</p>
557	get shared memory segment identifier failed.	An error was found in the internal system call.	<p>No action is required because recovery is automatically made. However, the message is output repeatedly, follow the procedure described below.</p> <p>The following system resources are required for a Redundant Line Control Function:</p> <p>* shmsys:shminfo_shmmax (The maximum size of the shared memory segment) : 5120 or greater</p> <p>* shmsys:shminfo_shmmni (The maximum number of the shared memory segments) : two or greater</p> <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(0xde.....) has already been used by another application. Verify if the same identifier is used in the system using ipcs command.</p> <p>If the problem still remains even after the identifier has been changed, collect examination materials of a 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 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..

Message number	Message	Meaning	Action
561	daemon process does not exist.	An internal error occurred.	If not rebooted after the installation, first reboot, then execute again. If the same message is output even after rebooted, Collect materials for examination of Redundant Line Control Function, and tell field engineers an 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(SHAIOPATROLL) fail.	An error was found in the internal system call.	Execute the command again. If the same error message is output, contact a field engineers about 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 a 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..
567	ioctl(SIOCGIFADDR) fail.	An error occurred in the internally used system call.	Check there is no mistake in the setting of a 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 tell field engineers an error message.
568	ioctl(SIOCGIFNETMASK) fail.	An error occurred in the internally used system call.	Check there is no mistake in the setting of a 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 tell field engineers an error message.
569	could not communicate with daemon process.	Failed to communicate between a command and a daemon.	Collect materials for examination of Redundant Line Control Function, and tell field engineers an error message.
570	failed to get socket.	An error occurred in the internally used system call.	Collect materials for examination of Redundant Line Control Function, and tell field engineers an 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 tell field engineers an 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 tell field engineers an error message.

Message number	Message	Meaning	Action
573	request timeout.	An error occurred in the internally used system call.	Collect materials for examination of Redundant Line Control Function, and tell field engineers an error message.
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 a Redundant Line Control Function and inform field engineers about an error message.
575	failed to restart hanet.	Failed to reactivate a Redundant Line Control Function.	Execute the command again. If the same phenomenon still occurs, collect the examination materials of a Redundant Line Control Function and inform field engineers about an 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 field engineers with the reported error message.
577	failed to create a directory.	Creation of a work directory failed when the command for collecting troubleshooting information was executed.	Check if a directory on which the troubleshooting information should be stored exists, and the user has access privileges. If there is nothing wrong with the above, execute the command again. If there are any problems, solve the problems then execute the command again.
578	could not create file.	A file cannot be created.	With "hanetconfig delete", delete the virtual interface setting of the GLS most recently created with "hanetconfig create". Then create the virtual interface setting of the GLS with "hanetconfig create" again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.
579	could not create symbolic link.	A symbolic link cannot be created.	With "hanetconfig delete", delete the virtual interface setting of the GLS most recently created with "hanetconfig create". Then create the virtual interface setting of the GLS with "hanetconfig create" again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.
580	could not execute script. script=/XXX/YYY/ZZZ	Script execution has failed.	Check whether the corresponding script exists or not and its authority. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, uninstall the package of the GLS and install it again.
581	system call fail. func=XXXX errno=YY	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
582	could not start monitoring.	Network monitoring cannot be started.	Start network monitoring with the " hanetpathmon on" command. If the same phenomenon occurs, collect materials for the examination of the Redundant Line

Message number	Message	Meaning	Action
			Control Function and contact field engineers to report the error message.
583	could not stop monitoring.	Network monitoring cannot be stopped.	Stop network monitoring with the "hanetpathmon off" command. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
585	network path monitoring is running.	As network monitoring is running, monitoring parameters cannot be changed.	Execute the command again after stopping network monitoring with the "hanetpathmon off" command.
586	virtual interface is inactive.	As the virtual interface is inactivated, network monitoring cannot be started.	Execute the command again after activating the virtual interface with the "strhanet" command.

Table A.4 Message number 7xx

Message number	Message	Meaning	Action
700	invalid network mask.	The specified subnet mask is invalid.	Specify the correct subnet mask and execute the command again.
701	ipv6 module is not loaded.	ipv6 module is not loaded.	Configure the system to load ipv6 module during the system startup and then reboot the system.
702	the number of specified IP address is different.	The number of specified IP addresses is different.	Specify the correct number of IP address and re-execute the command.
703	could not switch interface because standby interface does not exist.	As there is no interface in standby state, an interface cannot be switched.	Check that there is a physical interface in standby state with "dsphanet" command.
704	specified interface is connected to a virtual bridge.	The specified virtual interface is connected to a virtual bridge.	Disconnect from a virtual bridge and execute the command again.
705	invalid VLAN-ID.	The specified VLAN ID is invalid.	Specify the valid VLAN ID and execute the command again.
706	could not start hanetpathmd.	Network monitoring daemon cannot be activated.	Check that there is no problem in the network monitoring setting. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.



Message number	Message	Meaning	Action
707	the name of the virtual interface is already used..name=xxx	The name of the virtual interface has already been used.	With " ifconfig -a", find the interface which has the same name. If it is the virtual bridge, delete it with the "brctl" command.
708	bundled interface is unused because the vlan interface is created.	As the VLAN interface is created for the bundled physical interface, a physical interface was not used.	Check whether the interface is created for the bundled physical interface with "ifconfig -a". If so, delete the VLAN interface with the "vconfig" or "ip" command and execute the command again.
730	different network addresses are inappropriate.	Network addresses set for the NICs to be used are different.	Set the same network addresses for the NICs to be used. Review the assigned IP address (hostname) and netmask (prefix length).
760	ioctl(SHAIOCSETPDEVRCV) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control function is correctly set. If no problem has been found, re-execute the command. If the same error occurs, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.
761	ioctl(SHAIOCDELPDEVRCV) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control function is correctly set. If no problem has been found, re-execute the command. If the same error occurs, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.
762	ioctl(SHAIOCTCPABORT) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control function is correctly set. If no problem has been found, re-execute the command. If the same error occurs, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.
763	A process has failed on some of the NIC shared virtual interfaces.	A process has failed on some of the virtual interfaces sharing NICs.	Re-execute the command. If the same error occurs, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.
764	failed to get ip address information.	Failed to get the IP address information.	The IP address information for the specified NIC may not be set in the /etc/sysconfig/network-script/ifcfg-ethX file (X indicates the device number). Set the IP address information in the /etc/sysconfig/network-script/ifcfg-ethX file and re-execute the command. If the same error occurs, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.

Message number	Message	Meaning	Action
766	ioctl(SHAIOCSETNICCHANGE) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
767	ioctl(SHAIOCGETSHADEVATTR) fail.	An error occurred in the internally used system call	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
768	ioctl(SHAIOCSETLBMODE) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
769	ioctl(SHAIOCLBCTL) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
770	ioctl(SHAIOCGETLBPARAM) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
771	ioctl(SHAIOCGETLBINFO) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and contact field engineers to report the error message.
772	ioctl(SHAIOCPREUNPLUMB) fail.	An error occurred in the internally used system call.	Check that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same phenomenon occurs, collect materials for the

Message number	Message	Meaning	Action
			examination of the Redundant Line Control Function and 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.

Messages (numbers 910 to 914) are output to /var/log/messages in the following format by adding kern.info to /var/log/messages of /etc/syslog.conf (for RHEL5) or /etc/rsyslog.conf (for RHEL6).

Output example)

Message number 914 output when the virtual interface switches the physical interface

Jul 7 21:44:32 linux kernel: hanet: INFO: 91480: the physical interface of the virtual interface was switched. (sha1:untagged from=eth6 to=eth4)
Jul 7 21:44:32 linux kernel: hanet: INFO: 91480: the physical interface of the virtual interface was switched. (sha1:tagged from=eth6 to=eth4)

The following table shows facilities and priorities for the message numbers output to the system log.

Facility	Priority	Message number
kern	info	800, 801, 990, 991, 992
kern	error	910, 911, 912, 913, 914
user	info	856, 888, 889, 890, 891, 892, 893, 894, 895
user	warning	848
user	error	other than those above

Table A.5 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.
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.
802	file open failed.	Failed to open the file.	No action is required.
803	file read failed.	Failed to read the file.	Collect materials for examination of Redundant Line Control Function, and then

Message number	Message	Meaning	Action
			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.	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.	<p>If HWADDR is set in the operating system configuration file (ifcfg-ethX), check whether the file is set to disable HOTPLUG (for example, HOTPLUG=no). For details, see "<a href="#">3.2.2 Network configuration</a>". If a virtual bridge has been connected to the virtual interface, check that the virtual bridge has been activated.</p> <p>If no problem has been found, collect materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.</p>
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(SHAIOCSSETRSCMON) 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 a Redundant Line Control Function and a cluster system. If there is no mistake, Collect materials for examination of Redundant Line Control Function and a 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 a Redundant Line Control Function and a cluster system. If there is no mistake, Collect materials for examination of Redundant Line Control Function and a cluster system, and then contact field engineers to report the error message.. See the manual of a cluster

Message number	Message	Meaning	Action
			system as to the materials necessary for examining a cluster system.
823	ClSetStat failed.	The cluster resource status could not be set.	Check that there is no mistake in the setting of a Redundant Line Control Function and a cluster system. If there is no mistake, Collect materials for examination of Redundant Line Control Function and a 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 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

Message number	Message	Meaning	Action
			contact field engineers to report the error message..
834	interface does not exist.	The interface defined in NIC switching mode does not exist.	Please check that there is no error in the definition of a Redundant Line Control Function, and the definition of a system. Moreover, please check about the existence of the corresponding interface using the ifconfig command. When abnormalities cannot be discovered, Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message..
845	could not restart routed.	Failed to restart the routing daemon. The HUB monitoring function is stopped and cluster switching is performed.	Check that there is no mistake in the setting of a system, a Redundant Line Control Function, and a cluster system. If the same phenomenon occurs, Collect materials for examination of Redundant Line Control Function and a 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 rdisc.	Failed to restart the router discovery daemon. The HUB monitoring function is stopped and cluster switching is performed.	Check that there is no mistake in the setting of a system, a Redundant Line Control Function, and a cluster system. If the same phenomenon occurs, Collect materials for examination of Redundant Line Control Function and a 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.
847	internal error retry over. polling stop.	A HUB monitoring internal error occurred. The HUB monitoring is stopped.	Check that there is no mistake in the setting of a system, a Redundant Line Control Function, and a cluster system. If the same phenomenon occurs, Collect materials for examination of Redundant Line Control Function and a 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.
848	device is inactive. polling stop.	The virtual interface for HUB monitoring is not activated. The HUB monitoring function is disabled.	Activate the virtual interface. Then, inactivate and activate the HUB monitoring function. This message may be displayed when cluster switching occurs during cluster operation, but in this case, no action is needed.
849	poll fail retry over. polling stop.	The transmission line failed as many times as specified by the retry count consecutively. The HUB monitoring function is disabled.	Check the line failure. After checking the line recovery, inactivate and activate the HUB monitoring function.

Message number	Message	Meaning	Action
850	cannot down interface.	Failed to inactivate the physical interface.	Check that the Redundant Line Control function and the system are correctly set. If HWADDR is set in the operating system configuration file (ifcfg-ethX), check whether the file is set to disable HOTPLUG (for example, HOTPLUG=no).  For details, see " <a href="#">3.2.2 Network configuration</a> ". If no problem has been found, collect materials for the examination of the Redundant Line Control function and 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 a Redundant Line Control Function and a 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 a Redundant Line Control Function and a 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, a Redundant Line Control Function, and a cluster system. If the same phenomenon occurs, Collect materials for examination of Redundant Line Control Function and a 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	Review the cluster system settings, and reboot the system

Message number	Message	Meaning	Action
		cluster settings are incomplete.	
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.
860	interface does not exist.	There is no interface which NIC switching mode is using.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message..
861	cannot set interface flags.	The flag operation to an interface in use became failure.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message..
870	polling status changed: Primary polling failed. (ifname,target=pollip)	Ping monitoring on the primary side has failed. ifname: Interface name pollip: Monitoring destination address vlanid: VLAN for monitoring destination	Check that there is no problem in communication routes to the monitoring destination. Perform recovery steps as needed (see " <a href="#">F.3.1 Error messages(870) and corresponding actions for HUB monitoring</a> "). When monitoring is failed even if communication is normal, tuning is required for the monitoring interval and the number of monitoring.
	polling status changed: Primary polling failed. (ifname,target=pollip, vlan=vlanid)		
871	polling status changed: Secondary polling failed. (ifname,target=pollip)	Ping monitoring on the secondary side has failed. ifname: Interface name pollip: Monitoring destination address vlanid: VLAN for monitoring destination	Check that there is no problem in communication routes to the monitoring destination. Perform recovery steps as needed (see " <a href="#">F.3.1 Error messages(870) and corresponding actions for HUB monitoring</a> "). When monitoring is failed even if communication is normal, tuning is required for the monitoring interval and the number of monitoring.
	polling status changed: Secondary polling failed. (ifname,target=pollip, vlan=vlanid)		
872	polling status changed: PrimaryHUB to SecondaryHUB polling failed. (ifname,target=pollip)	HUB-to-HUB communication 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. Review " <a href="#">F.3.1 Error messages(870) and corresponding actions for HUB monitoring</a> ".
873	polling status changed: SecondaryHUB to PrimaryHUB polling failed. (ifname,target=pollip)	HUB-to-HUB communication 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. Review " <a href="#">F.3.1 Error messages(870) and corresponding actions for HUB monitoring</a> ".
874	polling status changed: HUB repair (target=pollip)	Line failure in ping monitoring has repaired. pollip: Monitoring destination address	No action is required.
	polling status changed: HUB repair (target=pollip,vlan=vlanid)	pollip: Monitoring destination address vlanid: VLAN for monitoring destination	



Message number	Message	Meaning	Action
875	standby interface failed.(ifname)	Route failure was detected by the standby patrol. ifname: Interface name of standby patrol vlanid: VLAN for monitoring destination	Check that there is no problem in communication routes between the operating NIC and the standby NIC. Perform recovery steps as needed (see " <a href="#">F.3.2 Error messages(875) and corresponding actions for standby patrol</a> "). When monitoring is failed even if communication is normal, tuning is required for the monitoring interval and the number of monitoring.
	standby interface failed.(ifname, vlan=vlanid)		
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.
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.	It is not necessary to deal with.
882	shared memory is broken. (errno)	Creates a shared memory again because it is deleted.	It is 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. Note that no action is required when this message is output at the timing of connecting LAN cable in the environment which uses IPv6, which leads to turn the status of the physical interface from link down to link up. This is caused by the automatic activation of a physical interface due to the automatic allocation of a link local address by the OS.
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.

Message number	Message	Meaning	Action
885	standby interface recovered. (ifname)	The recovery of the route in the standby side was detected by standby patrol. ifname: Interface name of standby patrol vlanid: VLAN for monitoring destination	It is not necessary to deal with.
	standby interface recovered. (ifname, vlan=vlanid)		
886	recover from route error is noticed. (ifname)	The recovery was notified from the remote system. ifname: Interface name	It is 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	It is not necessary to deal with.
888	interface is activated. (ifname)	The physical interface was activated. ifname: Interface name	It is not necessary to deal with.
889	interface is inactivated. (ifname)	The physical interface was inactivated. ifname: Interface name	It is not necessary to deal with.
890	logical IP address is activated. (logicalIP)	The logical IP address was activated. logicalIP: Logical IP	It is not necessary to deal with.
891	logical IP address is inactivated. (logicalIP)	The logical IP address was inactivated. logicalIP: Logical IP	It is not necessary to deal with.
892	logical virtual interface is activated. (ifname)	The logical virtual interface was activated. ifname: Interface name	It is not necessary to deal with.
893	logical virtual interface is inactivated. (ifname)	The logical virtual interface was inactivated. ifname: Interface name	It is not necessary to deal with.
894	virtual interface is activated. (ifname)	The virtual interface was activated. ifname: Interface name	It is not necessary to deal with.
895	virtual interface is inactivated. (ifname)	The virtual interface was inactivated. ifname: Interface name	It is not necessary to deal with.
896	path to standby interface is established. (ifname)	Monitoring by standby patrol has started normally. Ifname: Interface name of standby patrol vlanid: VLAN for monitoring destination	It is not necessary to deal with.
	path to standby interface is established. (ifname, vlan=vlanid)		
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	It is not necessary to deal with.

Message number	Message	Meaning	Action
		set by a hanetpoll create command is other than HUB.	
898	unexpected interface flags have been detected. (ifname) (code)	Since the interface was unjustly changed by the user, the state of an interface is restored. ifname: interface name code: detailed code	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 interface flag change.
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 you are using NIC switching (operation mode "e"), change the operation mode, or perform asynchronous switching. Also, change the monitored remote system settings according to the message.

Table A.6 Message number 9xx

Message number	Message	Meaning	Action
900	routing information has inconsistency.	Routing information of the communication target, which is set by using the hanetobserv command, is not registered into the routing table, or inconsistent routing information is registered.	Check if there is any inconsistency between the following information: <ul style="list-style-type: none"> <li>- A gateway address of the real IP address of the communication target set by using the hanetobserv command</li> <li>- Routing information registered into the routing table</li> </ul>
906	route error to virtual ip address is detected. (target=xxx.xxx.xxx.xxx)	Every monitoring path for the virtual addresses of the remote system failed.	Check that there is no problem with the communication path to the virtual IP addresses of the remote system.
907	recover from route error to virtual ip address is detected. (target=xxx.xxx.xxx.xxx)	Monitoring the virtual IP addresses of the remote system is now possible.	No action is required.
908	hanetctld restarted.	The control daemon of the GLS is restarted.	No action is required.
909	failed to restart daemon.	Restarting the control daemon of the GLS is failed.	Restart the Redundant Line Control Function for recovery (/opt/FJSVhanet/usr/sbin/resethanet -s). When recovery is failed, restart the OS.
910	link up detected: the physical interface link is up. (devicename: ifname)	The physical interface is linked up. devicename: Virtual interface name	No action is required.

Message number	Message	Meaning	Action
		ifname: Physical interface name	
911	link down detected: the physical interface link is down. (devicename: ifname)	The physical interface is linked down.  devicename: Virtual interface name  ifname: Physical interface name	Check the link state based on the execution results of the /sbin/ifconfig ifname command (RUNNING flag displayed) and the /sbin/ethtool ifname command ("Link detected: yes" displayed).  If the link is down, check whether the neighboring switch works, and whether the speed settings (auto negotiation, full-duplex, etc) for the switch and server are correctly set.
912	link up detected: the virtual interface link is up. (devicename)	The virtual interface is linked up.  devicename: Virtual interface name	No action is required.
913	link down detected: the virtual interface link is down. (devicename)	The virtual interface is linked down.  devicename: Virtual interface name	Check the link status of the physical interface bundled by the virtual interface.
914	the physical interface of the virtual interface was switched. (devicename: vlantype from=ifname1 to=ifname2)	The physical interface which is used for communication of the virtual interface has been switched.  devicename: Virtual interface name  vlantype: "untagged" or "tagged"  ifname1: Physical interface before switching  ifname2: Physical interface after switching	Check the link status of the physical interface bundled by the virtual interface.  No action is required when the "hnetnic change" command is executed.  *vlantype  The "vlantype" is output only when a tagged VLAN interface is created on the virtual interface.
916	monitoring function detected failures in the entire transfer route. (ifname)	Failures in all transfer routes are detected by the network monitoring function.	Check that there is no problem in transfer routes to the monitoring destination and transfer routes between the operating NIC and the standby NIC.
	monitoring function detected failures in the entire transfer route. (ifname, vlan=vlanid)	ifname: Interface name vlanid: VLAN for monitoring destination	
927	physical interface settings is incorrect.(name=device ifname=interface param=XXXX)	There is an error in the physical interface settings.	Modify the physical interface configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX). For details, see <a href="#">"3.2.2 Network configuration."</a> After the modification is completed, restart the operating system.
928	physical interface configuration file not found.(name=device ifname=interface)	There is no physical interface configuration file.	Failed to see the physical interface configuration file (/etc/sysconfig/network-scripts/ifcfg-ethX). Check the file. For details, see <a href="#">"3.2.2 Network</a>

Message number	Message	Meaning	Action
			<a href="#">configuration</a> ." After the modification is completed, restart the operating system.
929	SHAMACADDR is not specified. (name=device)	SHAMACADDR is not specified. device: Virtual interface name	It is necessary to specify SHAMACADDR on a guest OS in VMware. Check the setting of SHAMACADDR in the virtual interface configuration file (/etc/sysconfig/network-scripts/ifcfg-shaX).
930	SHAMACADDR is invalid MAC address. (name=device)	The MAC address specified to SHAMACADDR is invalid. device: Virtual interface name	Specify the correct MAC address to SHAMACADDR. After that, restart the operating system.
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 " <a href="#">3.11.2.2 Error detection of the self-checking function</a> " 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 " <a href="#">3.11.2.2 Error detection of the self-checking function</a> " to take the appropriate action. t
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. # rpm -qi FJSVhanet # lsmod sha
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. # rpm -qi FJSVhanet # pgrep hanetctld
987	configuration is invalid.	Failed to switch virtual networks on the virtual machine.	Review the setting referenced in the message.
988	The virtual network link operation failed.	Failed to switch virtual networks on the virtual machine.	Check that there is no mistake in the setting of a Redundant Line Control Function and a 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..
989	The virtual network link operation ended normally.	Successfully switched virtual networks on the virtual machine.	No action is required.

Message number	Message	Meaning	Action
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)	Link is down for the primary interface in use.  ifname: interface name  pollip: monitoring destination address	Check the link state based on the execution results of the /sbin/ifconfig ifname command (RUNNING flag displayed) and the /sbin/ethtool ifname command ("Link detected: yes" displayed). If the link is down, check whether the neighboring switch works, and whether the speed settings (auto negotiation, full-duplex, etc) for the switch and server are correctly set.
994	link down detected: Secondary polling failed. (ifname,target=pollip)	Link is down for the primary interface in use.  ifname: interface name  pollip: monitoring destination address	Check the link state based on the execution results of the /sbin/ifconfig ifname command (RUNNING flag displayed) and the /sbin/ethtool ifname command ("Link detected: yes" displayed). If the link is down, check whether the neighboring switch works, and the speed settings (auto negotiation, full-duplex, etc) for the switch and server are correctly set.

## 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.	<p>Pay attention to the following points and check that there is no mistake in the settings of Redundant Line Control function and cluster system.</p> <ul style="list-style-type: none"> <li>- Ensure that the setting of the takeover IP address is identical in each node of the cluster which takes over the IP address.</li> </ul> <p>Execute "hanethvrsc print" to check it.</p>
-	(GLs): ERROR: GdBegin failed. (rsc_name, host_name)	<p>Failed to activate the GLs detector.</p> <p>rsc_name: Resource name of the cluster</p> <p>host_name: Takeover virtual IP address (host name)</p>	<ul style="list-style-type: none"> <li>- For NIC switching mode, ensure that the ping monitoring is set.</li> </ul> <p>Execute "hanetpoll print" to check it.</p> <ul style="list-style-type: none"> <li>- If a host name is used in GLS, ensure that host name is already recorded in /etc/hosts.</li> <li>- Ensure that the IP address setting of RMS Wizard is identical to that of the GLS takeover IP address.</li> </ul> <p>If those settings are not correct, see the following sections to configure the settings correctly. After that, reboot the system or execute resethanet -s.</p> <p><a href="#">"3.3 Additional system setup"</a></p> <p><a href="#">"3.4 Changing system setup"</a></p> <p><a href="#">"3.5 Deleting configuration information"</a></p> <p><a href="#">"5.2 Configuration for Cluster system"</a></p> <p>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.</p>
-	online request failed.(errno)	<p>Failed to activate the GLs resource in the online or standby state.</p> <p>19: An appropriate is not recognized by GLS.</p> <p>201: Failed to activate the physical interface.</p> <p>203: Failed to activate the takeover virtual interface.</p>	<p>Pay attention to the following points and check that there is no mistake in the settings of Redundant Line Control function and cluster system.</p> <ul style="list-style-type: none"> <li>- Ensure that the setting of the takeover IP address is identical in each node of the cluster which takes over the IP address.</li> </ul> <p>Execute "hanethvrsc print" to check it.</p> <ul style="list-style-type: none"> <li>- For NIC switching mode, ensure that the ping monitoring is set.</li> </ul> <p>Execute "hanetpoll print" to check it.</p> <ul style="list-style-type: none"> <li>- If a host name is used in GLS, ensure that host name is already recorded in /etc/hosts.</li> <li>- Ensure that the IP address setting of RMS Wizard is identical to that of the GLS takeover IP address.</li> <li>- Ensure that the network settings of the operating system (such as the setting of ifcfg-ethX or deactivation of HOTPLUG) are correct. For the network settings, see <a href="#">"3.2.2.1 Setup common to modes."</a></li> </ul> <p>If those settings are not correct, see the following sections to configure the settings correctly. After that, reboot the system or execute resethanet -s.</p> <p><a href="#">"3.3 Additional system setup"</a></p> <p><a href="#">"3.4 Changing system setup"</a></p> <p><a href="#">"3.5 Deleting configuration information"</a></p> <p><a href="#">"5.2 Configuration for Cluster system"</a></p> <p>If those settings are correct or the same phenomenon still occurs after configuring the settings, collect materials for examination of Redundant</p>

Message number	Message	Meaning	Action
			Line Control Function and cluster system, and then contact field engineers to report the error message.



## Appendix B Examples of configuring system environments

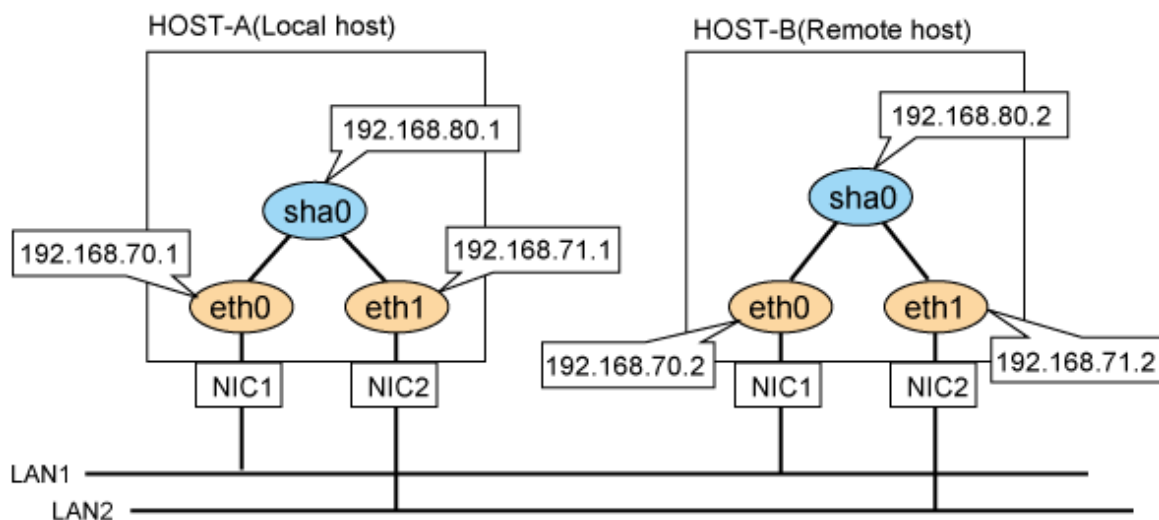
This appendix explains how to configure the system environment with redundant network control.

### 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.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
```

```
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

# [HOST-B]

## 1) Setting up the system

- 1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

- 1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

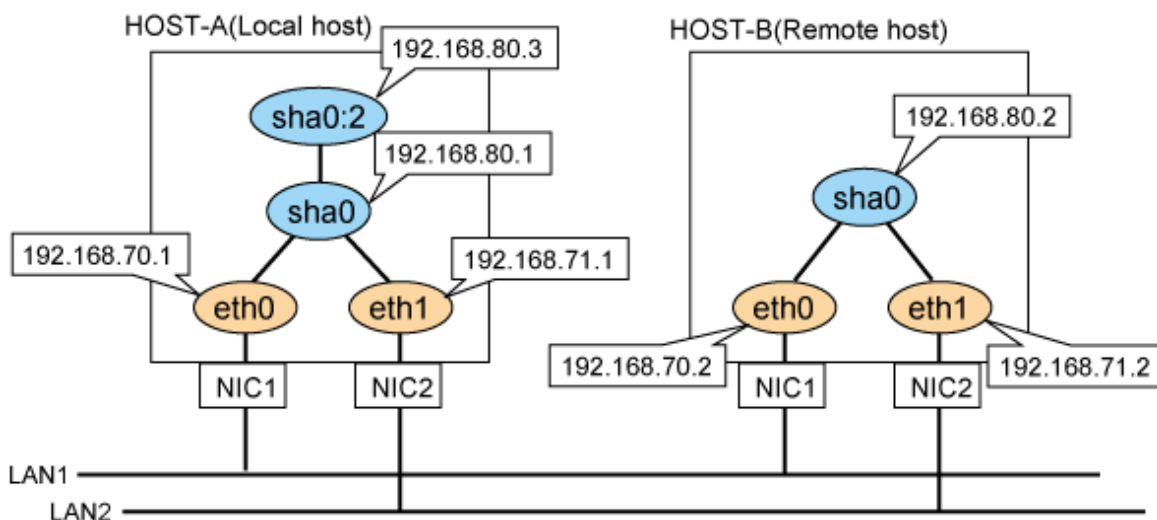
## 5) Activating of virtual interface

```
/opt/FJSVhanet/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.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
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
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

### 5) Creating of logical virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
```

### 6) Activating of virtual interface and logical virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

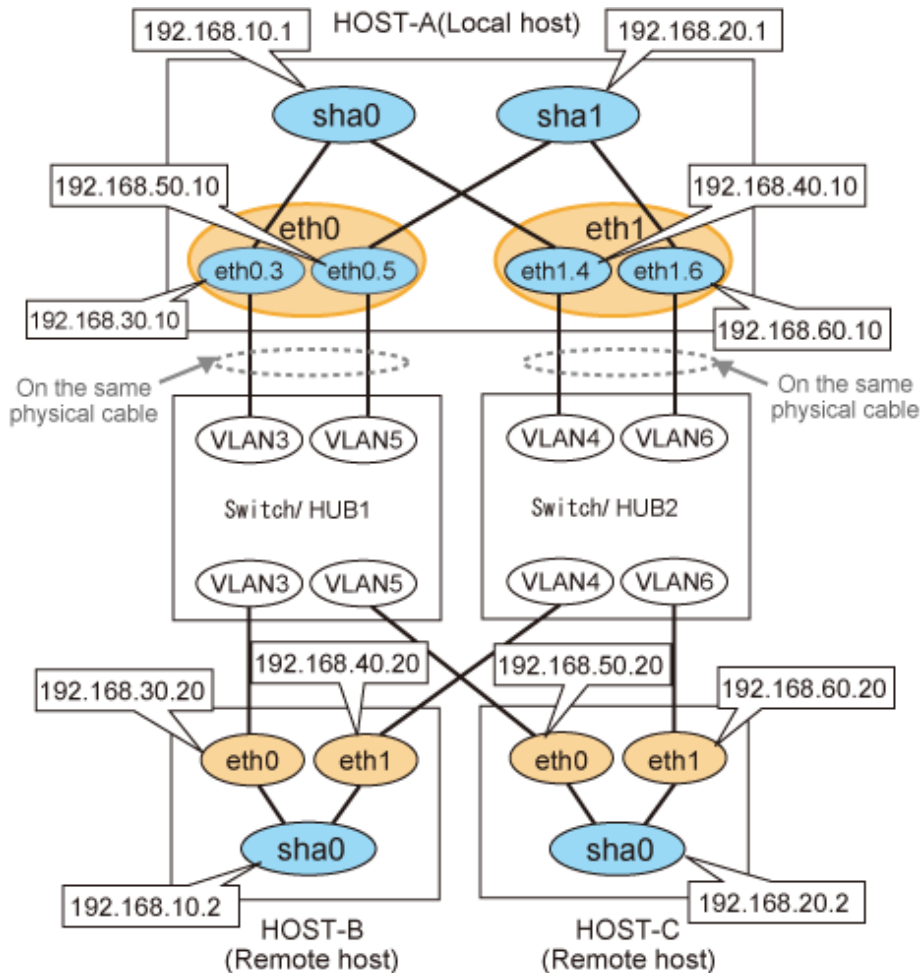
```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Activating of virtual interface

```
/opt/FJSVhanet/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.



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 3,4,5,6) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.3

```
DEVICE=eth0.3
BOOTPROTO=static
BROADCAST=192.168.30.255
IPADDR=192.168.30.10
NETMASK=255.255.255.0
NETWORK=192.168.30.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.4

```
DEVICE=eth1.4
BOOTPROTO=static
BROADCAST=192.168.40.255
IPADDR=192.168.40.10
NETMASK=255.255.255.0
NETWORK=192.168.40.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.5

```
DEVICE=eth0.5
BOOTPROTO=static
BROADCAST=192.168.50.255
IPADDR=192.168.50.10
NETMASK=255.255.255.0
NETWORK=192.168.50.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.6

```
DEVICE=eth1.6
BOOTPROTO=static
BROADCAST=192.168.60.255
IPADDR=192.168.60.10
NETMASK=255.255.255.0
NETWORK=192.168.60.0
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0.3, eth0.5, eth1.4 and eth1.6 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.10.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.20.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t eth0.3,eth1.4
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t eth0.5,eth1.6
```

## 5) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

# [HOST-B]

## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.30.255
IPADDR=192.168.30.20
NETMASK=255.255.255.0
NETWORK=192.168.30.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1



```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.40.255
IPADDR=192.168.40.20
NETMASK=255.255.255.0
NETWORK=192.168.40.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.10.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t eth0,eth1
```

## 5) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

# [HOST-C]

## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.50.255
IPADDR=192.168.50.20
NETMASK=255.255.255.0
NETWORK=192.168.50.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.60.255
IPADDR=192.168.60.20
NETMASK=255.255.255.0
NETWORK=192.168.60.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.20.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t eth0,eth1
```

## 5) Activating of virtual interface

```
/opt/FJSVhanet/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.

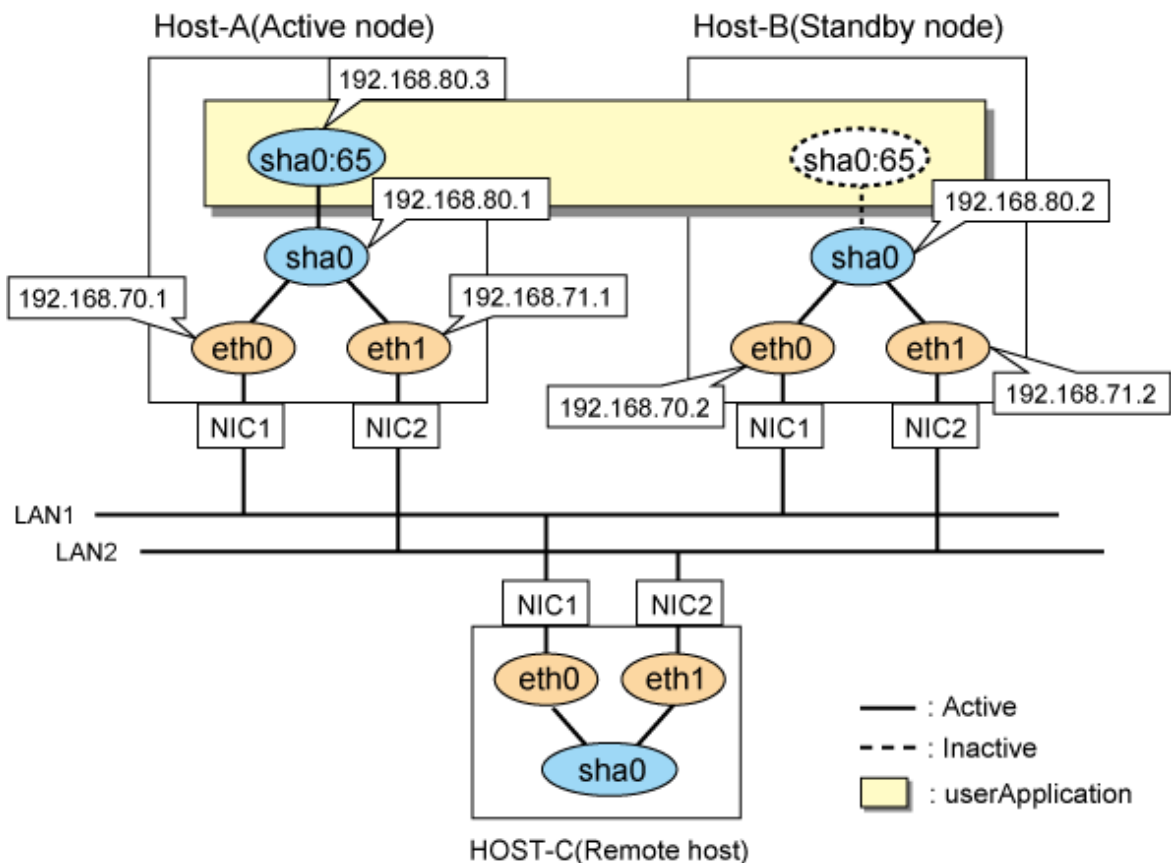
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.1.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.3    hosta1 # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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.

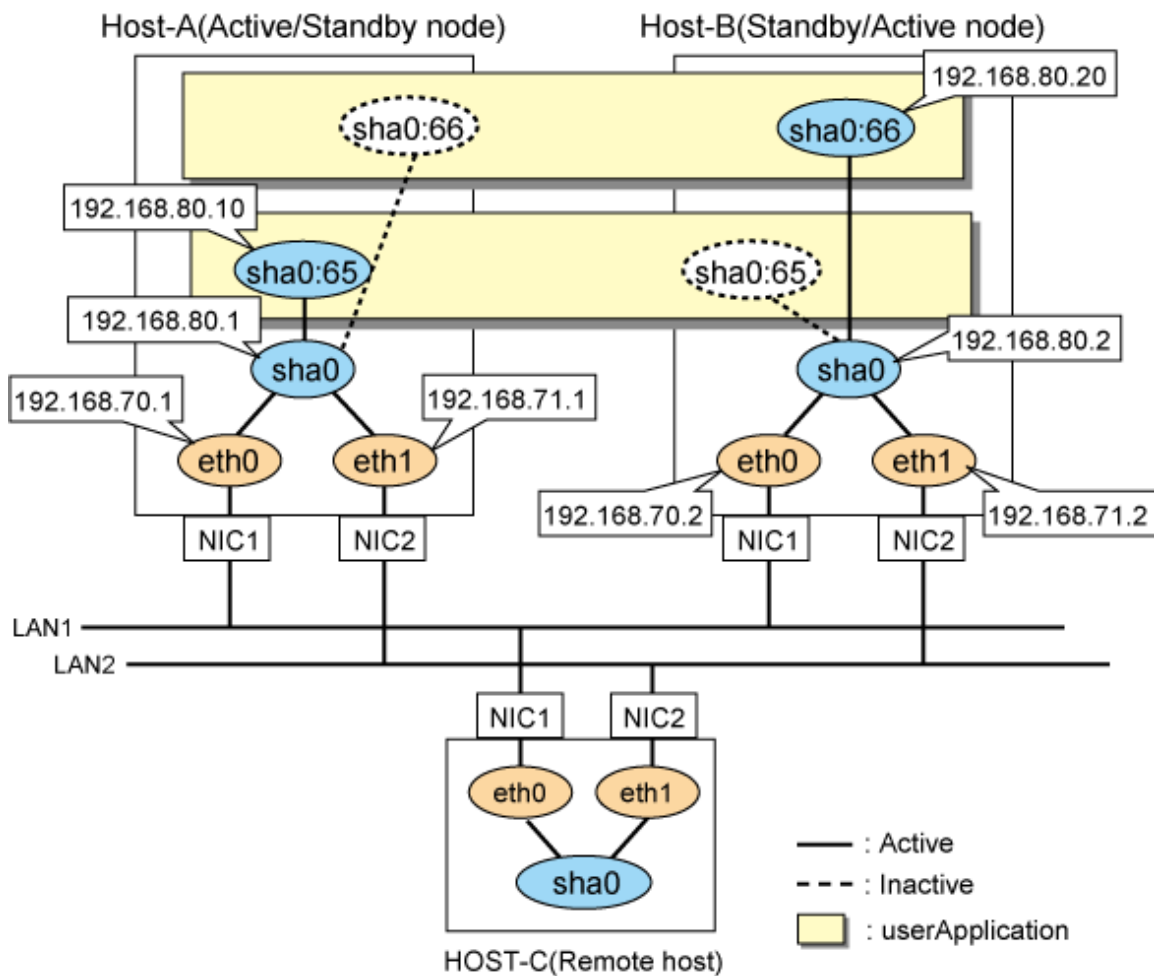
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.1.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.10   hosta1 # HOST-A/B Takeover virtual IP
192.168.80.20   hostb1 # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating 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/hosts file. Defined content is same as HOST-A.

- 1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
```

```
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating 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 configuring HOST-A and HOST-B, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

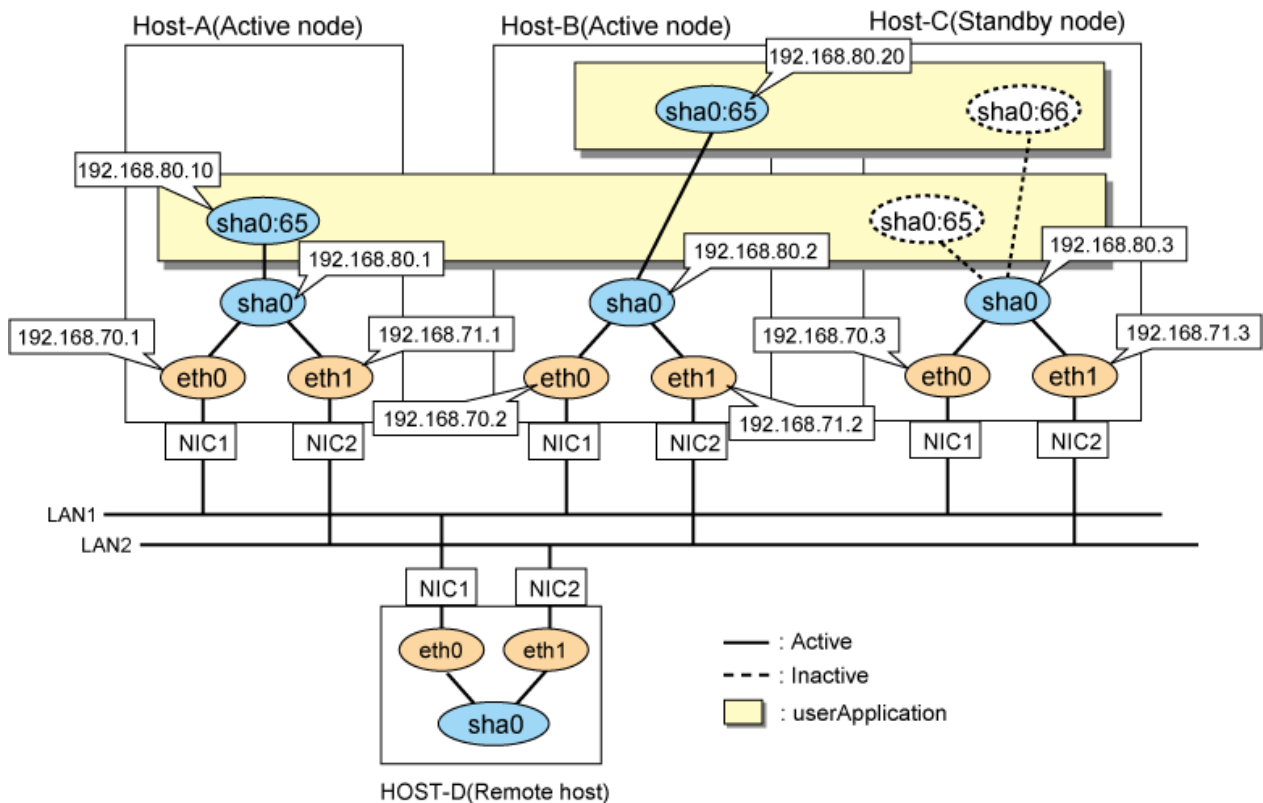
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.1.1 Example of the Single system](#)".





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP
192.168.71.3    host32 # HOST-C Physical IP
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.10   hosta1 # HOST-A/C Takeover virtual IP
192.168.80.20   hostb1 # HOST-B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
```

```
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/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/hosts file. Defined content is same as HOST-A.

- 1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
```

## 5) Creating 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 configuring HOST-A, HOST-B, and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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.

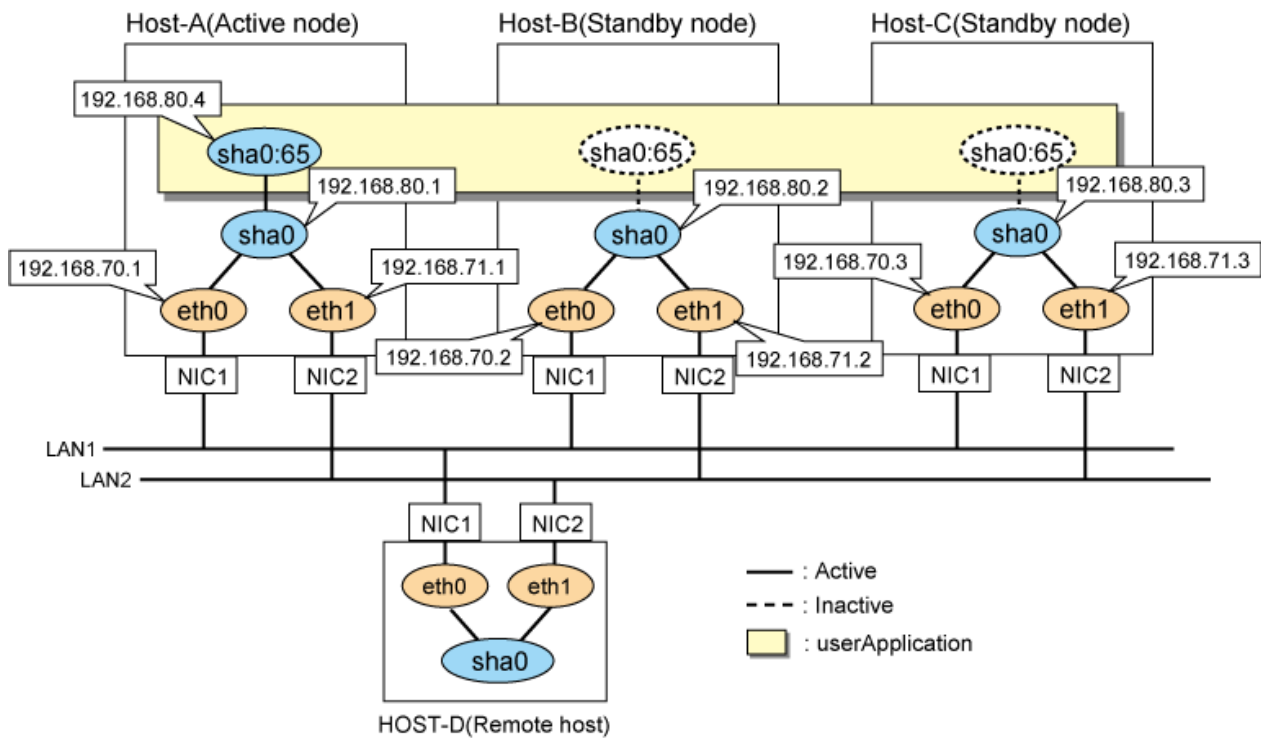
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.1.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP
192.168.71.3    host32 # HOST-C Physical IP
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.4    hosta1 # HOST-A/B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
```

## 5) Creating 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 configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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

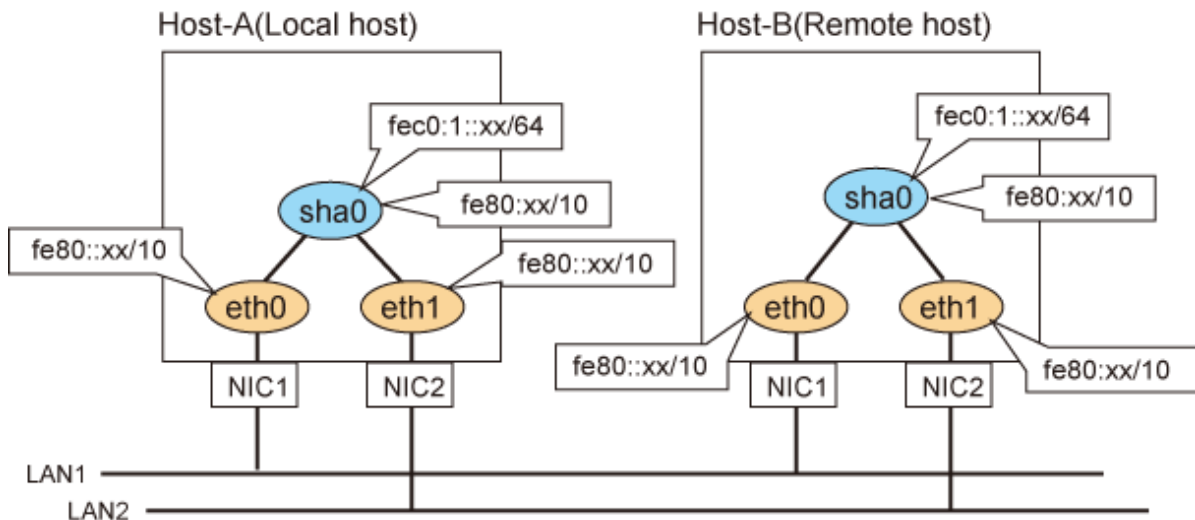
---

This section describes an example configuration procedure of the network shown in the diagram below.

The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".





## [HOST-A]

### 1) Setting up the system

1-1) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-2) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

#### 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

#### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

#### 5) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

### [HOST-B]

#### 1) Setting up the system

1-1) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-2) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 5) Reboot

Run the following command and reboot the system.

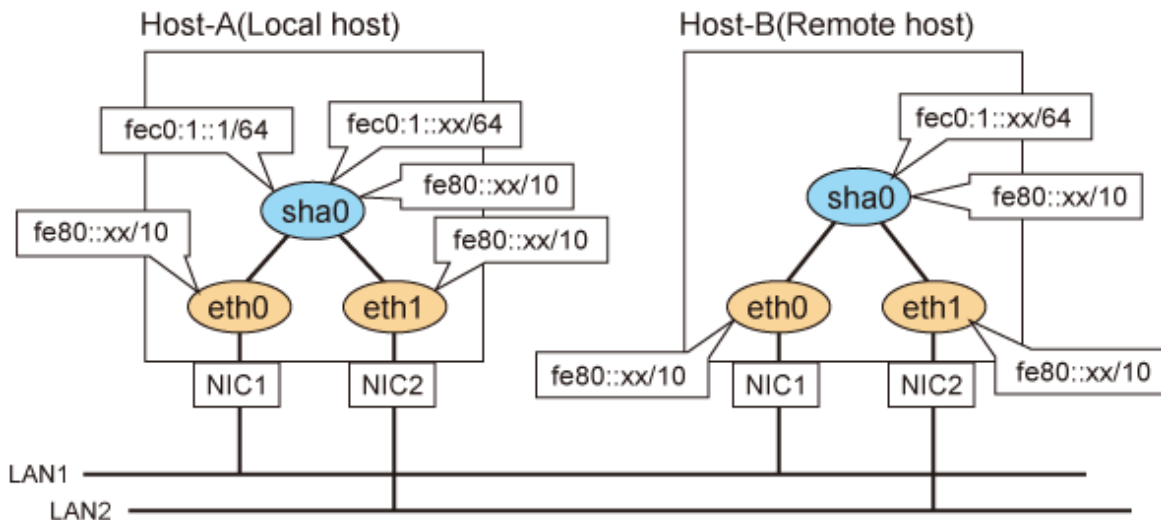
```
/sbin/shutdown -r now
```

## 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 in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define an address for logical virtual IP and host name in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta1  # HOST-A Logical virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 4) Creating of logical virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::1/64
```

### 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



#### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

### 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 5) Reboot

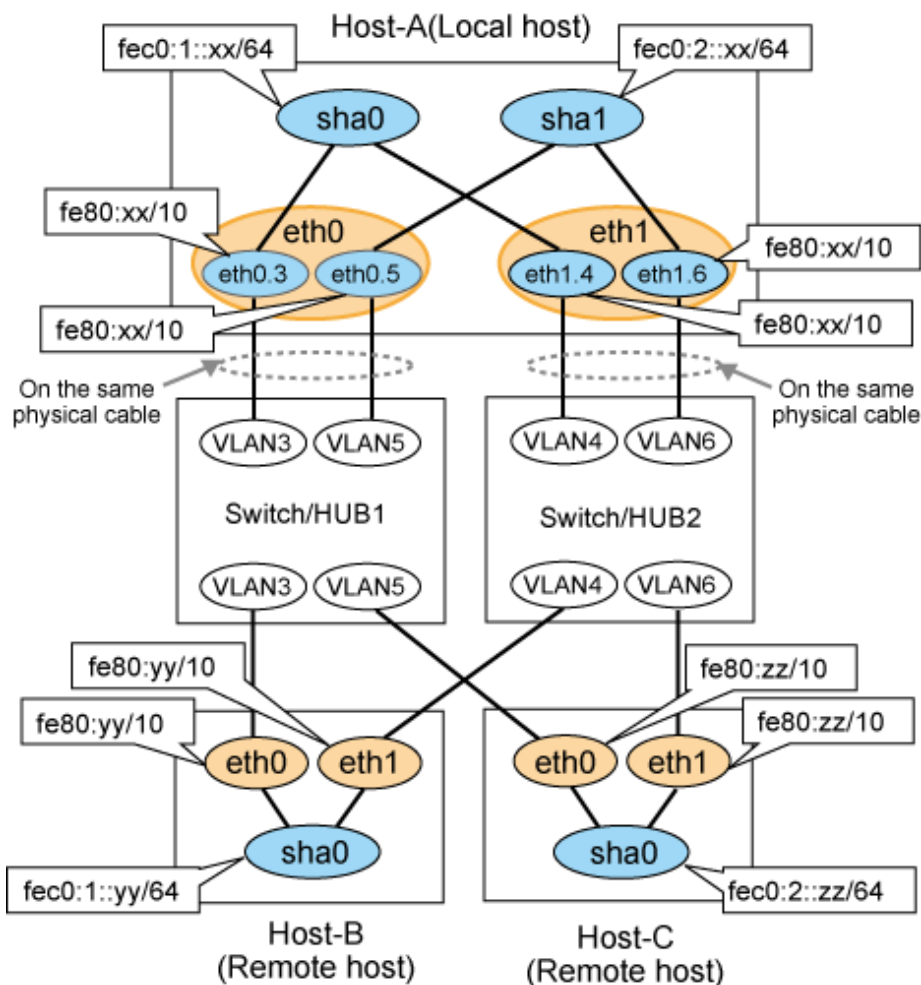
Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## 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.



## [HOST-A]

### 1) Setting up the system

1-1) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 3,4,5,6) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.3

```
DEVICE=eth0.3
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.4

```
DEVICE=eth1.4
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.5

```
DEVICE=eth0.5
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.6

```
DEVICE=eth1.6
BOOTPROTO=static
ONBOOT=yes
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0.3, eth0.5, eth1.4 and eth1.6 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0.3,eth1.4
```

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t eth0.5,eth1.6
```

## 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64         # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
interface sha1
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
```



```

        prefix fec0:2::0/64          # Sending Prefix fec0:2::0/64 from shal
        {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
        };
};

```

## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file.

For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

## 5) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.

## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet

```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet

```

1-2) When the system is RHEL, on `/etc/sysconfig/network` file, define a statement allows the system to load IPv6 module.

```

NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no

```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify `eth0` and `eth1` are active using `ifconfig` command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

### 5) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-C]

### 1) Setting up the system

1-1) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-2) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:2::0/64         # Sending Prefix fec0:2::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

## 5) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## 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 in the figure below are assigned automatically by the automatic address configuration.

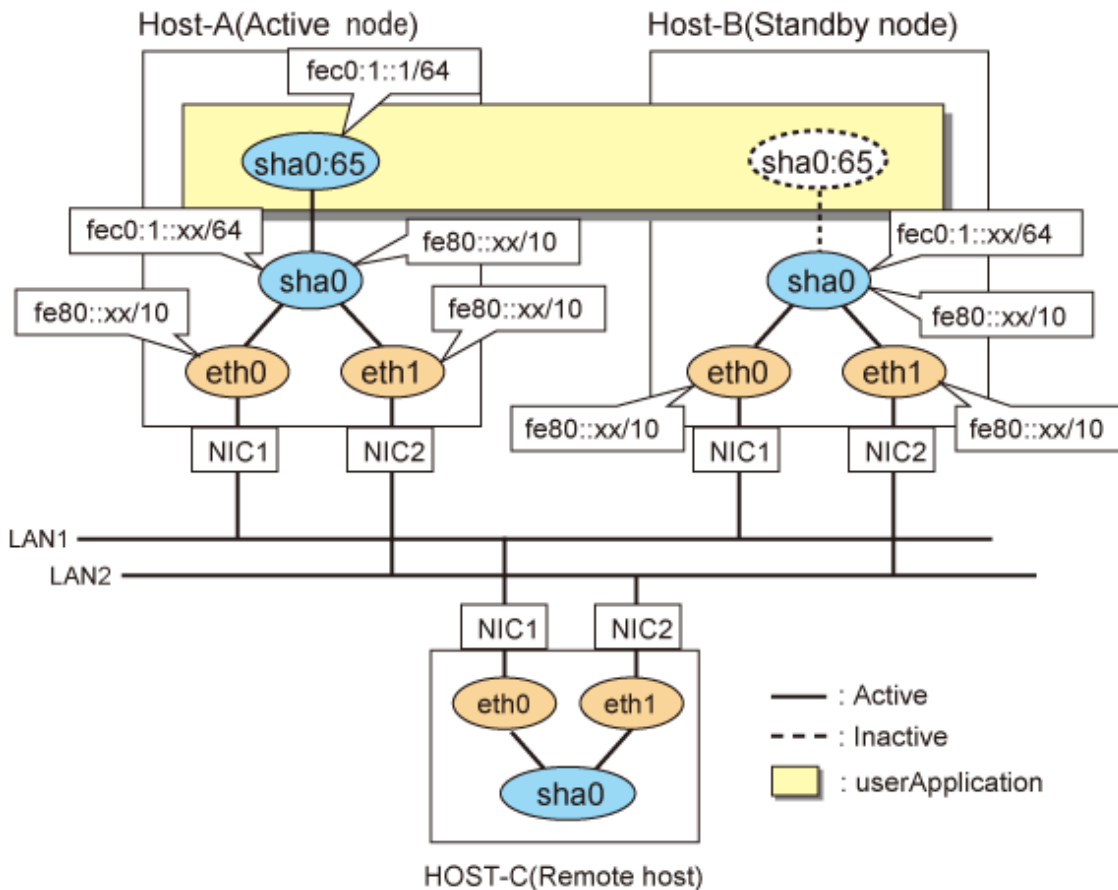
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.2.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta1  # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application.

Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the figure below are assigned automatically by the automatic address configuration.

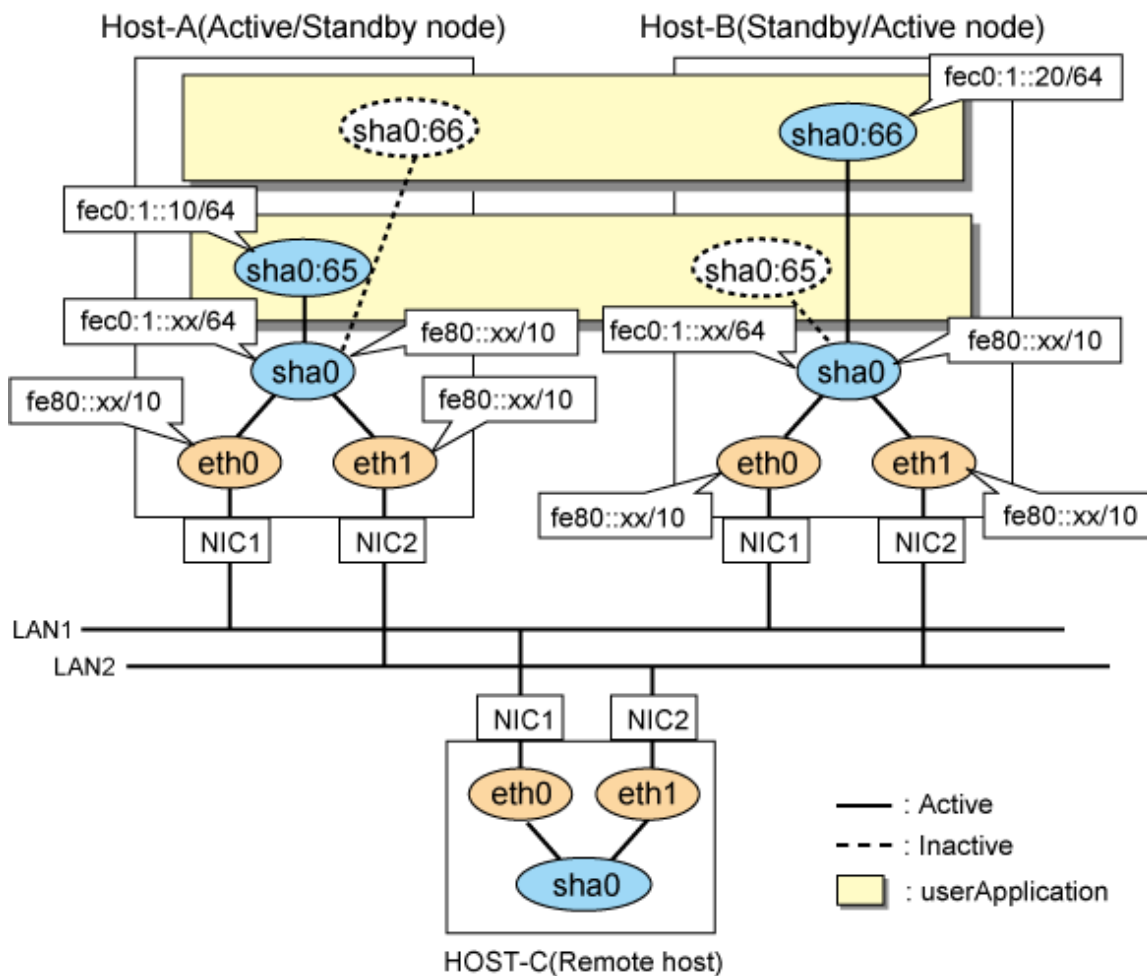
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.2.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::10    v6hosta1  # HOST-A/B Takeover virtual IP
fec0:1::20    v6hostb1  # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1



```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating 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
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 4) Creating 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
```

### 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
    }
}
```

```
};  
    AdvRouterAddr on;  
};
```

## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

### 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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, and yy in the IP address of the figure below are assigned automatically by the automatic address configuration.

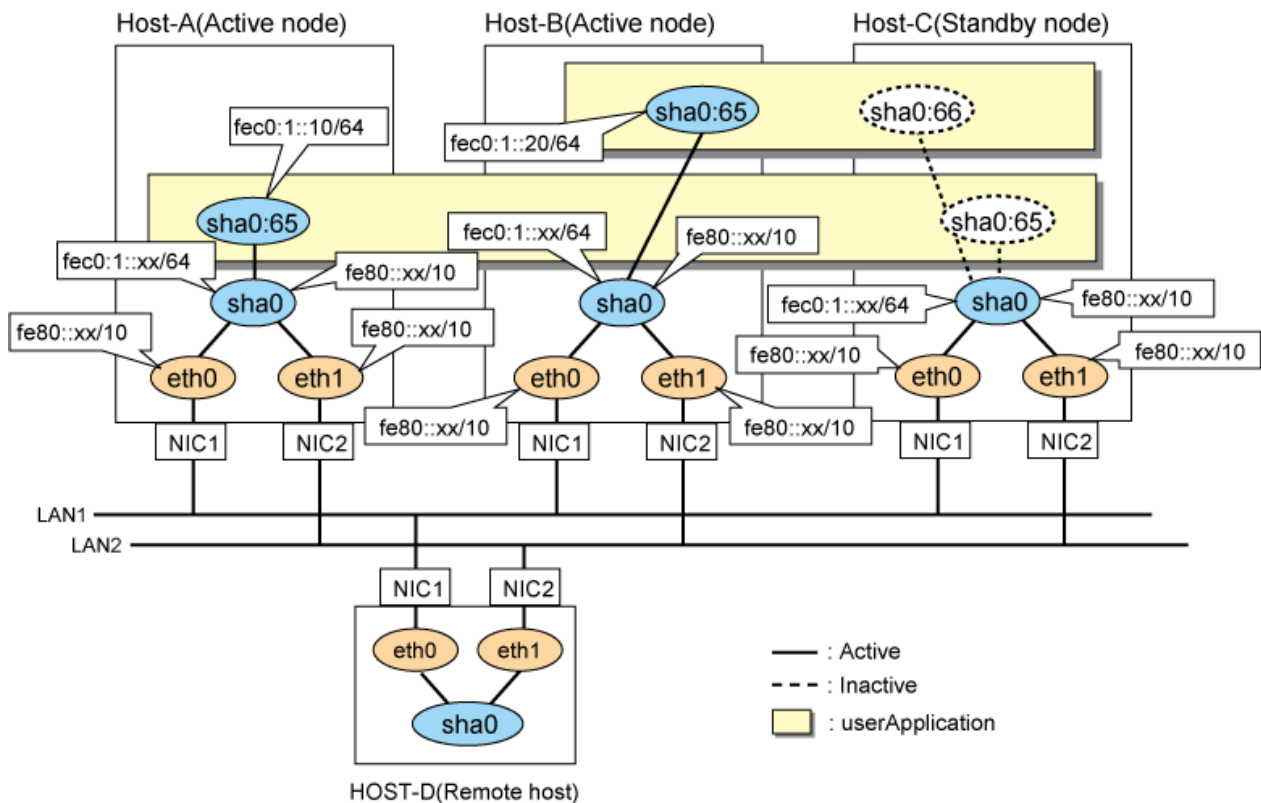
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.2.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::10      v6hosta1  # HOST-A/C Takeover virtual IP
fec0:1::20      v6hostb1  # HOST-B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::10/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64       # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::20/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64         # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-C]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.



## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the `/etc/sysconfig/network` file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify `eth0` and `eth1` are enabled as an IPv6 interface using `ifconfig` command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 4) Creating 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
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

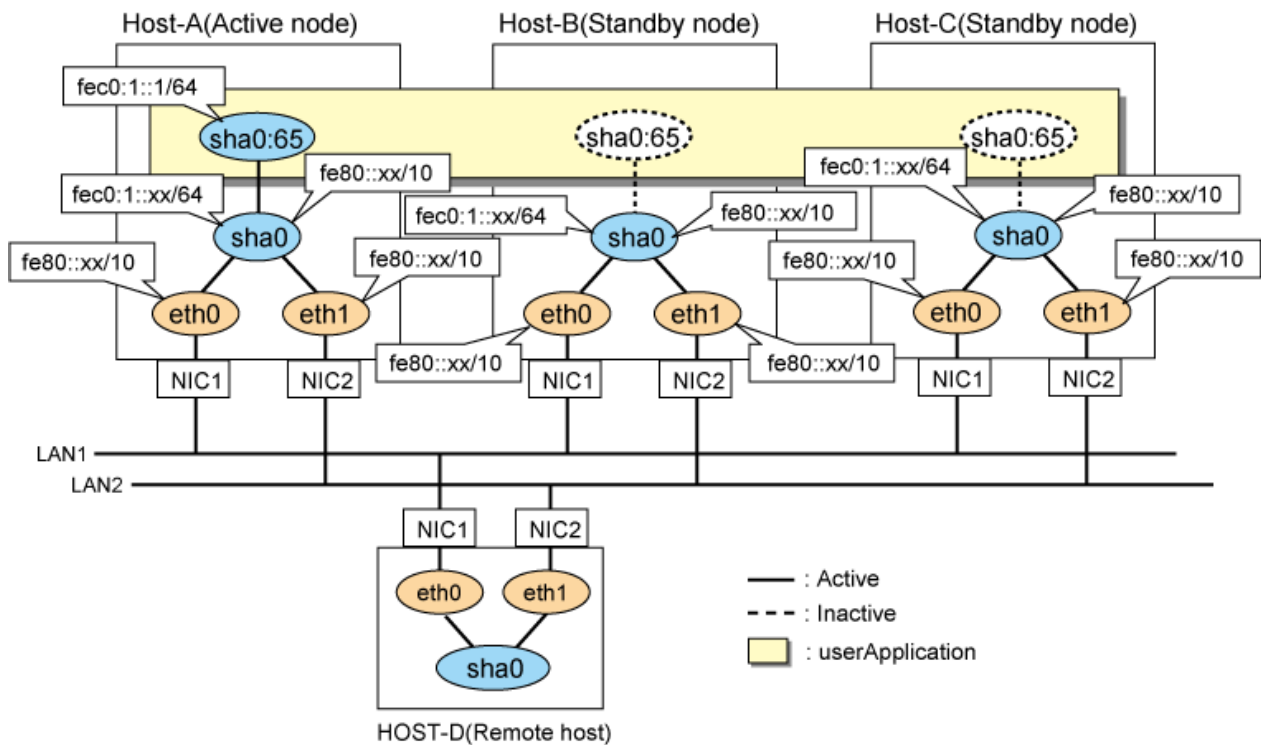
For configuring the cluster system, refer to the Cluster system manual.

In this section, description of private LAN is omitted.

The dotted line indicates that the interface is inactive.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.2.1 Example of the Single system](#)".





## [HOST-A]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta1    # HOST-A/B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-C]

### 1) Setting up the system

1-1) Define an address for takeover virtual IP and host name in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 4) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fec0:1::1/64
```

### 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```

interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};

```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

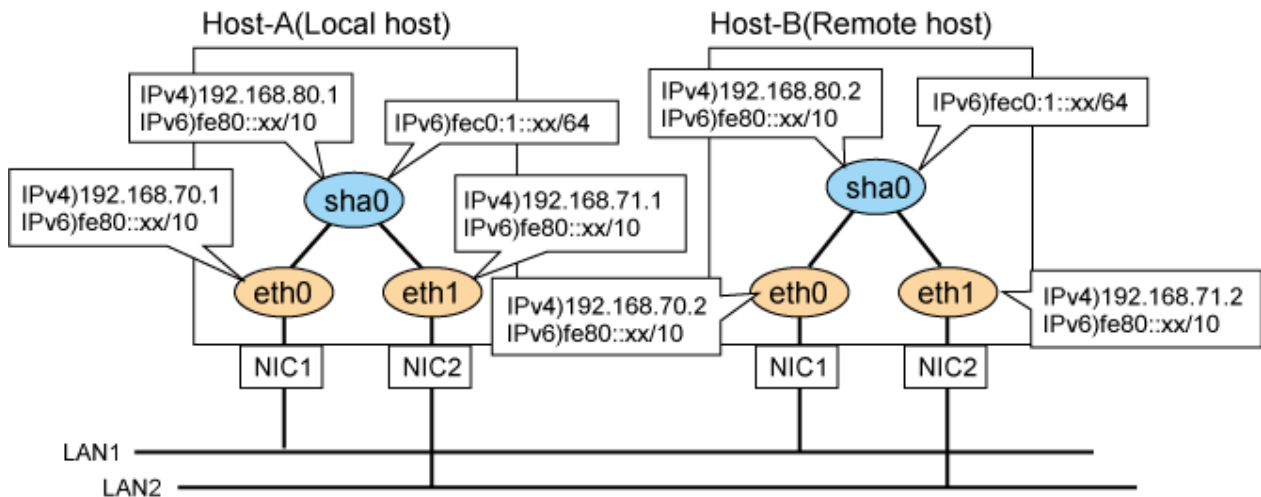
## B.3 Example of configuring Fast switching mode (IPv4/IPv6)

### 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 in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
```

```
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
```



```

MaxRtrAdvInterval 10;
prefix fec0:1::0/64      # Sending Prefix fec0:1::0/64 from sha0
{
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr on;
};
};

```

## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

Run the following command and reboot the system.

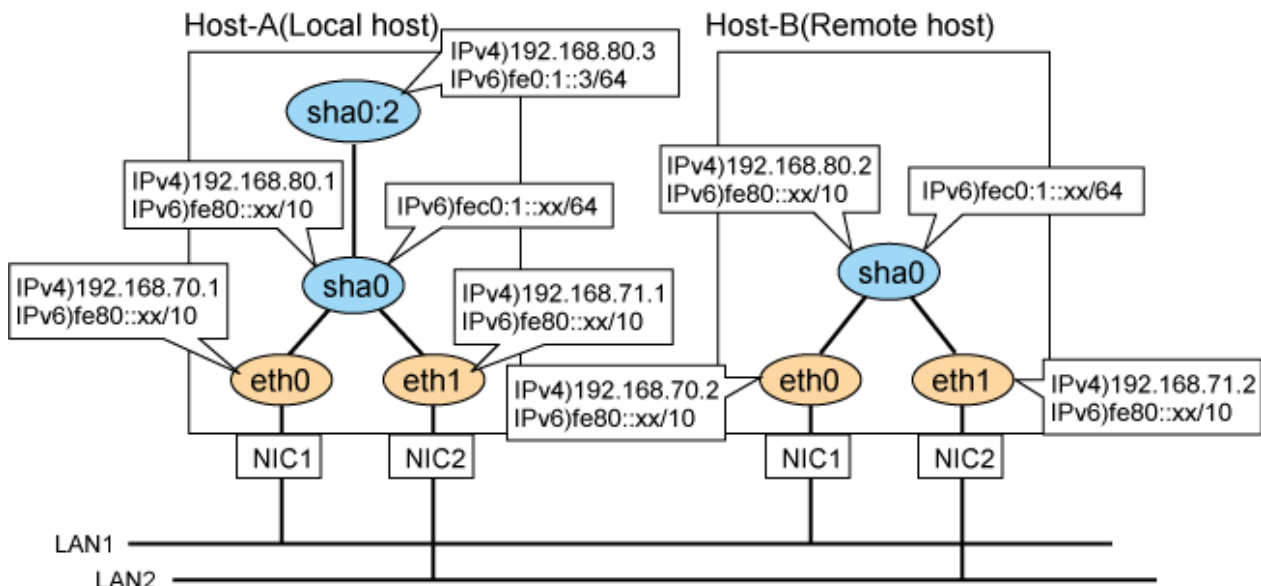
```
/sbin/shutdown -r now
```

## 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 in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "3.2.2 Network configuration".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```

192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP

```

```

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
192.168.71.2    host22   # HOST-B Physical IP
192.168.80.2    hostb    # HOST-B Virtual IP
fec0:1::3      v6hosta1  # HOST-A Logical virtual IP

```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet

```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```

NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no

```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```

/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1

```

## 5) Creating of logical virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0:2 -i fec0:1::3/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0  
{  
    AdvSendAdvert on;          # Sending router advertisements  
    MinRtrAdvInterval 3;  
    MaxRtrAdvInterval 10;  
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0  
    {  
        AdvOnLink on;  
        AdvAutonomous on;  
        AdvRouterAddr on;  
    };  
};
```



### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.70.255  
IPADDR=192.168.70.2  
NETMASK=255.255.255.0  
NETWORK=192.168.70.0  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 6) Reboot

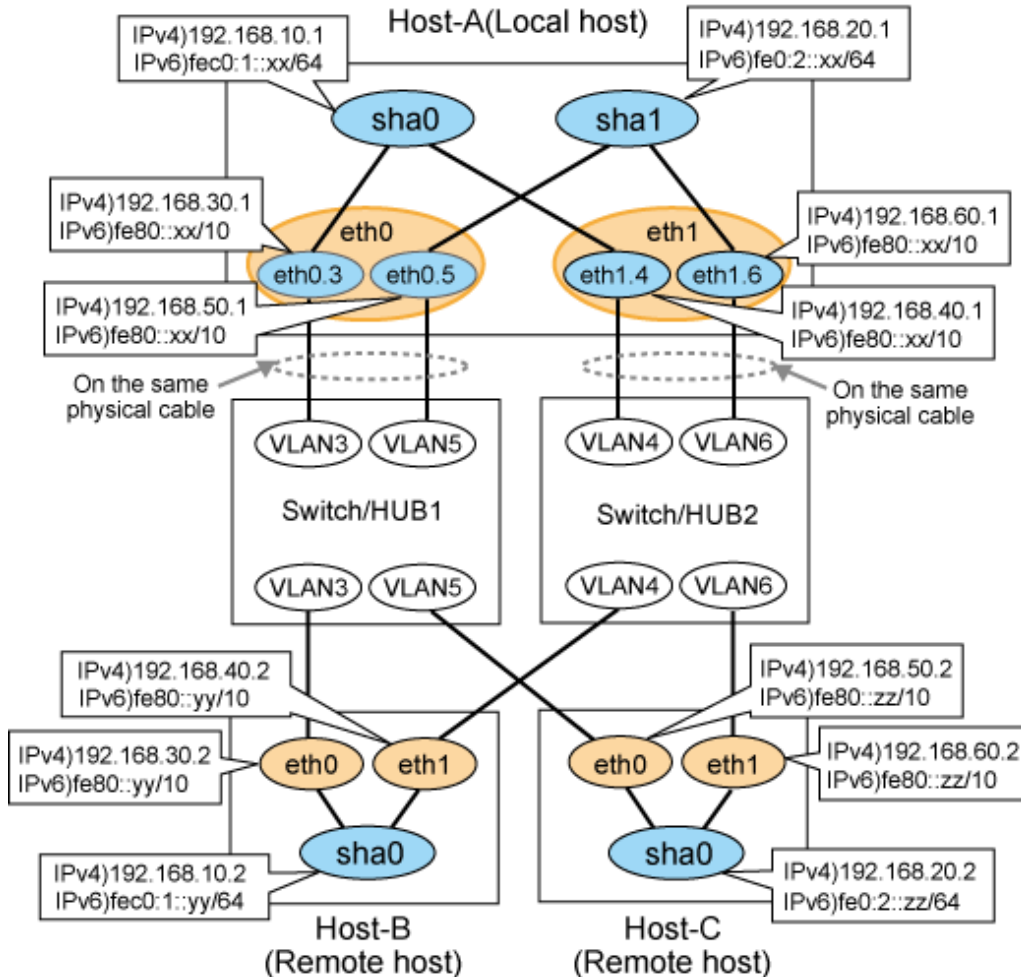
Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

### 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.



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 3,4,5,6) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.3

```
DEVICE=eth0.3
BOOTPROTO=static
BROADCAST=192.168.30.255
IPADDR=192.168.30.1
NETMASK=255.255.255.0
NETWORK=192.168.30.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.4

```
DEVICE=eth1.4
BOOTPROTO=static
BROADCAST=192.168.40.255
IPADDR=192.168.40.1
NETMASK=255.255.255.0
NETWORK=192.168.40.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.5

```
DEVICE=eth0.5
BOOTPROTO=static
BROADCAST=192.168.50.255
IPADDR=192.168.50.1
NETMASK=255.255.255.0
NETWORK=192.168.50.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.6

```
DEVICE=eth1.6
BOOTPROTO=static
BROADCAST=192.168.60.255
IPADDR=192.168.60.1
NETMASK=255.255.255.0
NETWORK=192.168.60.0
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0.3, eth0.5, eth1.4 and eth1.6 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.10.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.20.0 -m 255.255.255.0
```

## 4) Creating of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.1 -t eth0.3,eth1.4
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m t -i 192.168.20.1 -t eth0.5,eth1.6
```

## 5) Creating of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0.3,eth1.4
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m t -t eth0.5,eth1.6
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64         # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
interface sha1
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:2::0/64         # Sending Prefix fec0:2::0/64 from sha1
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

```
};  
};
```

## Note

In the 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. Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file.

For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

## 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.

## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.30.255  
IPADDR=192.168.30.2  
NETMASK=255.255.255.0  
NETWORK=192.168.30.0  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```
DEVICE=eth1  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.40.255  
IPADDR=192.168.40.2  
NETMASK=255.255.255.0  
NETWORK=192.168.40.0  
ONBOOT=yes  
TYPE=Ethernet
```

1-3) When the system is RHEL, on `/etc/sysconfig/network` file, define a statement allows the system to load IPv6 module.



```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.10.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64         # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

# [HOST-C]

## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.50.255
IPADDR=192.168.50.2
NETMASK=255.255.255.0
```

```
NETWORK=192.168.50.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.60.255
IPADDR=192.168.60.2
NETMASK=255.255.255.0
NETWORK=192.168.60.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.20.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:2::0/64         # Sending Prefix fec0:2::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

## 6) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## 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 in the figure below are assigned automatically by the automatic address configuration.

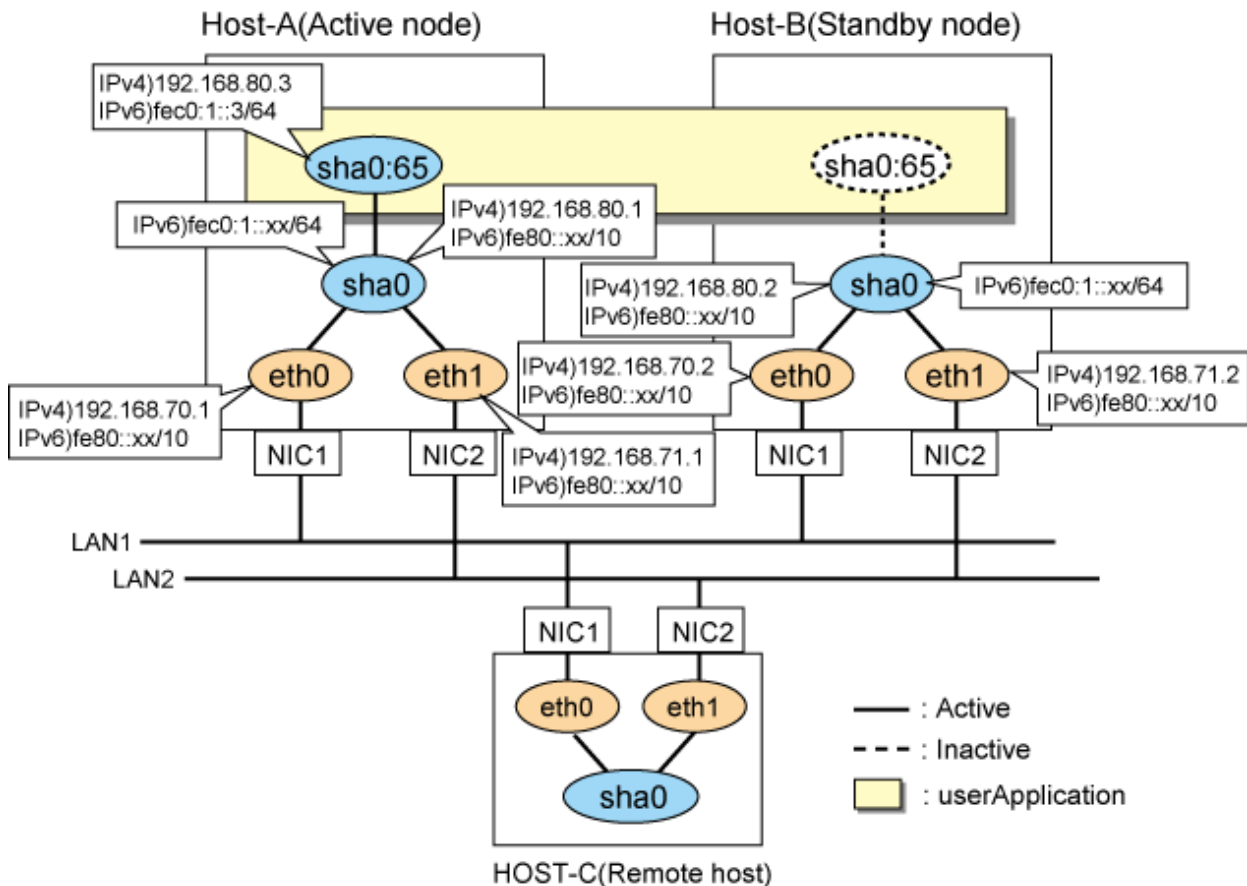
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.3.1 Example of the Single system](#)".



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/hosts` file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.3    hosta1 # HOST-A/B Takeover virtual IP
fec0:1::3      v6hosta1 # HOST-A/B Takeover virtual IP
```

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3, fec0:1::3/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
```

```

        AdvSendAdvert on;          # Sending router advertisements
        MinRtrAdvInterval 3;
        MaxRtrAdvInterval 10;
        prefix fec0:1::0/64      # Sending Prefix fec0:1::0/64 from sha0
        {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
        };
};

```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

## 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.



## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0

```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3, fec0:1::3/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

## 7) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the figure below are assigned automatically by the automatic address configuration.

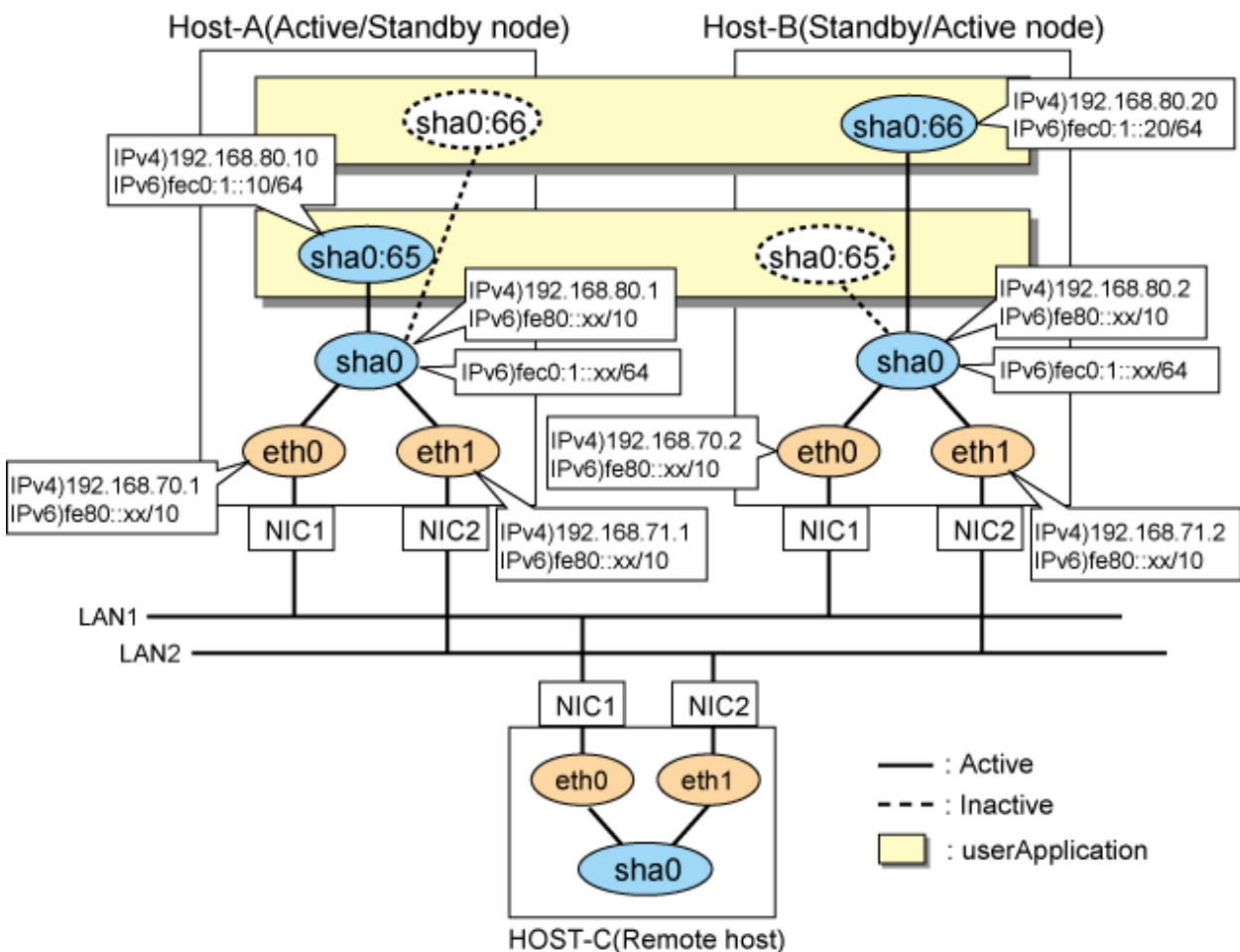
For the network configuration other than GLS, refer to "3.2.2 Network configuration".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "B.3.1 Example of the Single system".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```

192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.80.10   hosta1  # HOST-A/B Takeover virtual IP
192.168.80.20   hostb1  # HOST-A/B Takeover virtual IP
fec0:1::10      v6hosta1 # HOST-A/B Takeover virtual IP
fec0:1::20      v6hostb1 # HOST-A/B Takeover virtual IP

```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet

```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```

NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no

```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```



#### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

#### 5) Creating 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
```

#### 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0  
{  
    AdvSendAdvert on;          # Sending router advertisements  
    MinRtrAdvInterval 3;  
    MaxRtrAdvInterval 10;  
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0  
    {  
        AdvOnLink on;  
        AdvAutonomous on;  
        AdvRouterAddr on;  
    };  
};
```



#### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

#### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

### [HOST-B]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.70.255  
IPADDR=192.168.70.2
```

```
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating 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
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64       # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application.

Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the IP address of the figure below are assigned automatically by the automatic address configuration.

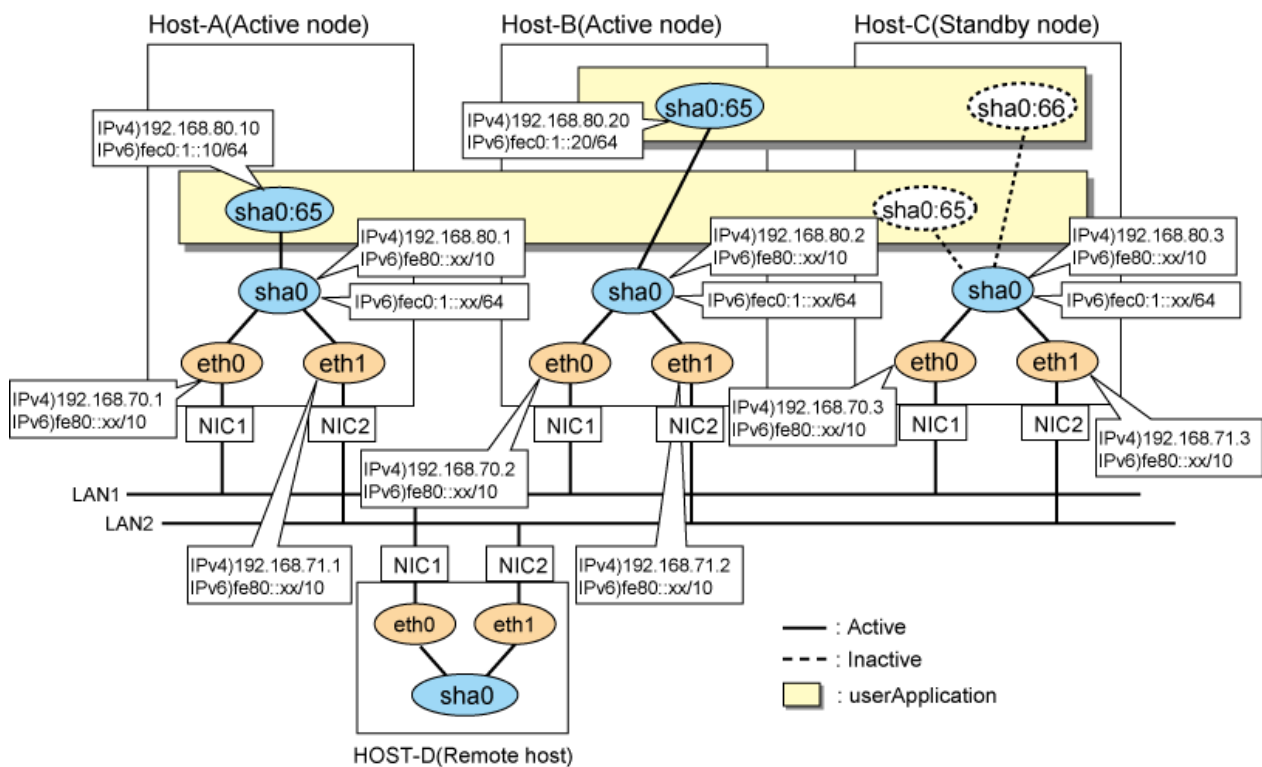
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.3.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP
192.168.71.3    host32 # HOST-C Physical IP
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.10   hosta1 # HOST-A/C Takeover virtual IP
192.168.80.20   hostb1 # HOST-B/C Takeover virtual IP
fec0:1::10      v6hosta1 # HOST-A/C Takeover virtual IP
fec0:1::20      v6hostb1 # HOST-B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
```

```
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10,fec0:1::10/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.



## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the `/etc/sysconfig/network` file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20, fec0:1::20/64
```

### 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0  
{  
    AdvSendAdvert on;          # Sending router advertisements  
    MinRtrAdvInterval 3;  
    MaxRtrAdvInterval 10;  
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0  
    {  
        AdvOnLink on;  
        AdvAutonomous on;  
        AdvRouterAddr on;  
    };  
};
```



#### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-C]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating 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
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
```



```

{
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr on;
};
};

```

## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the figure below are assigned automatically by the automatic address configuration.

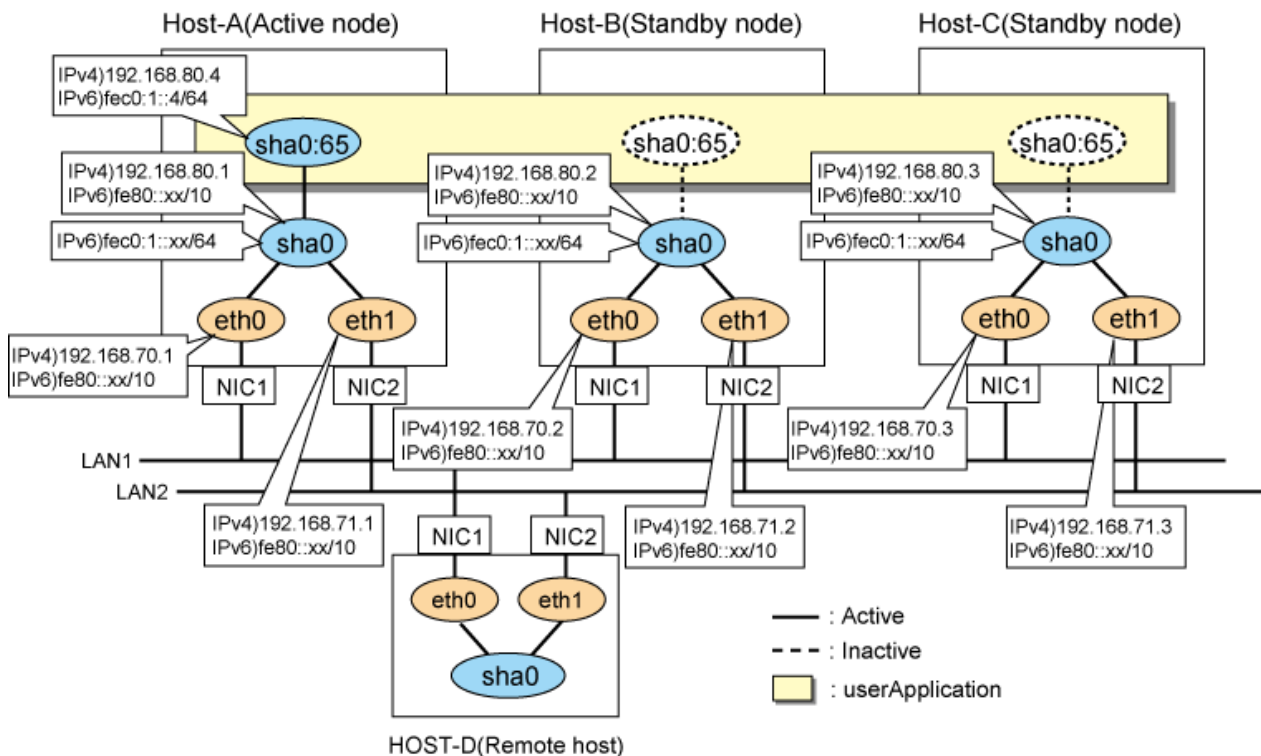
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.

You need at least a remote host using Fast switching mode other than a node used for configuring a Cluster system. For details on configuring a remote host, refer to "[B.3.1 Example of the Single system](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    host11 # HOST-A Physical IP
192.168.71.1    host12 # HOST-A Physical IP
192.168.80.1    hosta  # HOST-A Virtual IP
192.168.70.2    host21 # HOST-B Physical IP
192.168.71.2    host22 # HOST-B Physical IP
192.168.80.2    hostb  # HOST-B Virtual IP
192.168.70.3    host31 # HOST-C Physical IP
192.168.71.3    host32 # HOST-C Physical IP
192.168.80.3    hostc  # HOST-C Virtual IP
192.168.80.4    hosta1 # HOST-A/B/C Takeover virtual IP
fec0:1::4      v6hosta1 # HOST-A/B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
```

```
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4, fec0:1::4/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;           # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64         # Sending Prefix fec0:1::0/64 from sha0
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```



## Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

## 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Configure `/etc/sysconfig/network-scripts/ifcfg-ethX` (X is 0,1) file as follows.



## Note

The following setting example (`/etc/sysconfig/network-scripts/ifcfg-ethX`) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth0`

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of `/etc/sysconfig/network-scripts/ifcfg-eth1`

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the `/etc/sysconfig/network` file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

### 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4, fec0:1::4/64
```

### 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0  
{  
    AdvSendAdvert on;          # Sending router advertisements  
    MinRtrAdvInterval 3;  
    MaxRtrAdvInterval 10;  
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0  
    {  
        AdvOnLink on;  
        AdvAutonomous on;  
        AdvRouterAddr on;  
    };  
};
```



#### Note

In the 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.

Depending on the version of radvd, kernel parameter(net.ipv6.conf.all.forwarding=1) must be defined in /etc/sysctl.conf file. For details on /etc/radvd.conf, refer to the radvd.conf(5), radvd(8) manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-C]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth1 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m t -t eth0,eth1
```

## 5) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4,fec0:1::4/64
```

## 6) Setting up IPv6 routers

Create /etc/radvd.conf file and set the following.

```
interface sha0
{
    AdvSendAdvert on;          # Sending router advertisements
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 10;
    prefix fec0:1::0/64        # Sending Prefix fec0:1::0/64 from sha0
    {
```

```
AdvOnLink on;  
AdvAutonomous on;  
AdvRouterAddr on;  
};  
};
```

### Note

In the 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.

Depending on the version of radvd, kernel parameter(`net.ipv6.conf.all.forwarding=1`) must be defined in `/etc/sysctl.conf` file. For details on `/etc/radvd.conf`, refer to the `radvd.conf(5)`, `radvd(8)` manual.

### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

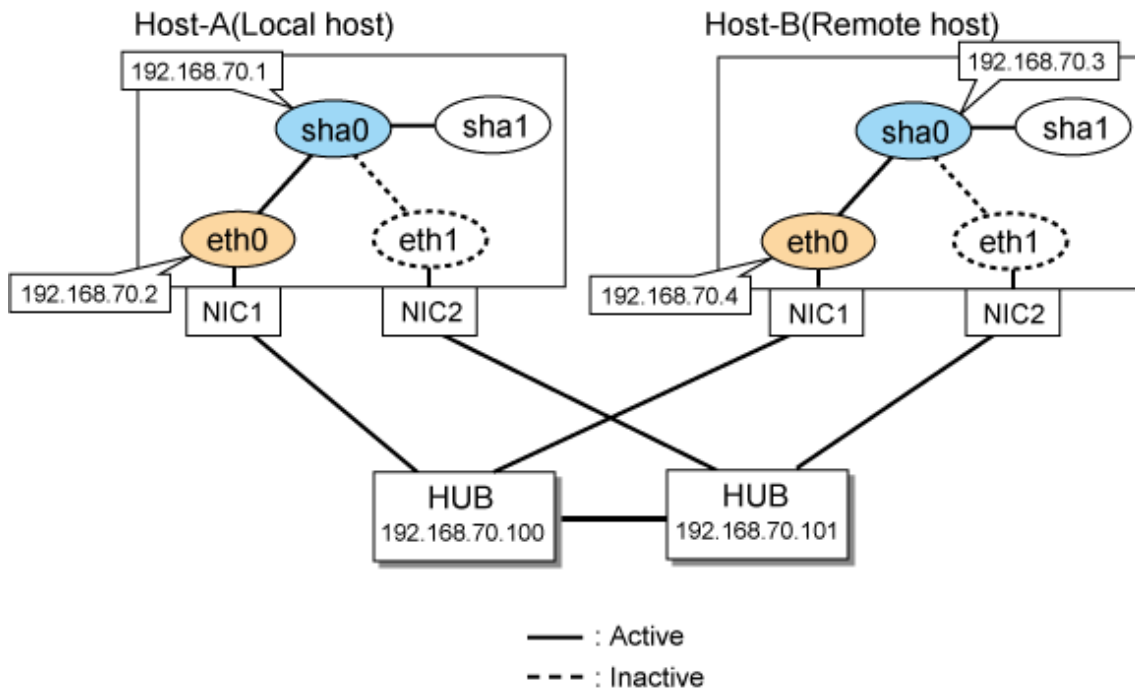
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## 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.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1



```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

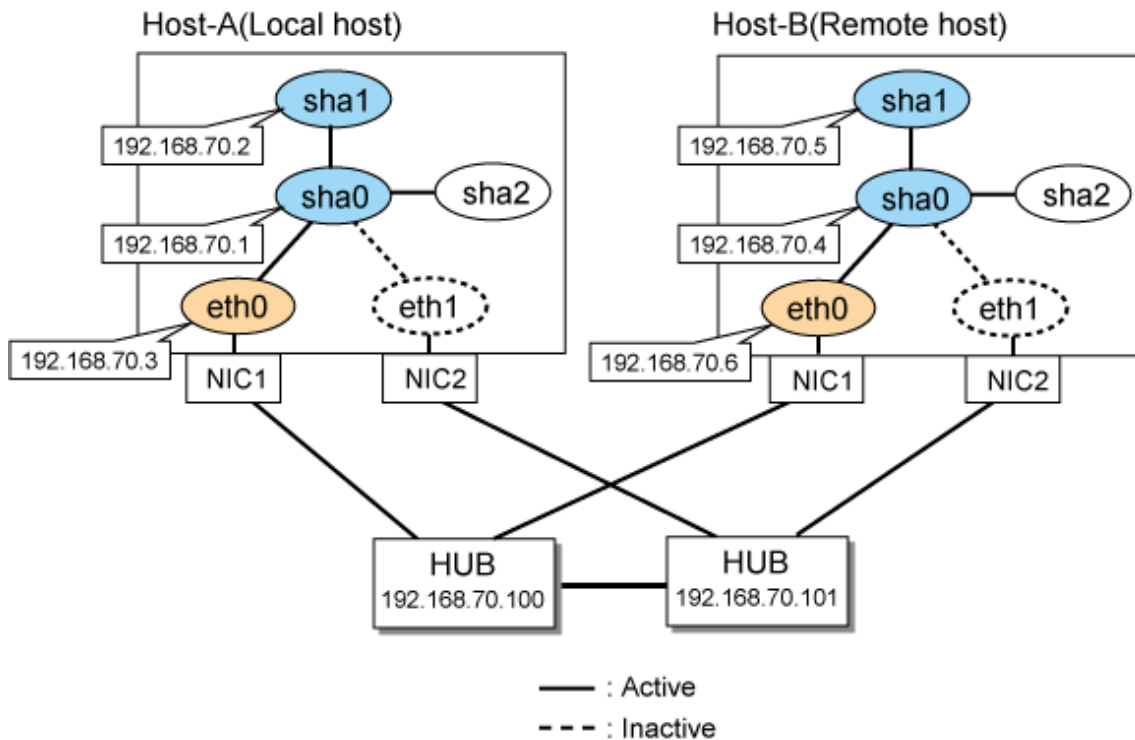
## 8) Starting the HUB monitoring function

```
/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.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta1 # HOST-A Virtual IP
192.168.70.2    hosta2 # HOST-A Virtual IP
192.168.70.3    host11 # HOST-A Physical IP
192.168.70.4    hostb1 # HOST-B Virtual IP
192.168.70.5    hostb1 # HOST-B Virtual IP
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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

## 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.6
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 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) Activating of virtual interface

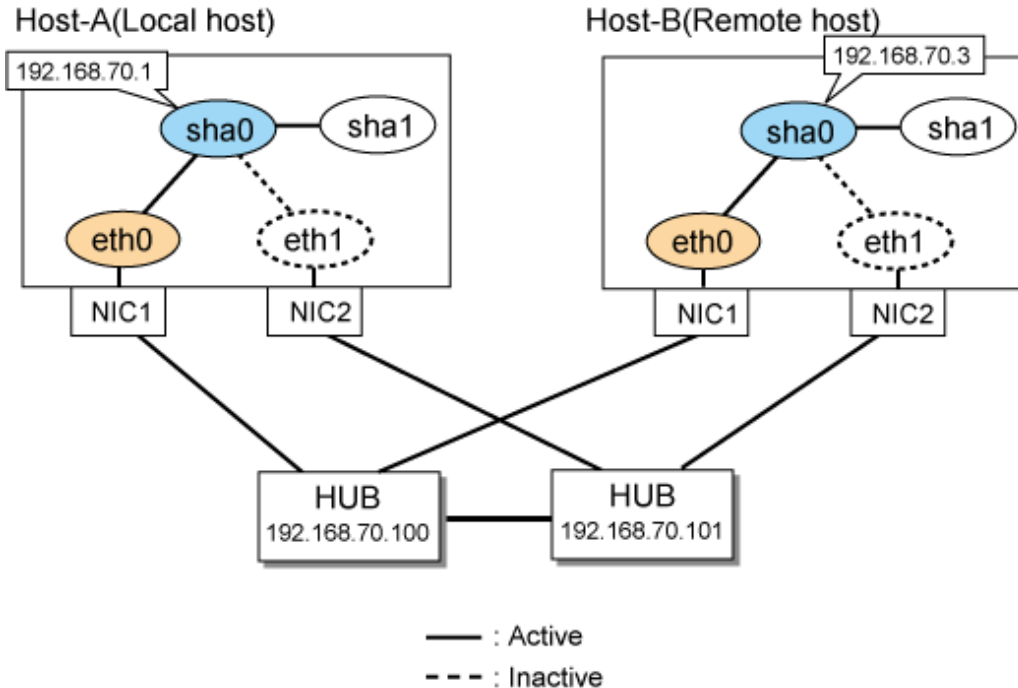
```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

## 8) Starting the HUB monitoring function

### B.4.3 Example of the Single system in Takeover physical IP address (pattern II)

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
```

```
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t eth0,eth1
```

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 8) Starting the HUB monitoring function

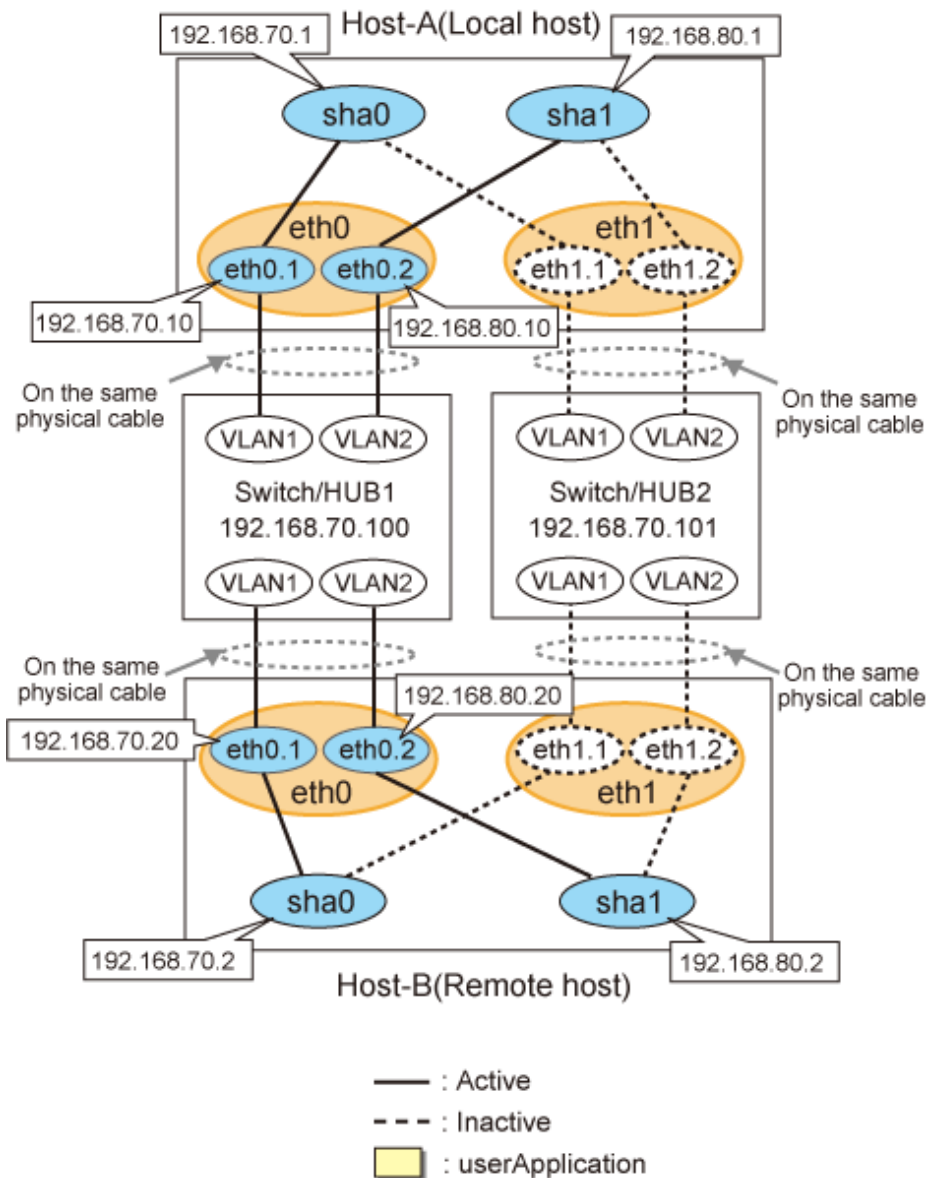
```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## B.4.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching)

---

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/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 Switch/HUB IP
192.168.70.101 swhub2   # Secondary Switch/HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.10
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.10
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
eth0.2,eth1.2
```



### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

## 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 HUB monitoring function (Synchronous switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

## 7) 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
```

## 8) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined information is the same as for HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.20
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.20
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0  
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t  
eth0.1,eth1.1  
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t  
eth0.2,eth1.2
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

#### 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 HUB monitoring function (Synchronous switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

#### 7) 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
```

#### 8) Reboot

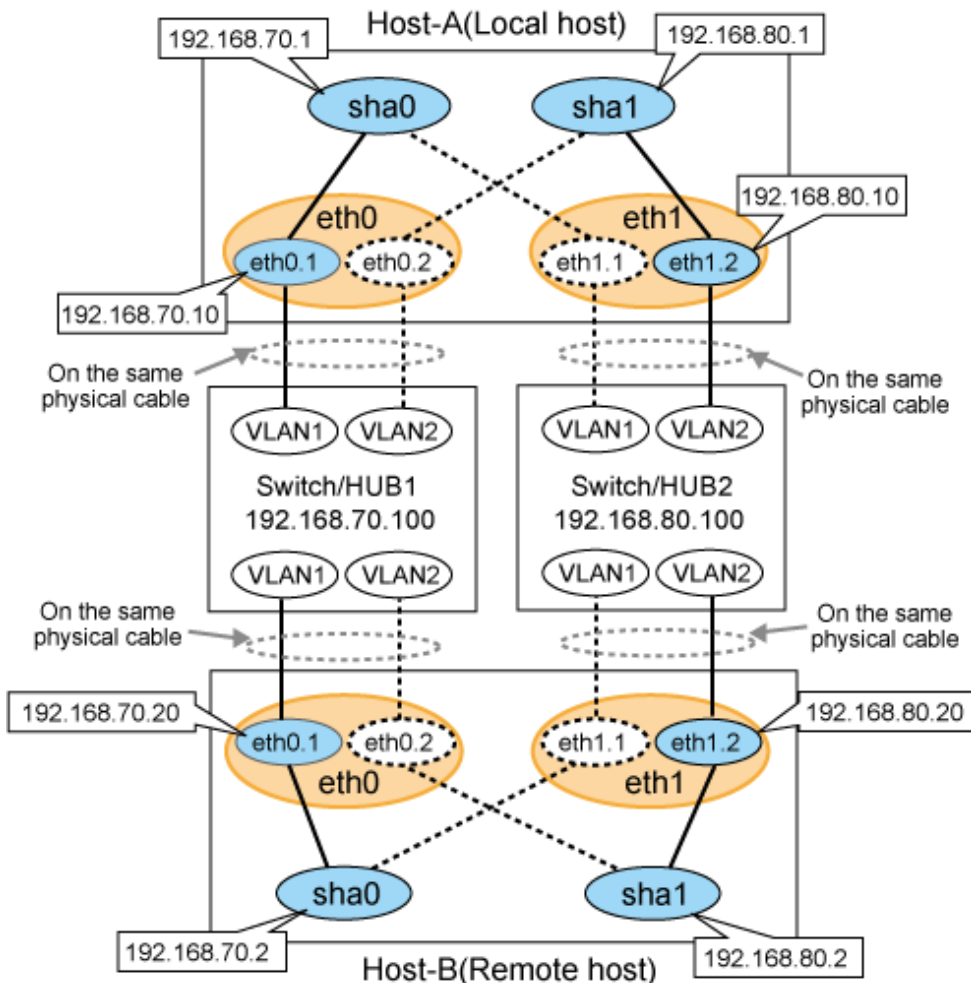
Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## B.4.5 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching)

---

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/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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.10
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.10
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.10 -t
eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.10 -t
eth1.2,eth0.2
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

### 5) 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
```

### 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 and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```



```
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.20
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.20
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.20 -t
eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.20 -t
eth1.2,eth0.2
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

### 5) 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
```

### 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
```

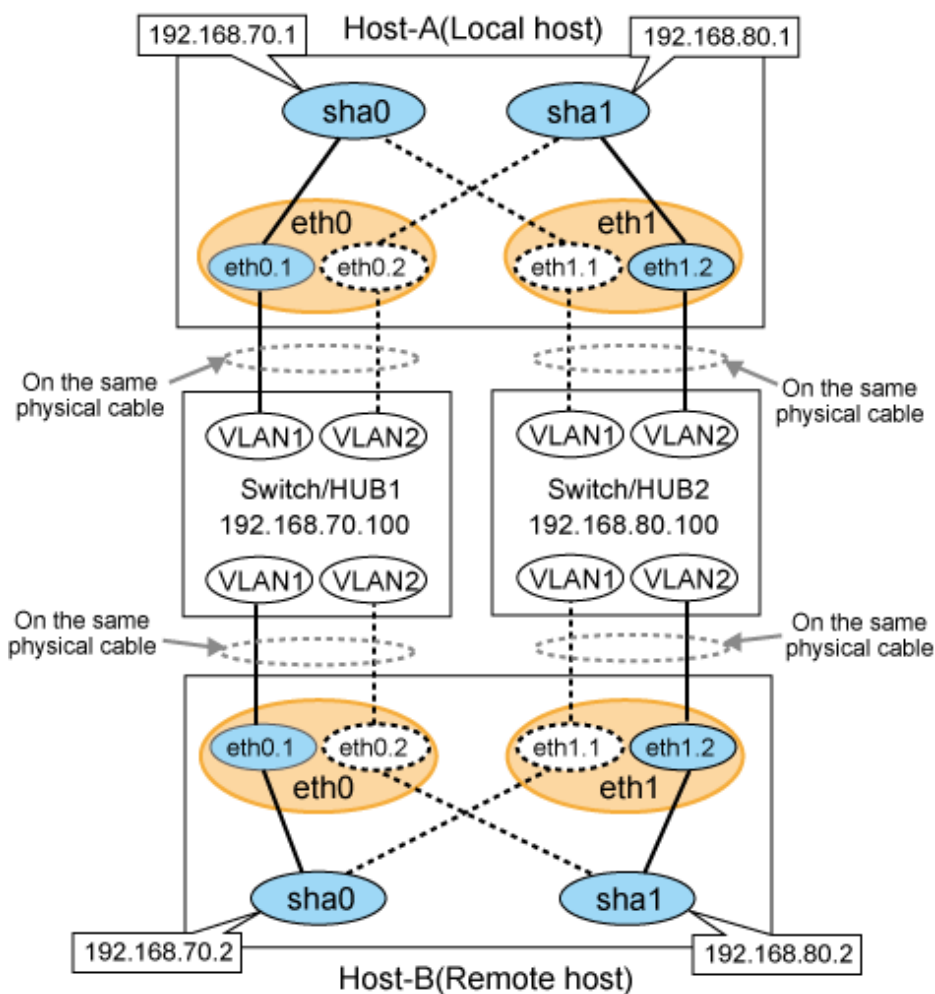
### 7) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## B.4.6 Configuring virtual interfaces with tagged VLAN (Physical IP takeover, Asynchronous switching)

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/hosts file.

```
192.168.70.1    hosta1    # HOST-A Virtual IP
192.168.80.1    hosta2    # HOST-A Virtual IP
192.168.70.2    hostb1    # HOST-B Virtual IP
192.168.80.2    hostb2    # HOST-B Virtual IP
192.168.70.100  swhub1    # Switch/HUB1 IP
192.168.80.100  swhub2    # Switch/HUB2 IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.1
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

- 1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m e -i 192.168.80.1 -t eth1.2,eth0.2
```



## Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

## 5) 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
```

## 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 and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.2
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

1-4) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.2 -t eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m e -i 192.168.80.2 -t eth1.2,eth0.2
```



### Note

Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

## 5) 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
```

## 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 and reboot the system.

```
/sbin/shutdown -r now
```

## B.4.7 Example of the Cluster system (1:1 Standby)

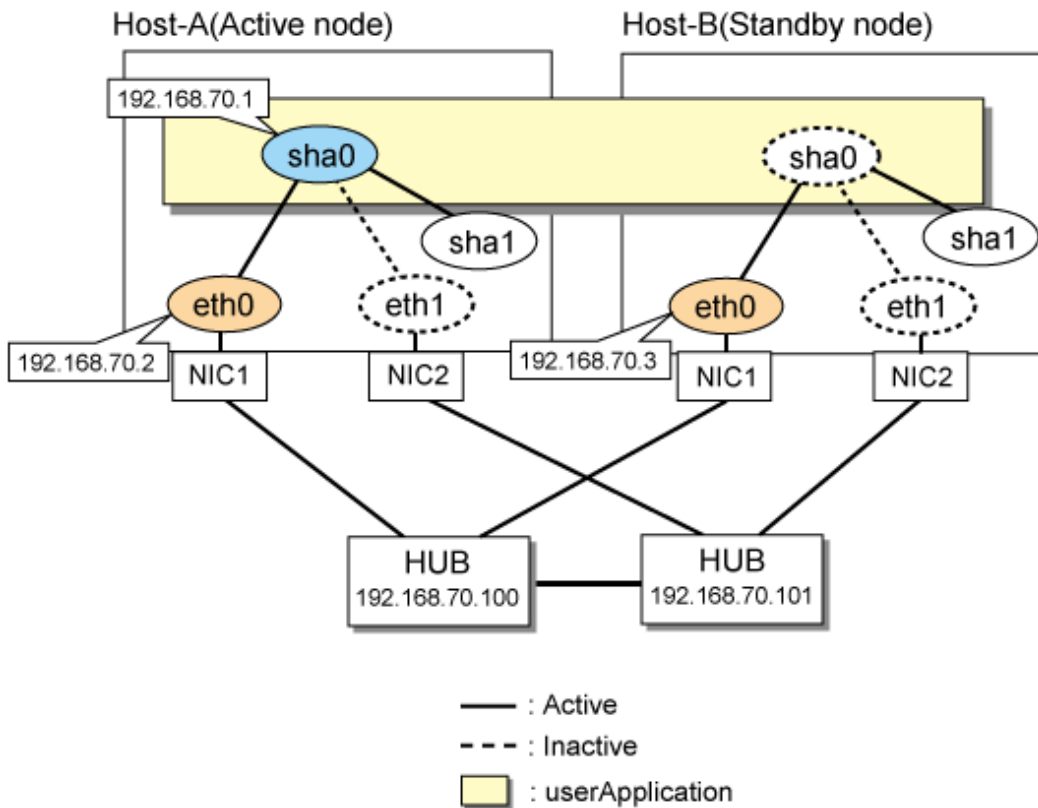
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover 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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".



- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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/FJShanet/usr/sbin/strptl -n sha1
```

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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) without NIC sharing

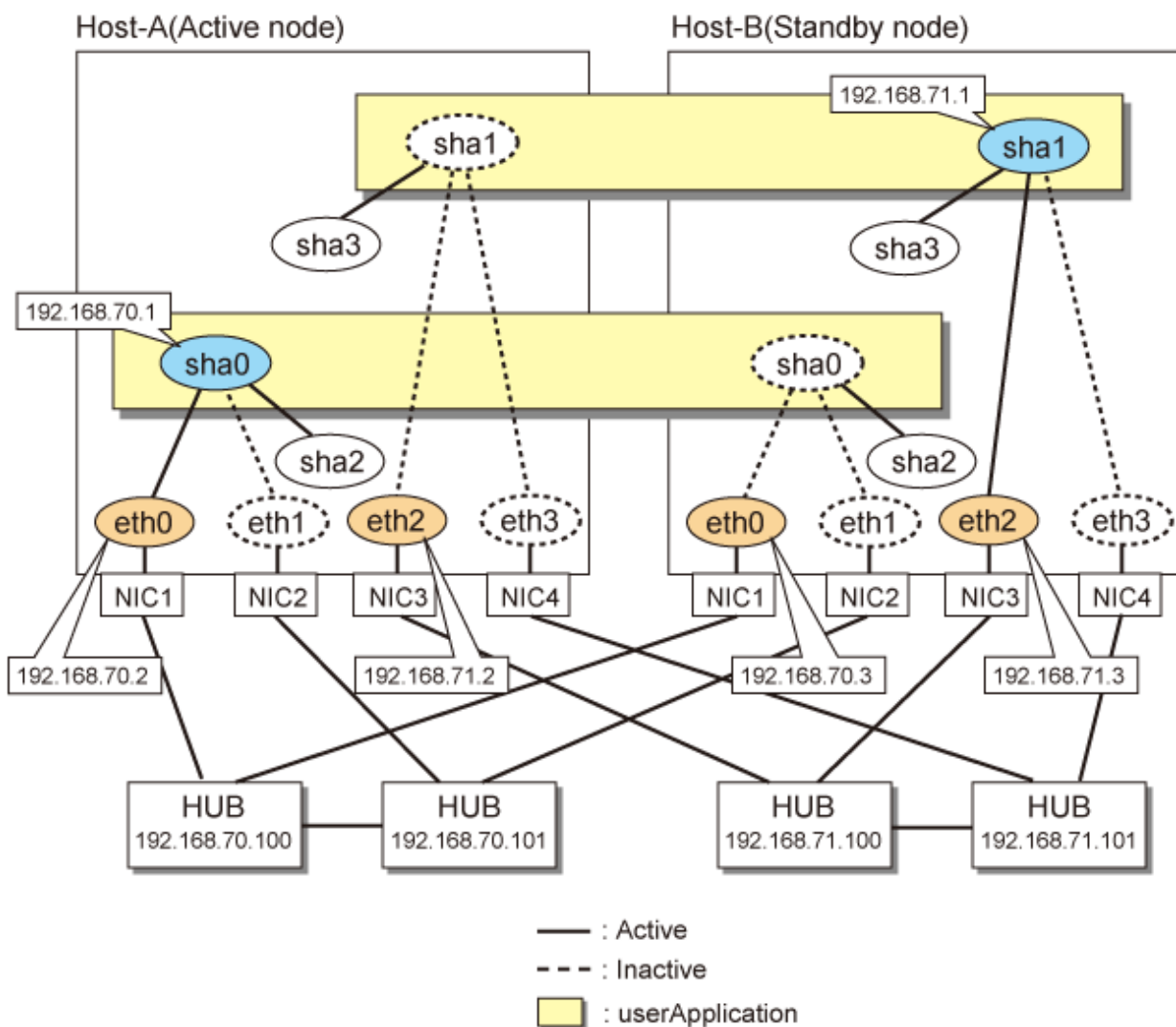
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.71.1    hostb    # HOST-A/B Virtual IP (Takeover IP2)
192.168.71.2    host12   # HOST-A Physical IP
192.168.71.3    host22   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
192.168.71.100  swhub3   # Primary HUB IP
192.168.71.101  swhub4   # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth2 are enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t eth2,eth3
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0 and /etc/sysconfig/network-scripts/ifcfg-eth2.

## 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 create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

## 6) 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
```

## 7) Creating 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
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system make sure eth0 and eth2 are enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
```

#### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t eth2,eth3
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0 and /etc/sysconfig/network-scripts/ifcfg-eth2.

#### 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 create -n sha1 -p 192.168.71.100,192.168.71.101 -b off
```

#### 6) 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
```

#### 7) Creating 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
/opt/FJSVhanet/usr/sbin/strptl -n sha3
```

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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 (Mutual standby) with NIC sharing

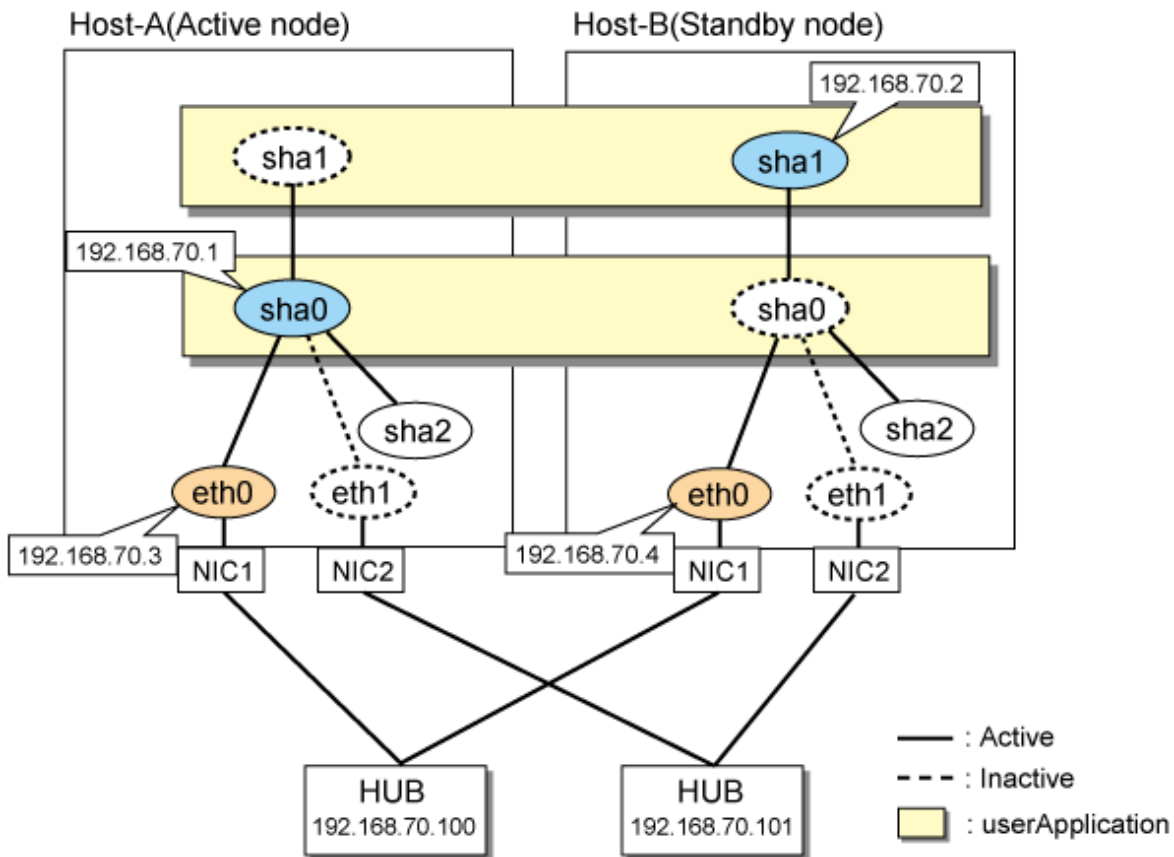
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2    hostb    # HOST-A/B Virtual IP (Takeover IP2)
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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.



1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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 RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 Takeover physical IP address (pattern I)

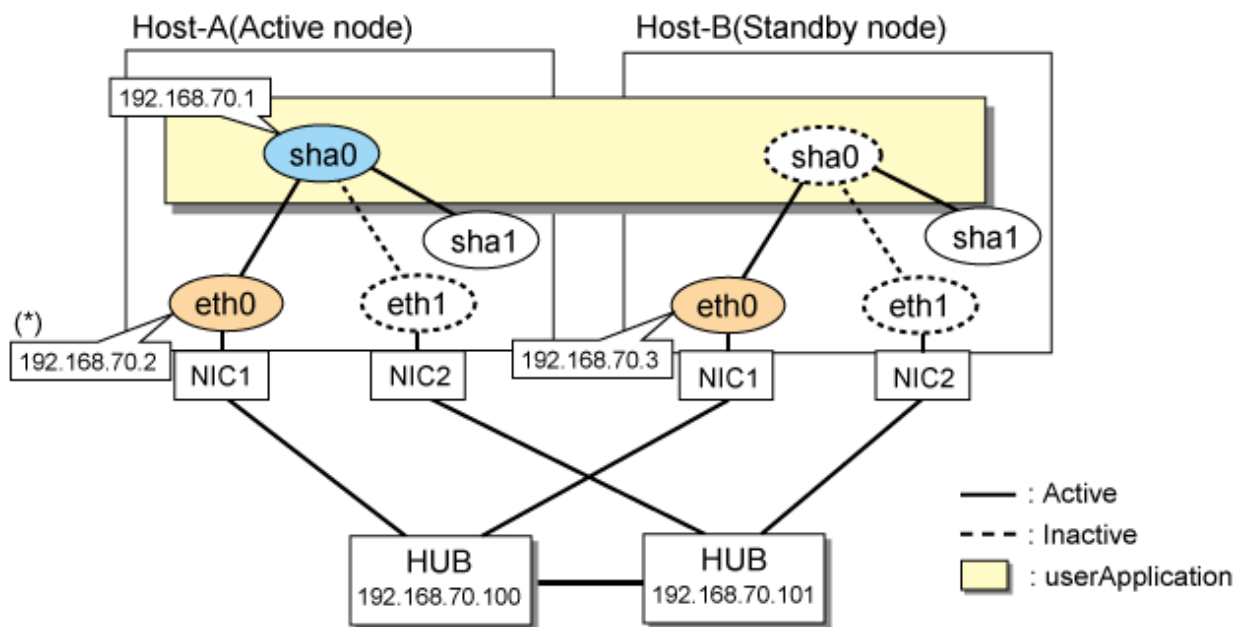
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for enabling physical interface on a standby node.)

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



\*) Physical IP address(192.168.70.2) is inactivated when takeover IP address(192.168.70.1) is activated.

## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```

192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover 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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet

```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
```

### 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) Creating 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 RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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 in Takeover physical IP address (pattern II)

---

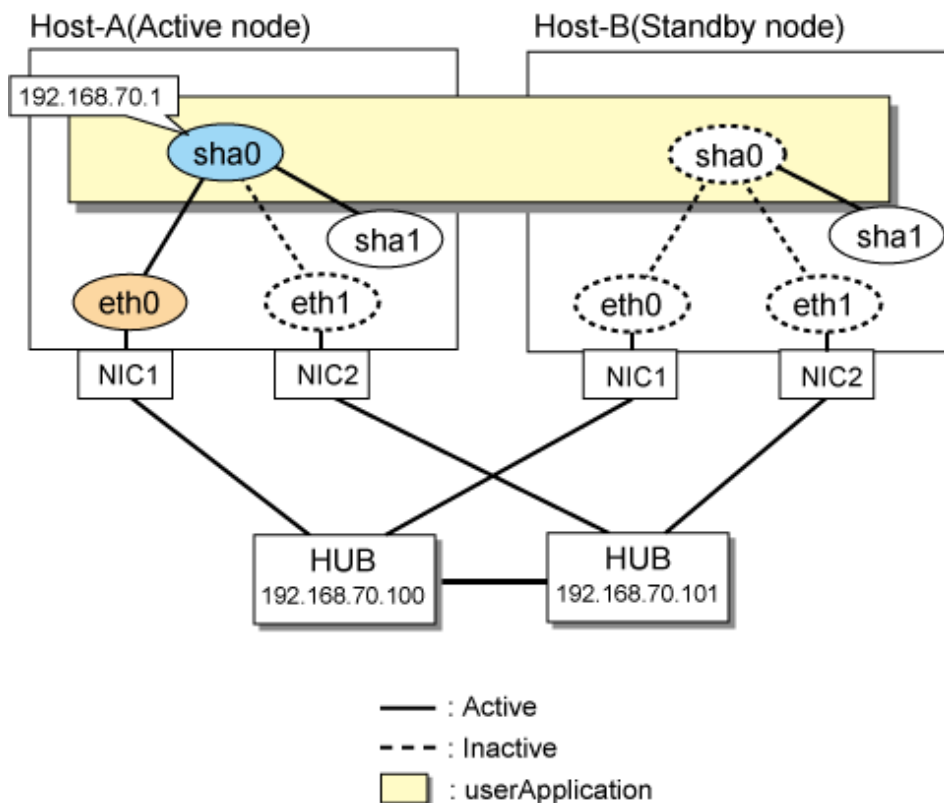
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for not enabling physical interface on a standby node.)

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP)
192.168.70.100 swhub1   # Primary HUB IP
192.168.70.101 swhub2   # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```



### Note

If the physical IP address (takeover IP address) specified to the option '-i' is defined in /etc/sysconfig/network-scripts/ifcfg-eth0, IP addresses may duplicate at the time of switching the cluster.

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```



### Note

If the physical IP address (takeover IP address) specified to the option '-i' is defined in /etc/sysconfig/network-scripts/ifcfg-eth0, IP addresses may duplicate at the time of switching the cluster.

## 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) Creating 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 RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".



## 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 (Cascade)

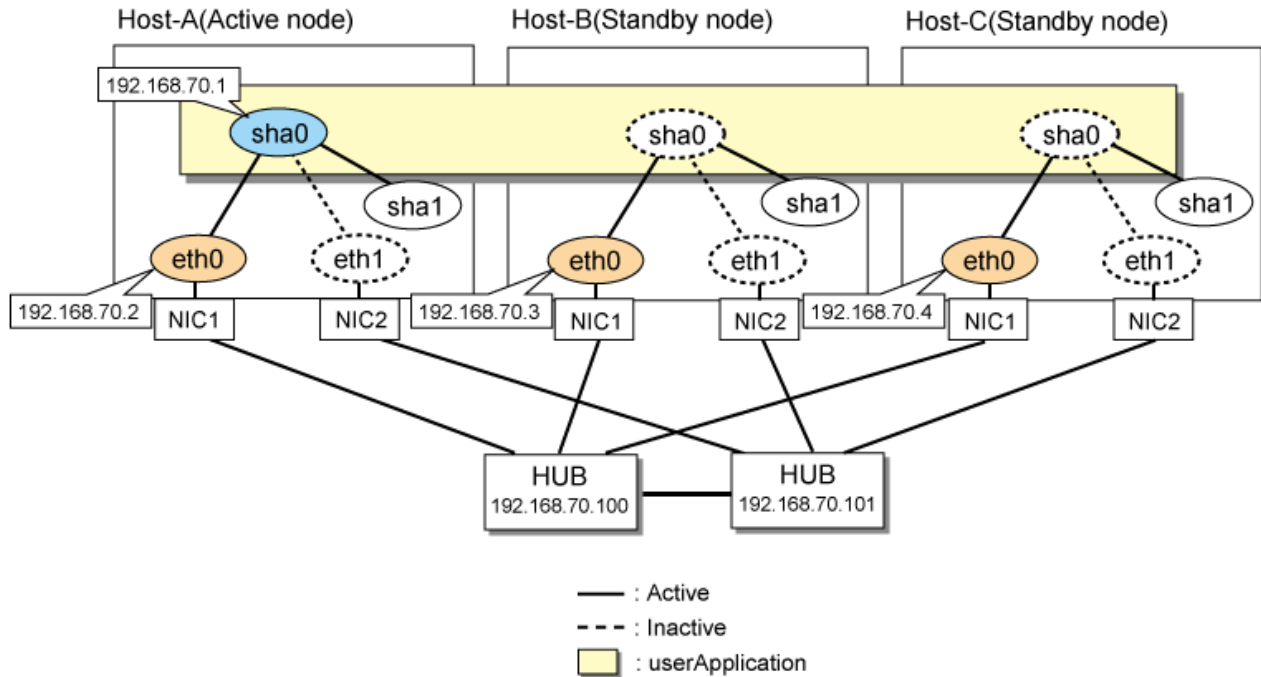
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B/C Virtual IP (Takeover 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) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

### 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) Creating 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 RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 (NIC non-redundant)

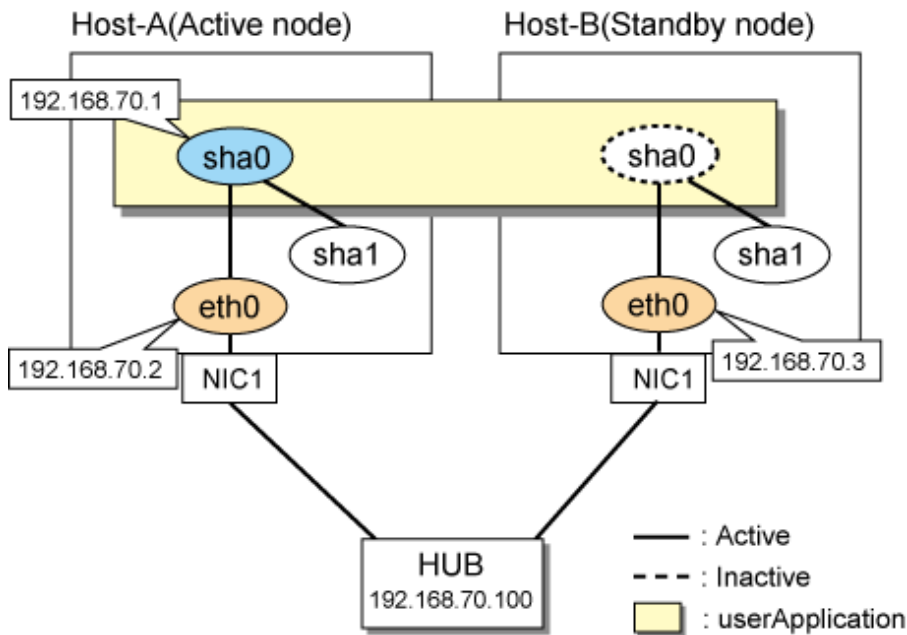
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover 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
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-eth0 file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
```

### 6) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

### 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-eth0 file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100 -b off
```

### 6) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

### 7) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## B.5 Example of configuring NIC switching mode (IPv6)

---

When using IPv6 address, 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

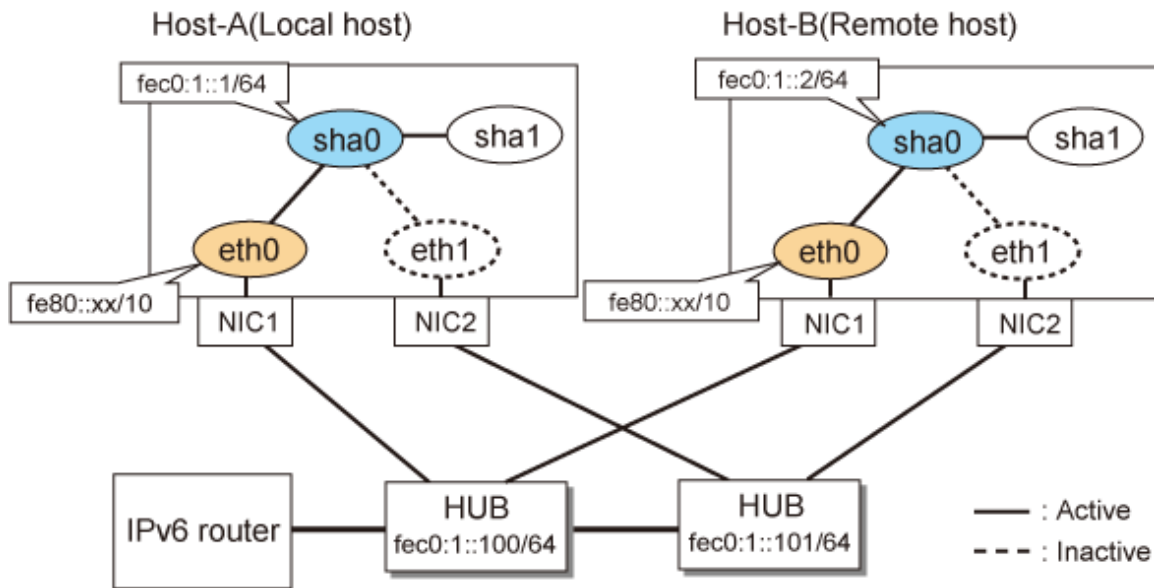
---

This section describes an example configuration procedure of the network shown in the diagram below.

The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
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
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 7) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

# [HOST-B]

## 1) Setting up the system

1-1) Create /etc/hostname6.eth0 file as an empty file.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t eth0,eth1
```

## 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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 7) Starting the HUB monitoring function

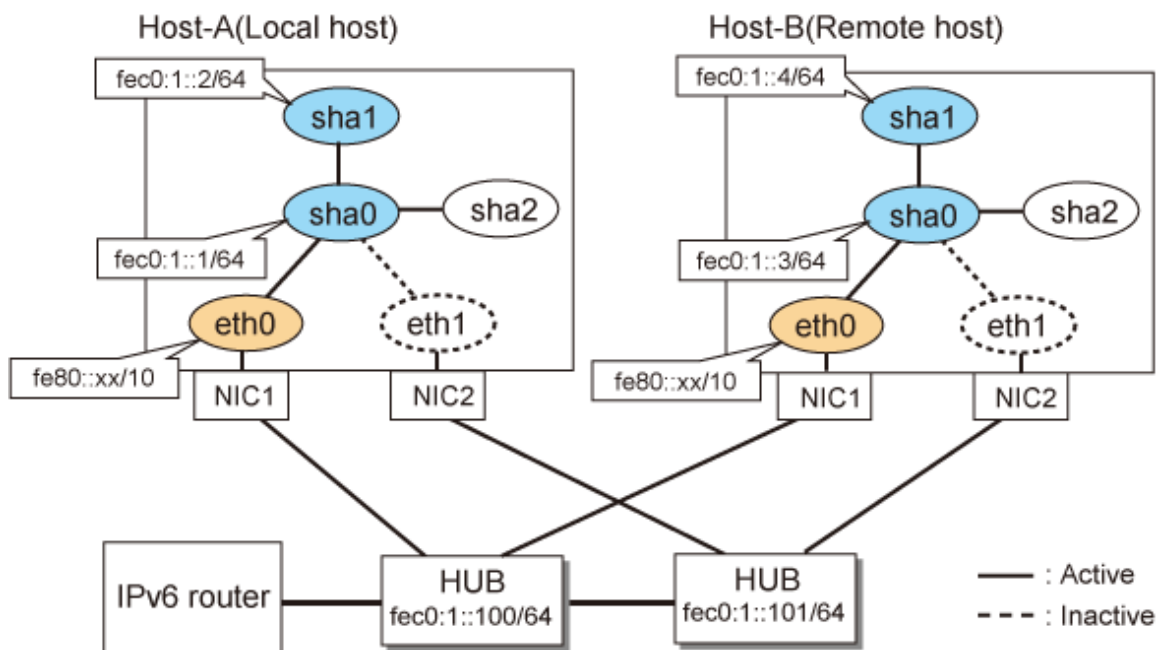
```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## 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 in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta1      # HOST-A Virtual IP
fec0:1::2      v6hosta2      # HOST-A Virtual IP
fec0:1::3      v6hostb1      # HOST-B Virtual IP
fec0:1::4      v6hostb2      # HOST-B Virtual IP
fec0:1::100    swhub1        # Primary HUB IP
fec0:1::101    swhub2        # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0  
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

## 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes  
NETWORKING_IPV6=yes  
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t eth0,eth1  
/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) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

#### 7) Starting the HUB monitoring function

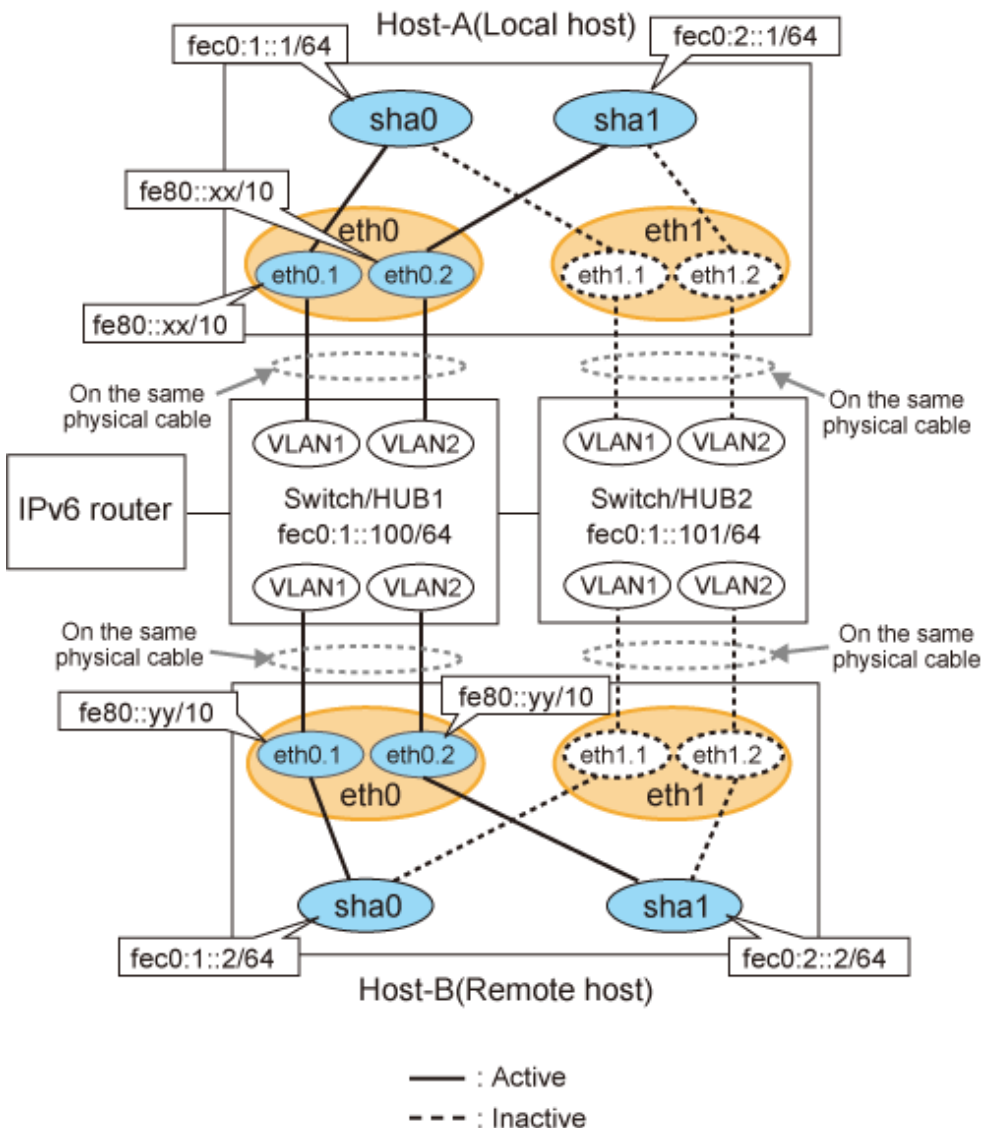
```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### B.5.3 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx and yy in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts 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 Switch/HUB IP
fec0:1::101    swhub2      # Secondary Switch/HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth0.2,eth1.2
```

## 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 HUB monitoring function (Synchronous 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 and reboot the system.

```
/sbin/shutdown -r now
```

# [HOST-B]

## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```



```
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t eth0.2,eth1.2
```

## 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 HUB monitoring function (Synchronous 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 and reboot the system.

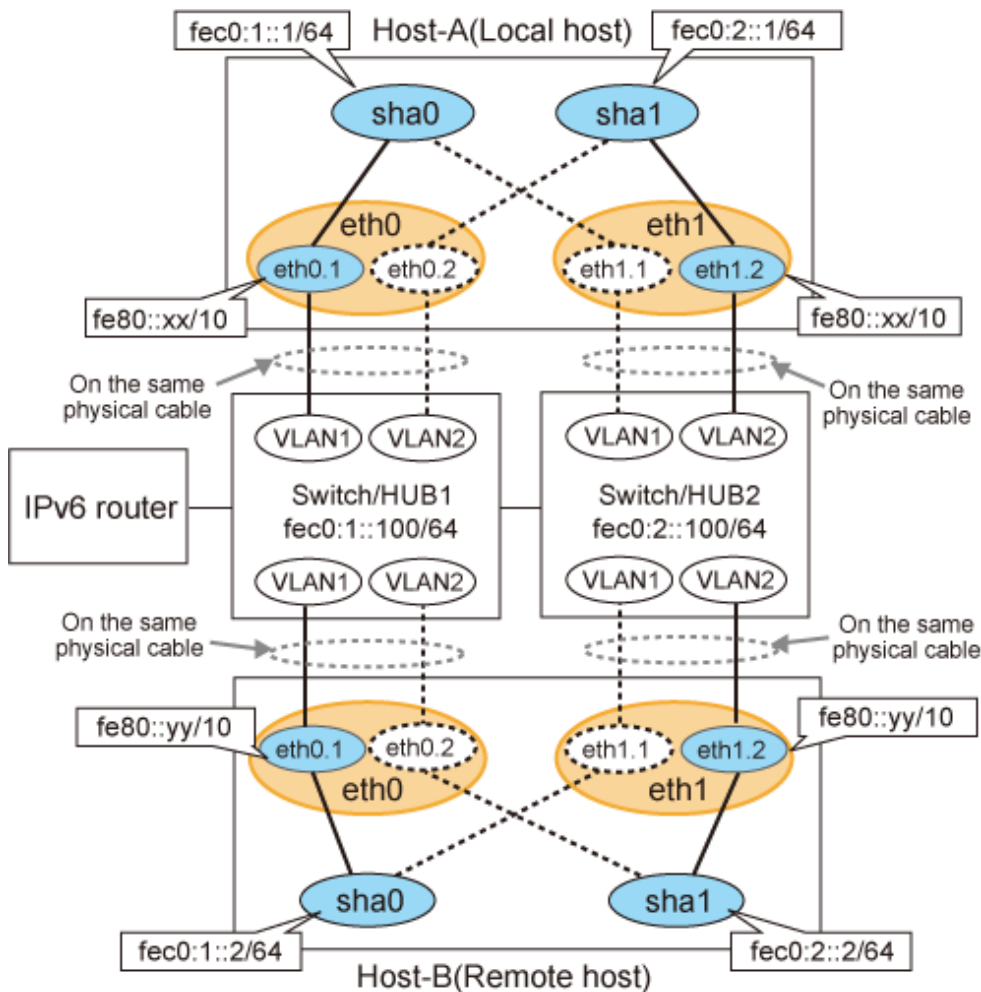
```
/sbin/shutdown -r now
```

## B.5.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching)

This section describes an example configuration procedure of the network shown in the diagram below.

The xx and yy in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "3.2.2 Network configuration".



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts 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
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0.1,eth1.1  
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth1.2,eth0.2
```

### 4) 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
```

### 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 and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1  
BOOTPROTO=static  
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::2/64 -t eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::2/64 -t eth1.2,eth0.2
```

## 4) 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
```

## 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 and reboot the system.

```
/sbin/shutdown -r now
```

## 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.

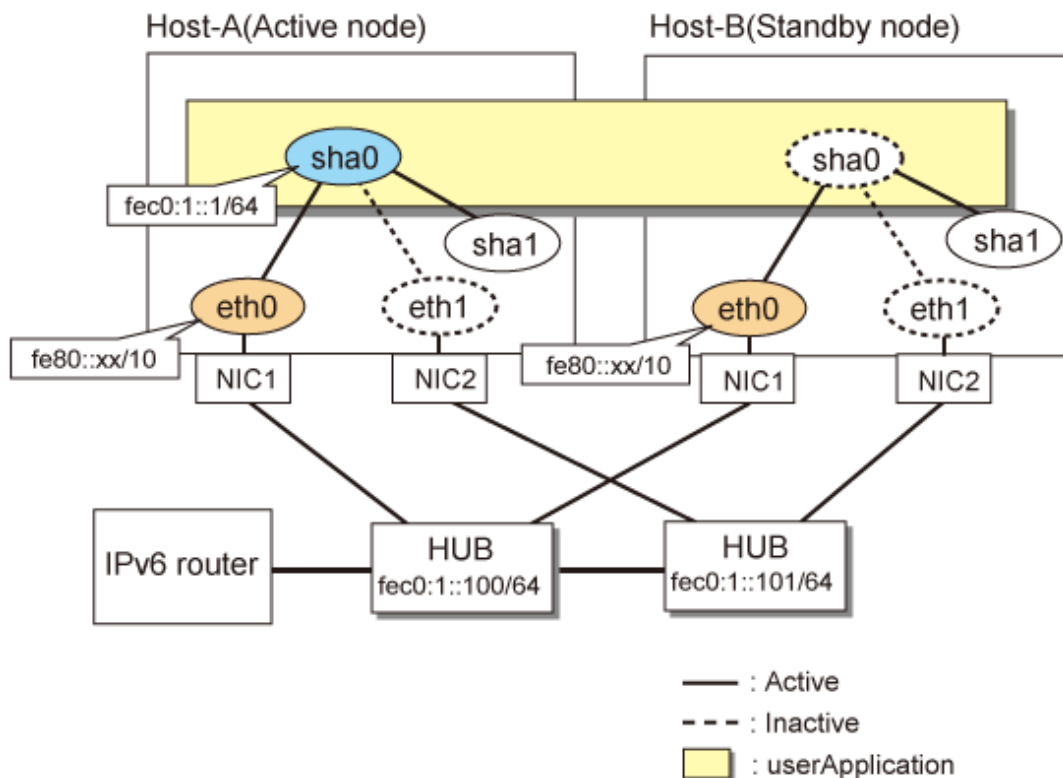
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta      # HOST-A/B Takeover virtual IP
fec0:1::100    swhub1       # Primary HUB IP
fec0:1::101    swhub2       # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Creating 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 configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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 in the figure below are assigned automatically by the automatic address configuration.

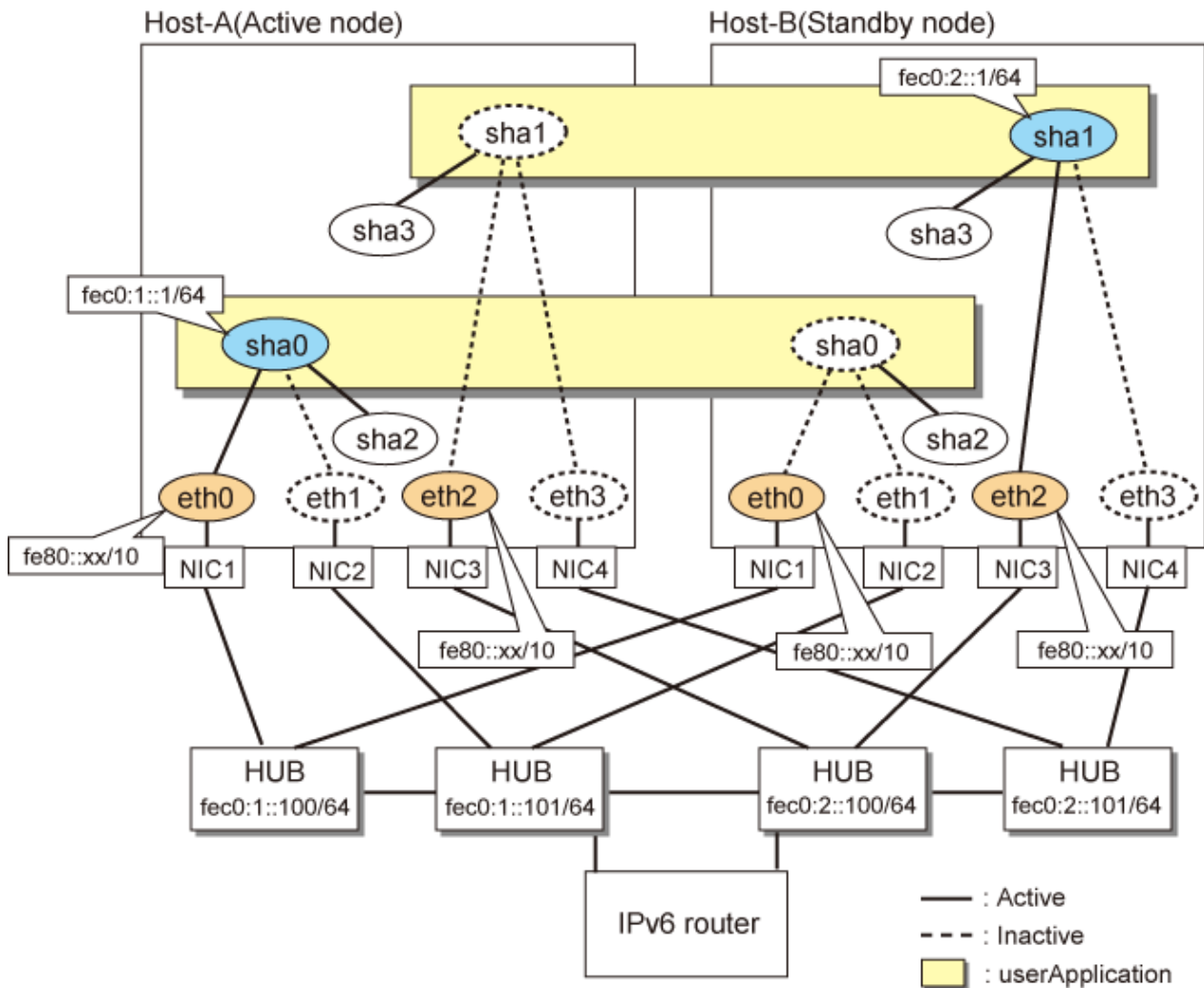
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta      # HOST-A/B Takeover virtual IP
fec0:1::100    swhub1       # Primary HUB IP
fec0:1::101    swhub2       # Secondary HUB IP
fec0:2::1      v6hostb      # HOST-A/B Takeover virtual IP
fec0:2::100    swhub3       # Primary HUB IP
fec0:2::101    swhub4       # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth2 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth2,eth3
```

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth2 are enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth2,eth3
```

## 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) Creating 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 configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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.

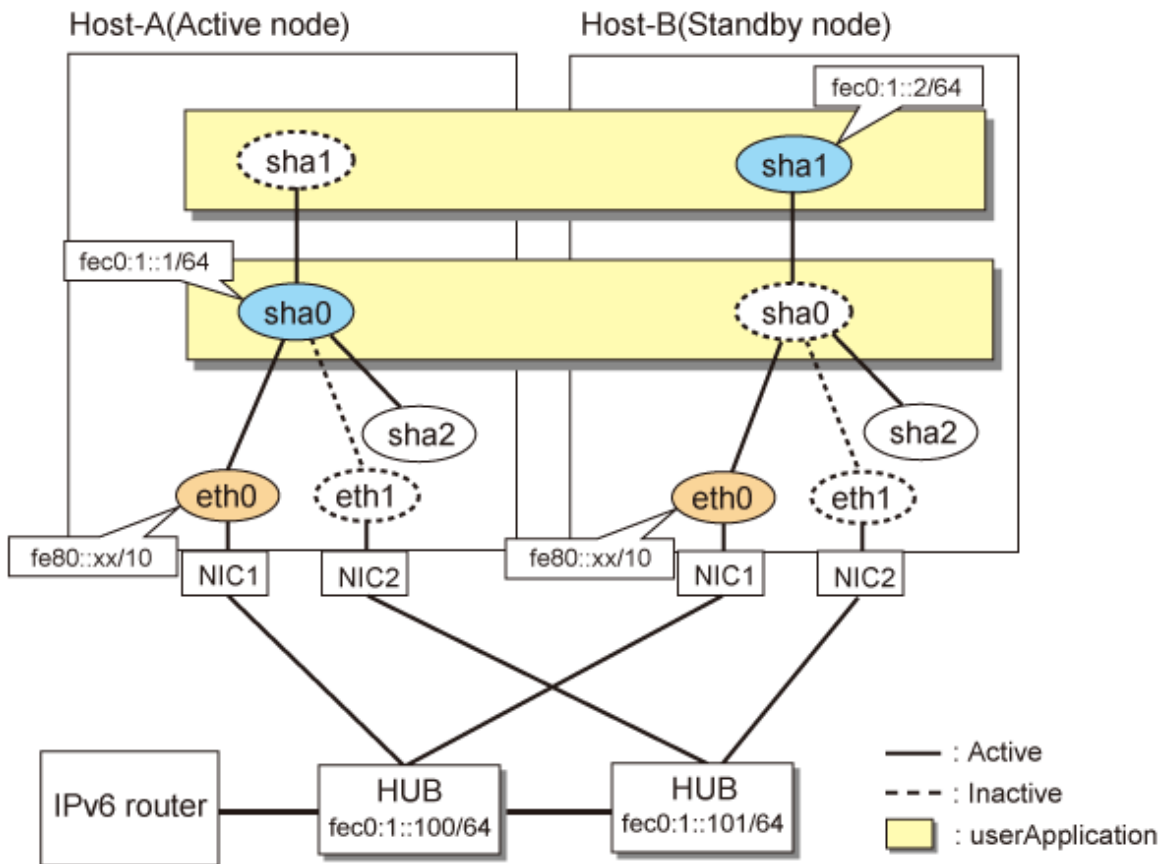
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
fec0:1::1      v6hosta      # HOST-A/B Takeover virtual IP
fec0:1::2      v6hostb      # HOST-A/B Takeover virtual IP
fec0:1::100    swhub1       # Primary HUB IP
fec0:1::101    swhub2       # Secondary HUB IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "3.2.2 Network configuration".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
```

```
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -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) Creating 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 configuring HOST-A and HOST-B, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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.

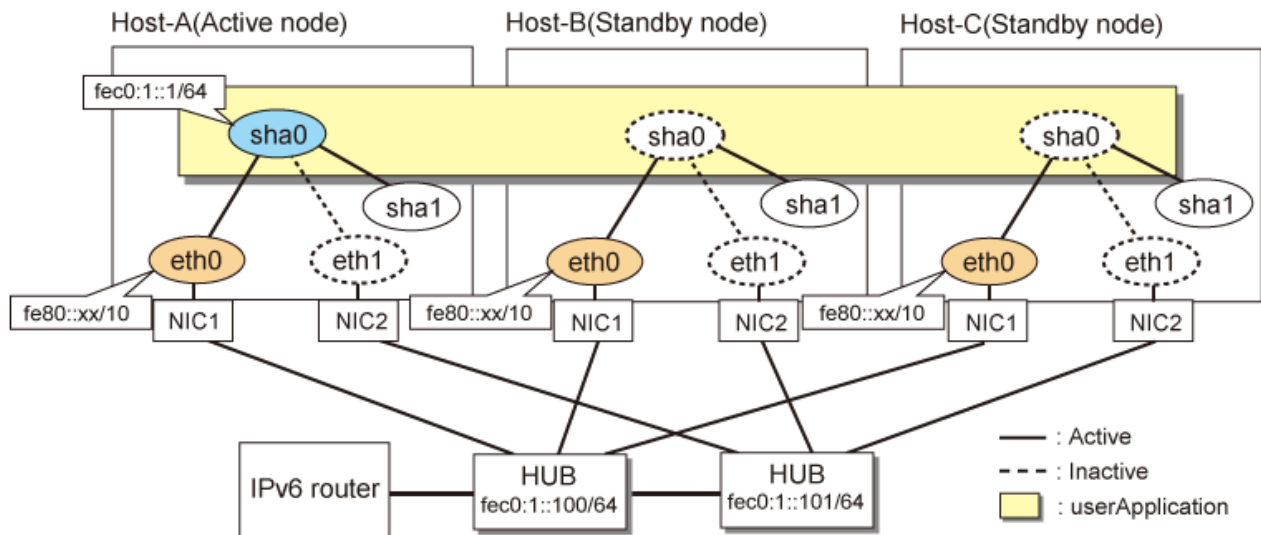
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
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
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
```



```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Creating 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/hosts file. Defined content is same as HOST-A.

- 1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 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) Creating 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 configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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, 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.

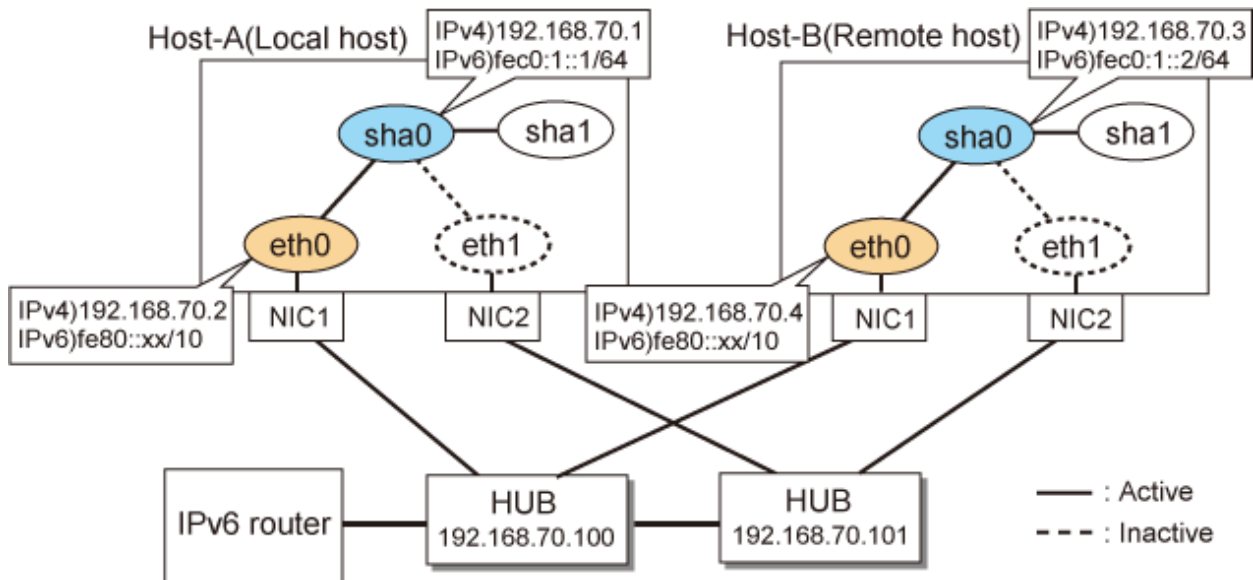
## B.6.1 Example of the Single system without NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
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
fec0:1::1      v6hosta   # HOST-A Virtual IP
fec0:1::2      v6hostb   # HOST-B Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
```

```
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::1/64
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 8) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 9) 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.3 -e 192.168.70.4 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha0 -i fec0:1::2/64
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 8) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0
```

## 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

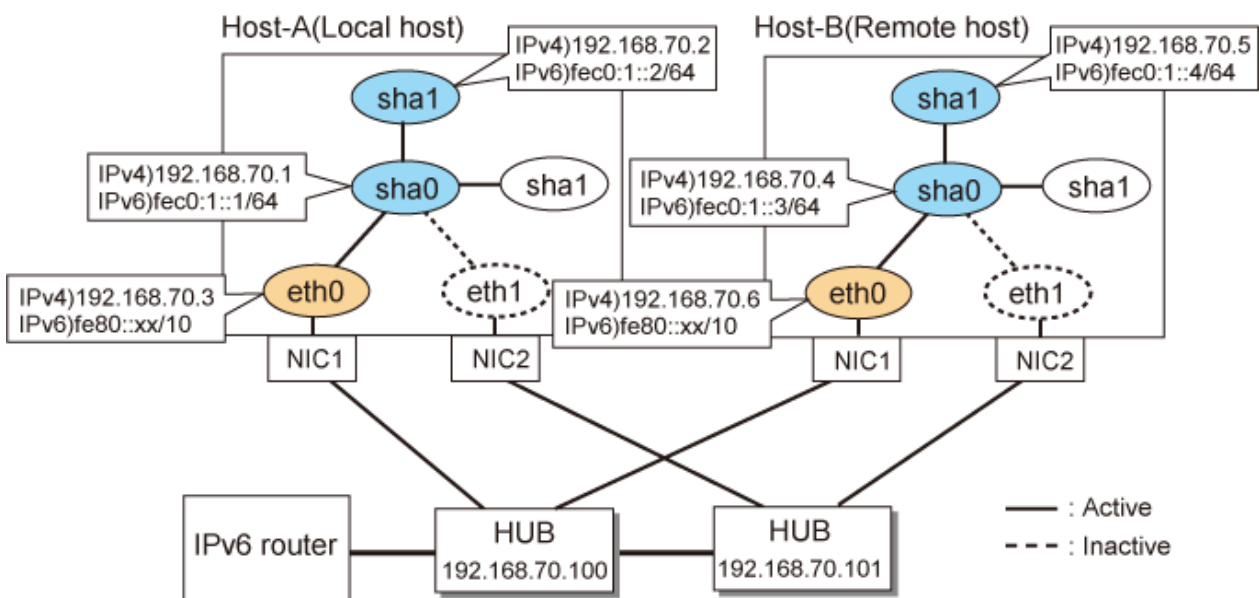
## B.6.2 Example of the Single system with NIC sharing

This section describes an example configuration procedure of the network shown in the diagram below.

The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    hosta1  # HOST-A Virtual IP
192.168.70.2    hosta2  # HOST-A Virtual IP
192.168.70.3    hostl1  # HOST-A Physical IP
192.168.70.4    hostb1  # HOST-B Virtual IP
192.168.70.5    hostb2  # HOST-B Virtual IP
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
fec0:1::1      v6hosta1  # HOST-A Virtual IP
fec0:1::2      v6hosta2  # HOST-A Virtual IP
fec0:1::3      v6hostb1  # HOST-B Virtual IP
fec0:1::4      v6hostb2  # HOST-B Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```



## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

## 8) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0  
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

## 9) 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.70.255  
IPADDR=192.168.70.6  
NETMASK=255.255.255.0  
NETWORK=192.168.70.0  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes  
NETWORKING_IPV6=yes  
IPv6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.4 -e 192.168.70.6 -t eth0,eth1  
/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/sysconfig/network-scripts/ifcfg-eth0.

### 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::3/64 -t eth0,eth1  
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::4/64
```

### 6) 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
```

### 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

### 8) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet -n sha0  
/opt/FJSVhanet/usr/sbin/strhanet -n sha1
```

### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

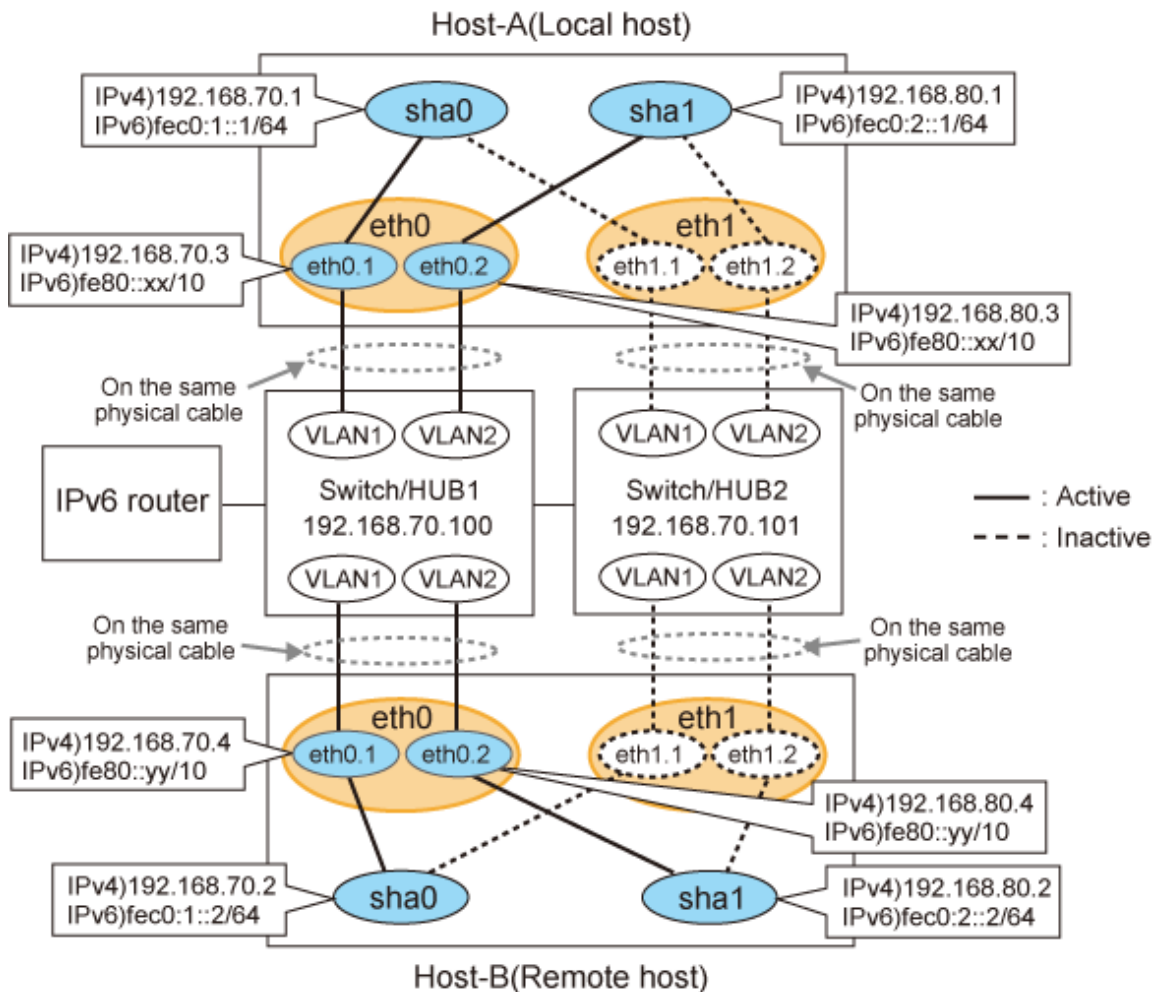
## B.6.3 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching)

---

This section describes an example configuration procedure of the network shown in the diagram below.

The xx and yy in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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
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)
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.3
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0  
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
eth0.1,eth1.1  
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t  
eth0.2,eth1.2
```



### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

### 5) Creating 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
```

### 6) 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
```

### 7) Setting up the HUB monitoring function (Synchronous switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

### 8) 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
```

### 9) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.4
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth0.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t
eth0.1,eth1.1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t
eth0.2,eth1.2
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

#### 5) Creating 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
```

#### 6) 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
```

#### 7) Setting up the HUB monitoring function (Synchronous switching)

```
/opt/FJSVhanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

#### 8) 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
```

#### 9) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

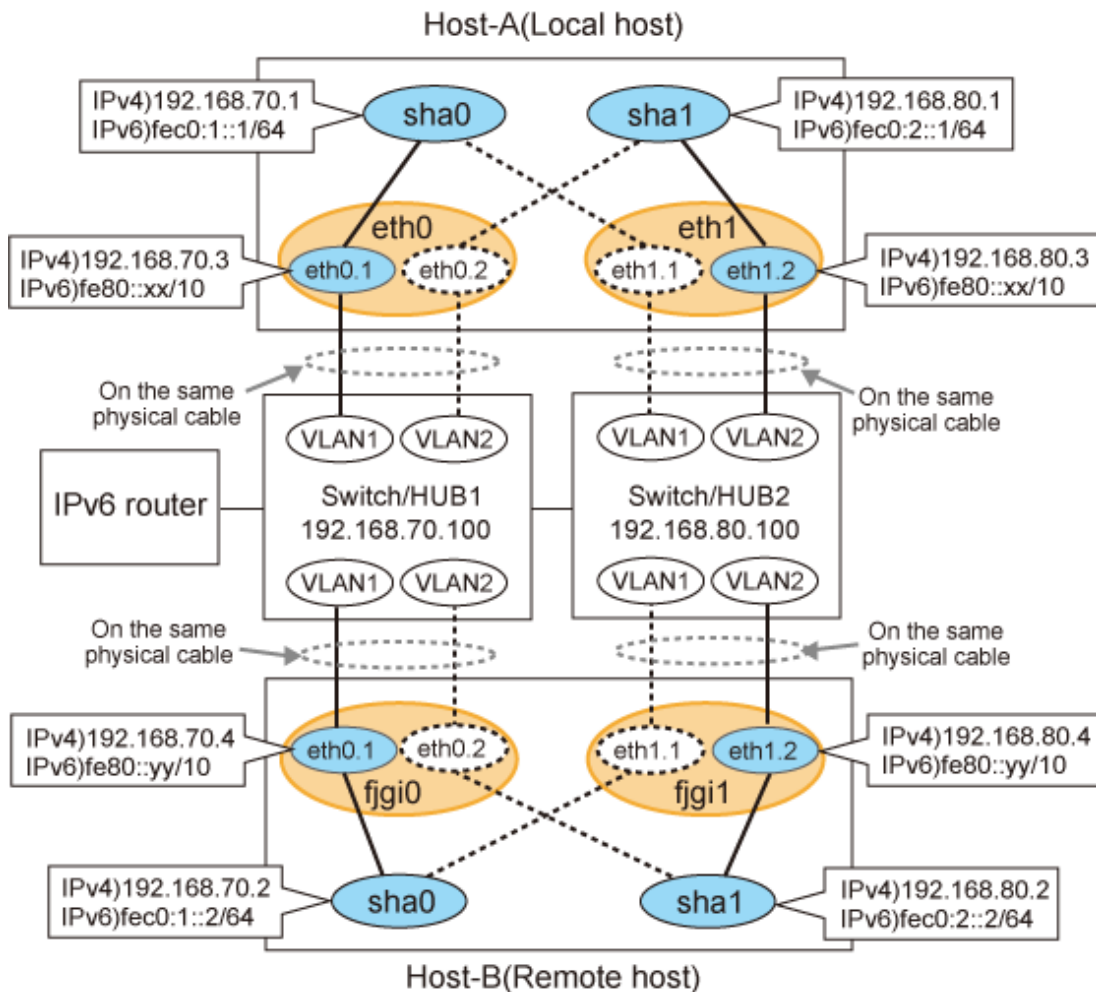
## B.6.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching)

---

This section describes an example configuration procedure of the network shown in the diagram below.

The xx and yy in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/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
192.168.80.100 swhub2   # Secondary Switch/HUB IP
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)
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".



- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.3
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0  
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t  
eth0.1,eth1.1  
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.1 -e 192.168.80.3 -t  
eth1.2,eth0.2
```



### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

### 5) Creating 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
```

### 6) 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
```

### 7) 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
```

### 8) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0,1. Y is 1,2) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
DEVICE=eth0.1
BOOTPROTO=static
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.2

```
DEVICE=eth0.2
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
DEVICE=eth1.1
BOOTPROTO=static
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
DEVICE=eth1.2
BOOTPROTO=static
BROADCAST=192.168.80.255
IPADDR=192.168.80.4
NETMASK=255.255.255.0
NETWORK=192.168.80.0
ONBOOT=yes
```

1-4) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
VLAN=yes
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0.1 and eth1.2 is enabled using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.2 -e 192.168.70.4 -t  
eth0.1,eth1.1  
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.80.2 -e 192.168.80.4 -t  
eth1.2,eth0.2
```



#### Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y.

#### 5) Creating 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
```

#### 6) 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
```

#### 7) 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
```

#### 8) Reboot

Run the following command and reboot the system.

```
/sbin/shutdown -r now
```

## 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.

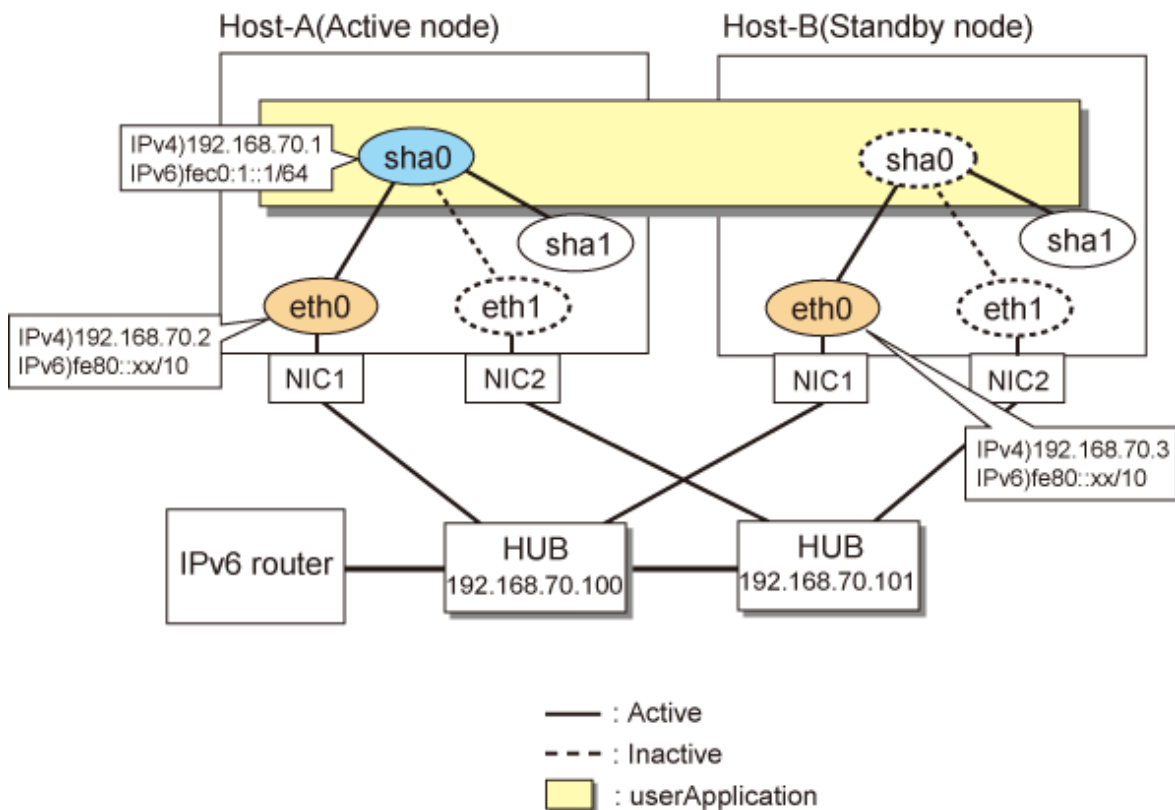
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
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
fec0:1::1      v6hosta1  # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

## 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## 10) 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

### 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

#### 6) 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
```

#### 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

#### 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

#### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

#### 10) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha1
```

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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 in the figure below are assigned automatically by the automatic address configuration.

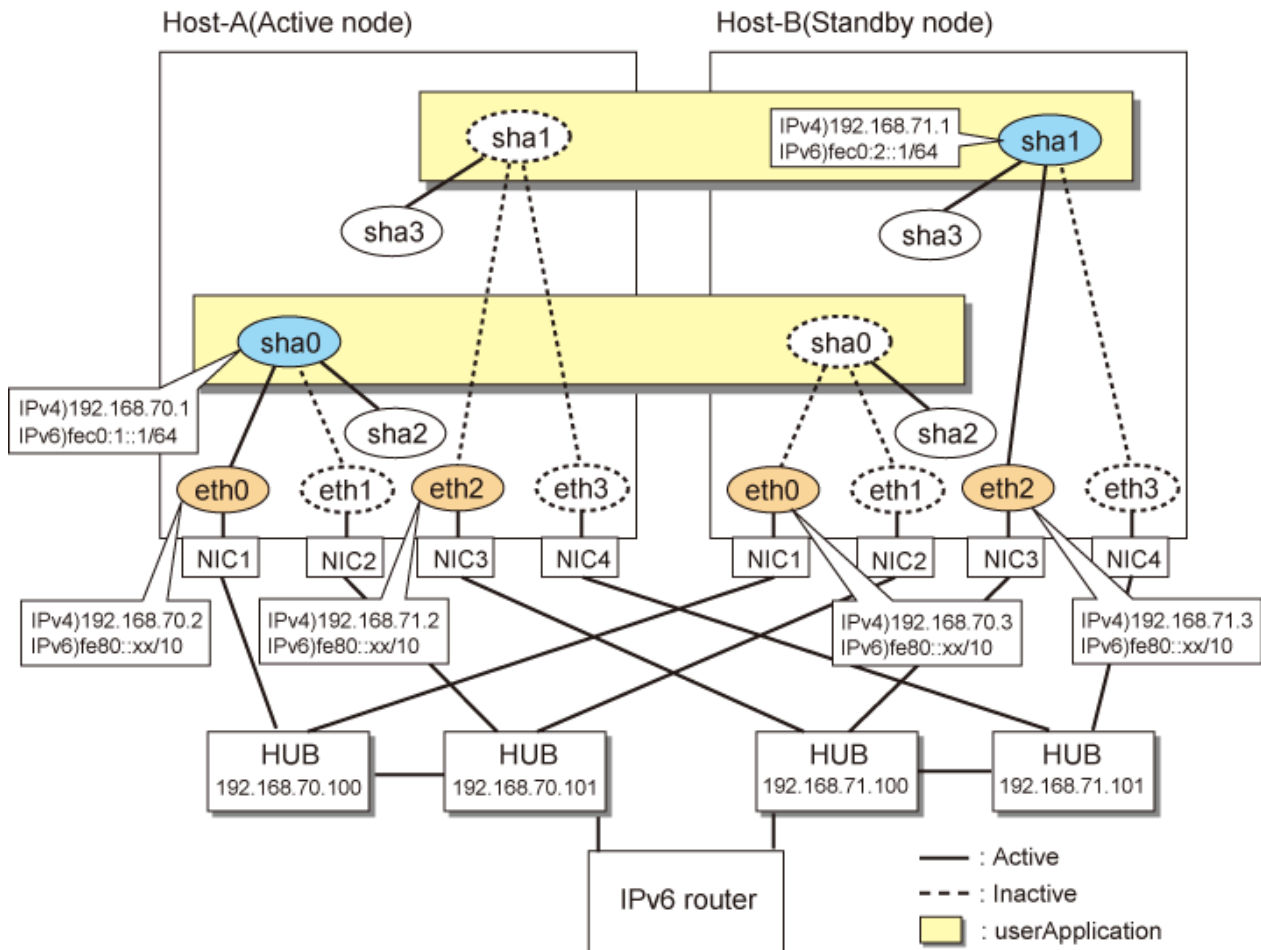
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.71.1    hostb    # HOST-A/B Virtual IP (Takeover IP2)
192.168.71.2    host12   # HOST-A Physical IP
192.168.71.3    host22   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
192.168.71.100  swhub3   # Primary HUB IP
192.168.71.101  swhub4   # Secondary HUB IP
fec0:1::1      v6hosta   # HOST-A/B Takeover virtual IP
fec0:2::1      v6hostb   # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth2 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.2 -t eth2,eth3
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0 and /etc/sysconfig/network-scripts/ifcfg-eth2.

### 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth2,eth3
```

### 6) 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
```

### 7) 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
```

### 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 10) 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/hosts file. Defined content is same as HOST-A.
- 1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.3
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 and eth2 are enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m d -i 192.168.71.1 -e 192.168.71.3 -t eth2,eth3
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0 and /etc/sysconfig/network-scripts/ifcfg-eth2.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha1 -m d -i fec0:2::1/64 -t eth2,eth3
```

#### 6) 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
```

#### 7) 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
```

#### 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

#### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

#### 10) 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 configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application.  
Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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.

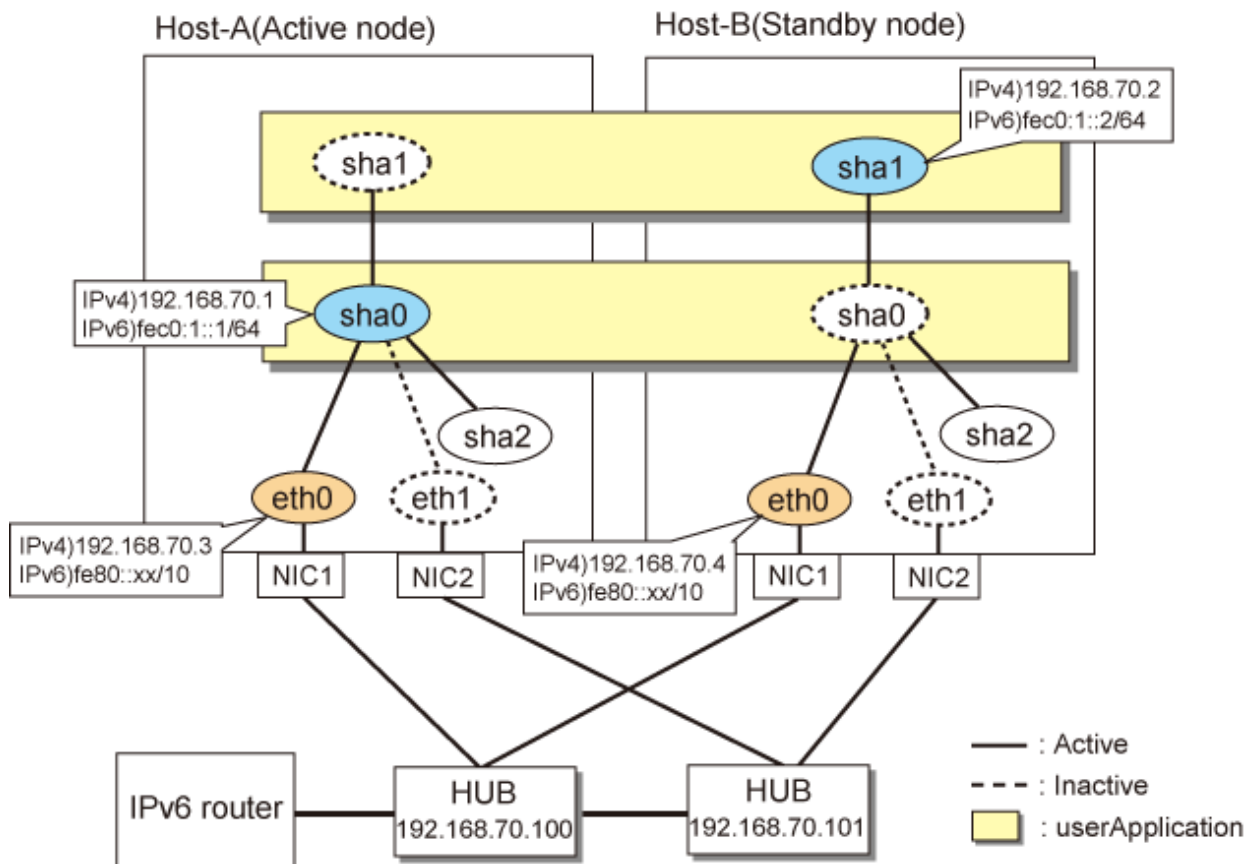
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP1)
192.168.70.2    hostb    # HOST-A/B Virtual IP (Takeover IP2)
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
fec0:1::1      v6hosta   # HOST-A/B Takeover virtual IP
fec0:1::2      v6hostb   # HOST-A/B Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
```

```
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

## 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## 10) 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/hosts file. Defined content is same as HOST-A.

1-2) Write the host name defined above in /etc/sysconfig/network-scripts/ifcfg-eth0 file. If the file does not exist, create a new file.



#### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

#### 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

#### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

#### 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t eth0,eth1
/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/sysconfig/network-scripts/ifcfg-eth0.

### 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig copy inet6 -n sha0,sha1 -i fec0:1::2/64
```

### 6) 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
```

### 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

### 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 10) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha2
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 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.

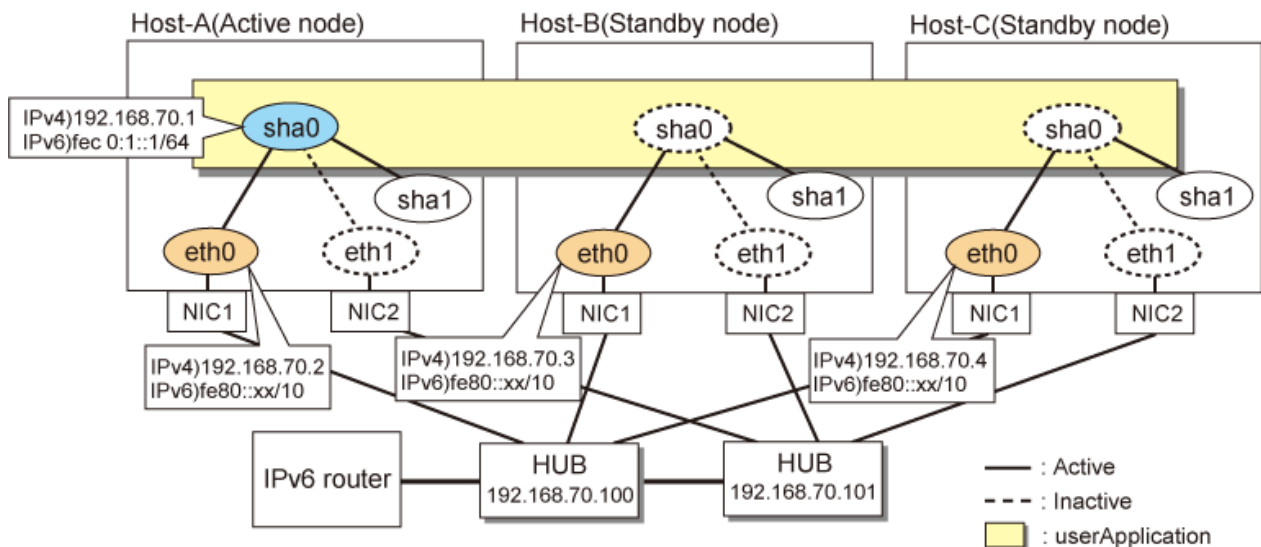
The xx in the figure below are assigned automatically by the automatic address configuration.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Note that it is not necessary to define an IPv6 address, which automatically allocates address by the Stateless Address Autoconfiguration feature.

```
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
fec0:1::1      v6hosta1  # HOST-A/B/C Takeover virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.2 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

## 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## 10) 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.3
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

## 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

## 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

## 6) 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
```

## 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 10) 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/hosts file. Defined content is same as HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.4
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on /etc/sysconfig/network file, define a statement allows the system to load IPv6 module.

```
NETWORKING=yes
NETWORKING_IPV6=yes
IPV6TO4INIT=no
```

### 2) Reboot

Run the following command and reboot the system. After rebooting the system, verify eth0 is enabled as an IPv4/IPv6 interface using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creation of IPv4 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.4 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0.

### 5) Creation of IPv6 virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create inet6 -n sha0 -m d -i fec0:1::1/64 -t eth0,eth1
```

### 6) 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
```

### 7) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 8) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

### 9) Starting the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 10) Starting the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/strptl -n sha1
```

## [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A, HOST-B and HOST-C, register the created takeover virtual interface as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 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 Virtual NIC mode

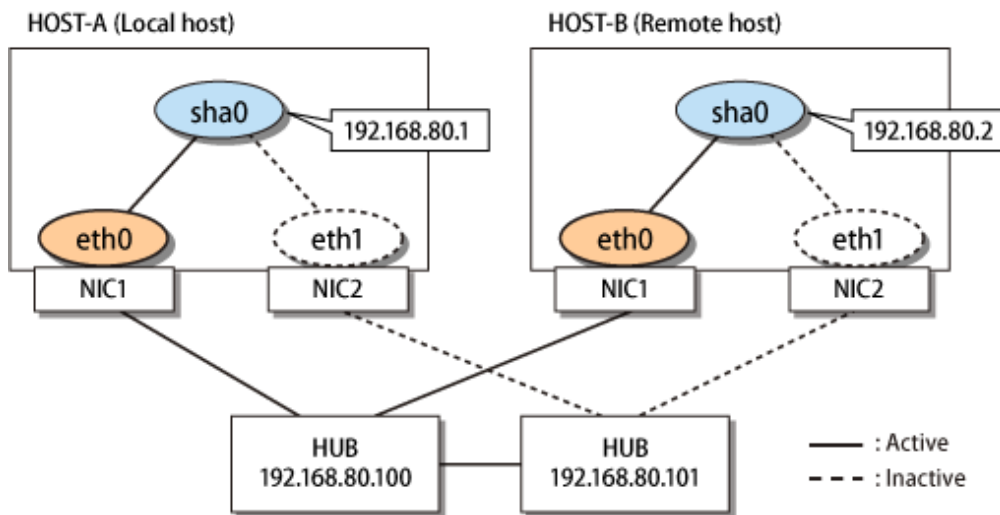
---

### B.7.1 Example of the Single system

---

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.100  swhub1   # Primary HUB IP
192.168.80.101  swhub2   # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

### [HOST-B]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

#### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

#### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

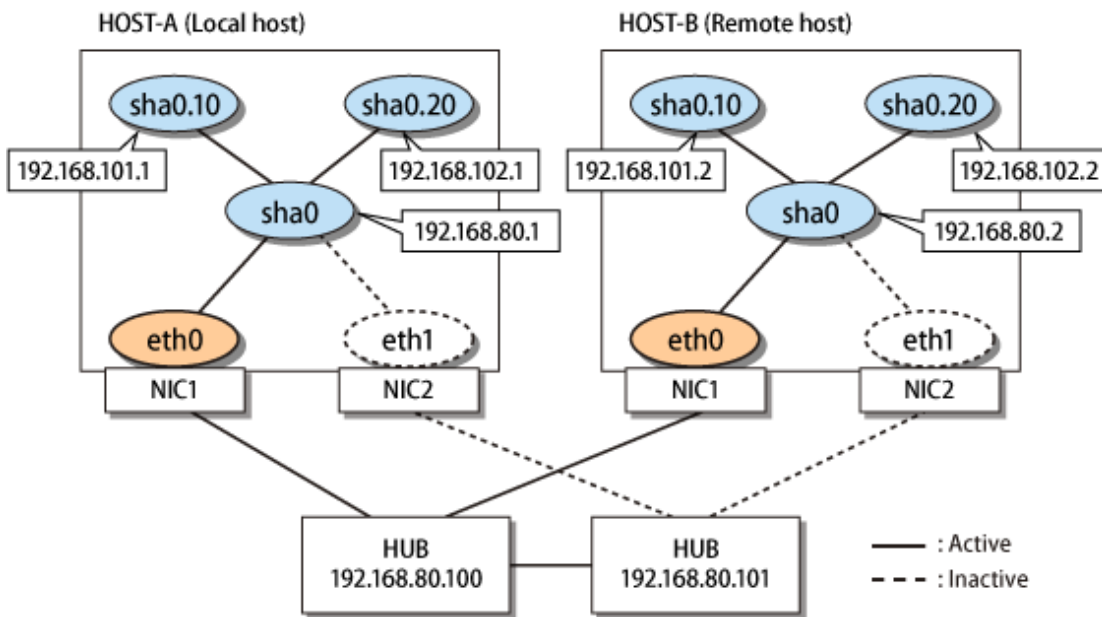
## B.7.2 Configuring virtual interfaces with tagged VLAN

---

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.101.1  hosta-v1 # HOST-A Virtual IP (Tagged VLAN interface)
192.168.102.1  hosta-v2 # HOST-A Virtual IP (Tagged VLAN interface)
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.101.2  hostb-v1 # HOST-B Virtual IP (Tagged VLAN interface)
192.168.102.2  hostb-v2 # HOST-B Virtual IP (Tagged VLAN interface)
192.168.80.100 swhub1   # Primary HUB IP
192.168.80.101 swhub2   # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network and the tagged VLAN in /etc/sysconfig/network file.

```
NETWORKING=yes
VLAN=yes
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

## 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

## 5) Adding tagged VLAN interfaces

To add tagged VLAN interfaces (sha0.10 and sha0.20) on the virtual interface (sha0), add the following interface setting files:

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.10

```
DEVICE=sha0.10
IPADDR=192.168.101.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.20

```
DEVICE=sha0.20
IPADDR=192.168.102.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

## 6) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network and the tagged VLAN in /etc/sysconfig/network file. Defined content is same as HOST-A.

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Adding tagged VLAN interfaces

To add tagged VLAN interfaces (sha0.10 and sha0.20) on the virtual interface (sha0), add the following interface setting files:

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.10

```
DEVICE=sha0.10
IPADDR=192.168.101.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.20

```
DEVICE=sha0.20
IPADDR=192.168.102.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

#### 6) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## B.7.3 Example of the Cluster system (1:1 Standby)

---

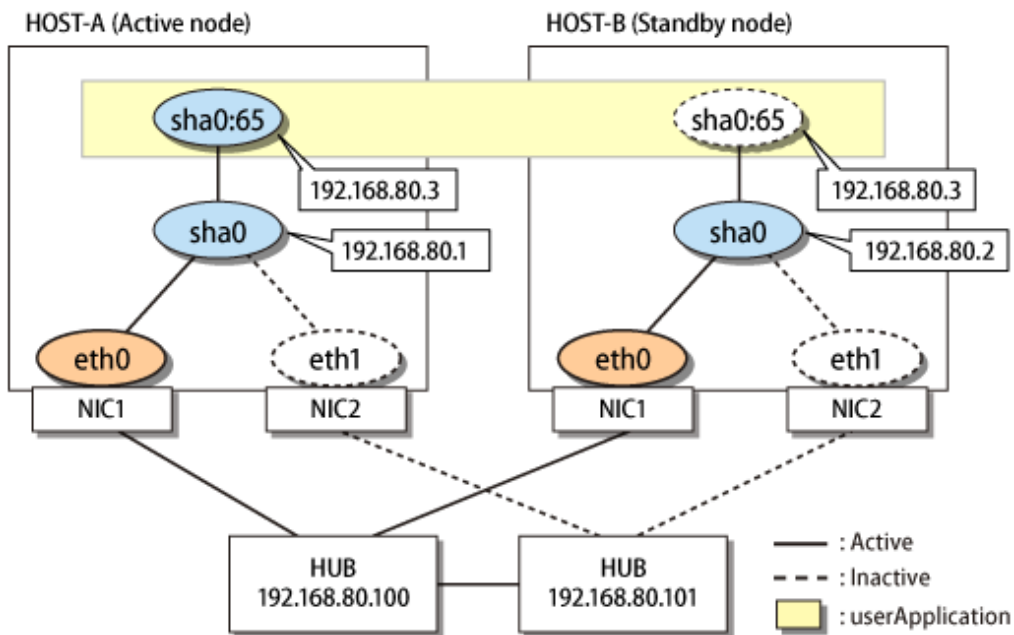
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.3    host1    # HOST-A/B (Takeover virtual IP)
192.168.80.100 swhub1    # Primary HUB IP
192.168.80.101 swhub2    # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

## 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLs resource to create a cluster application.  
Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## B.7.4 Example of the Cluster system (Mutual Standby)

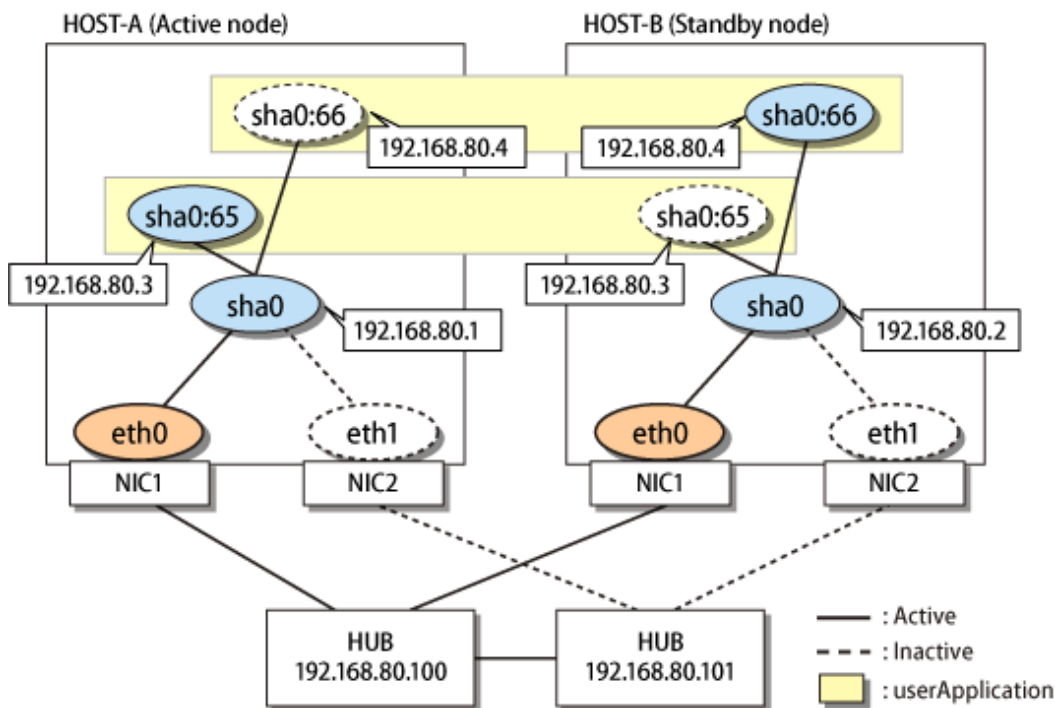
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "3.2.2 Network 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.



## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

192.168.80.1	hosta	# HOST-A Virtual IP
192.168.80.2	hostb	# HOST-B Virtual IP
192.168.80.3	host1	# HOST-A/B Virtual IP (Takeover virtual IP)
192.168.80.4	host2	# HOST-A/B Virtual IP (Takeover virtual IP)

```
192.168.80.100 swhub1 # Primary HUB IP
192.168.80.101 swhub2 # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

## 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

## 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

## 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GLS resource to create a cluster application.  
Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## B.7.5 Example of the Cluster system (Cascade)

This section describes an example configuration procedure of the network shown in the diagram below.

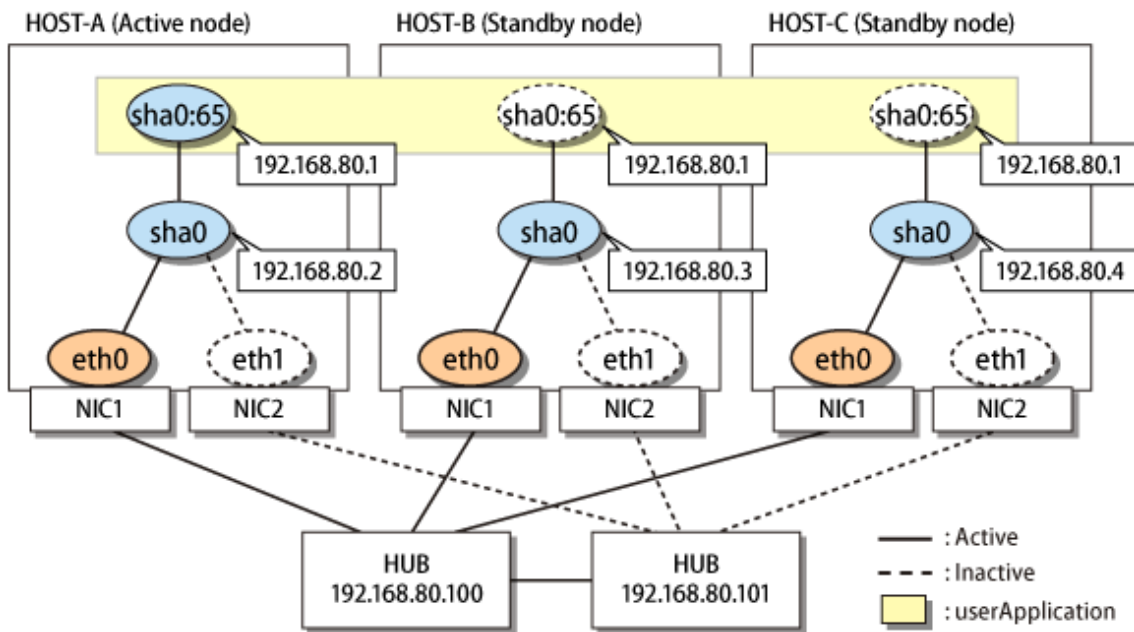
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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.





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.2    hosta    # HOST-A Virtual IP
192.168.80.3    hostb    # HOST-B Virtual IP
192.168.80.4    hostc    # HOST-C Virtual IP
192.168.80.1    host1    # HOST-A/B/C Virtual IP (Takeover virtual IP)
192.168.80.100  swhub1   # Primary HUB IP
192.168.80.101  swhub2   # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.1
```

### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.3
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.1
```

#### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

### [HOST-C]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

#### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

#### 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.4
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Setting a subnet mask of the takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 6) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.1
```

#### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A, HOST-B, and HOST-C, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

## 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 (No IP takeover)

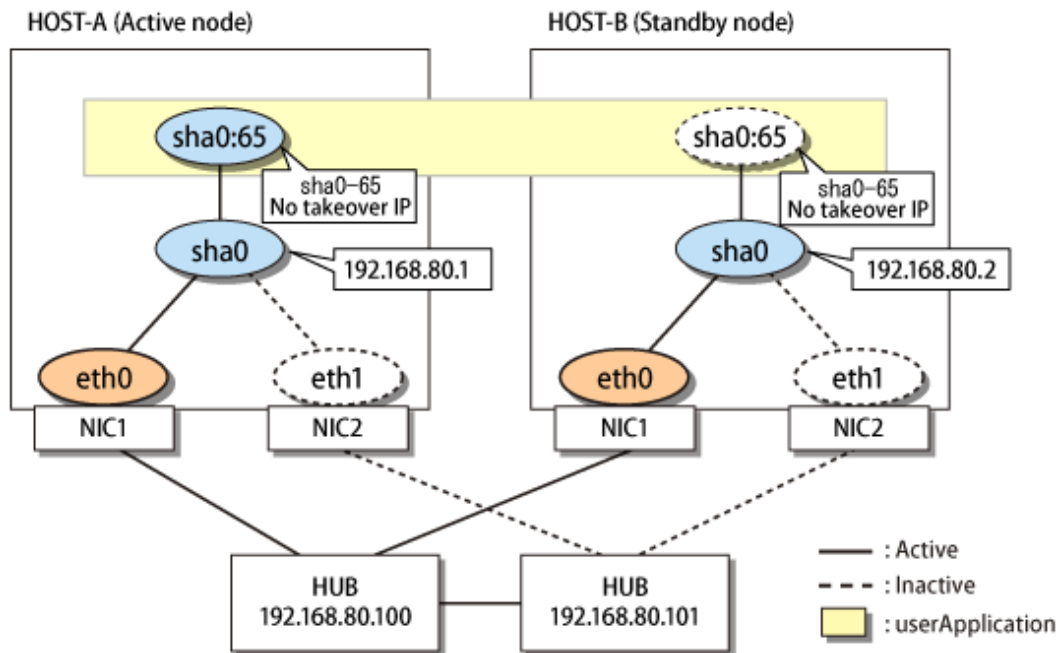
This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



#### [HOST-A]

##### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.1    hosta    # HOST-A Virtual IP
192.168.80.2    hostb    # HOST-B Virtual IP
192.168.80.100  swhub1   # Primary HUB IP
192.168.80.101 swhub2   # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

## 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

## 6) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

# [HOST-B]

## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file. Defined content is same as HOST-A other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as HOST-A.

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.2
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
```

```
DEVICETYPE=sha  
HOTPLUG=no
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

#### 6) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface (sha0:65) as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

#### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

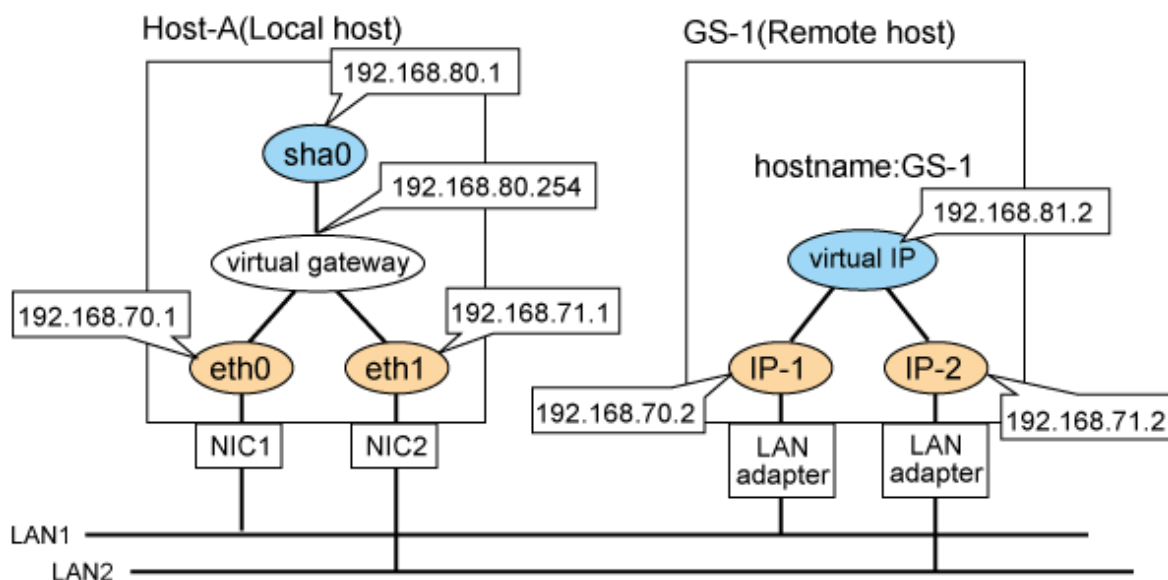
## B.8 Example of configuring GS linkage mode

### B.8.1 Example of the Single system

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

For the GS configuration, refer to GS manual.



### [HOST-A]

#### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```

192.168.70.1    host11    # HOST-A Physical IP
192.168.71.1    host12    # HOST-A Physical IP
192.168.80.1    hosta     # HOST-A Virtual IP
192.168.80.254 virgw    # Virtual gateway
192.168.70.2    gs11     # GS-1 Physical IP(IP-1)
192.168.71.2    gs12     # GS-1 Physical IP(IP-2)
192.168.81.2    gsa      # GS-1 Virtual IP

```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet

```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```

GATEWAY0=192.168.80.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.81.2   # GS-1 Virtual IP

```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### **4) Creating of virtual interface**

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
```

#### **5) Setting the Communication target monitoring function**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.2 -t 192.168.70.2,192.168.71.2
```

#### **6) Setting a virtual gateway**

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

#### **7) Activating of virtual interface**

```
/opt/FJSVhanet/usr/sbin/strhanet
```

### **[GS-1]**

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## **B.8.2 Example of the Single system on remote network**

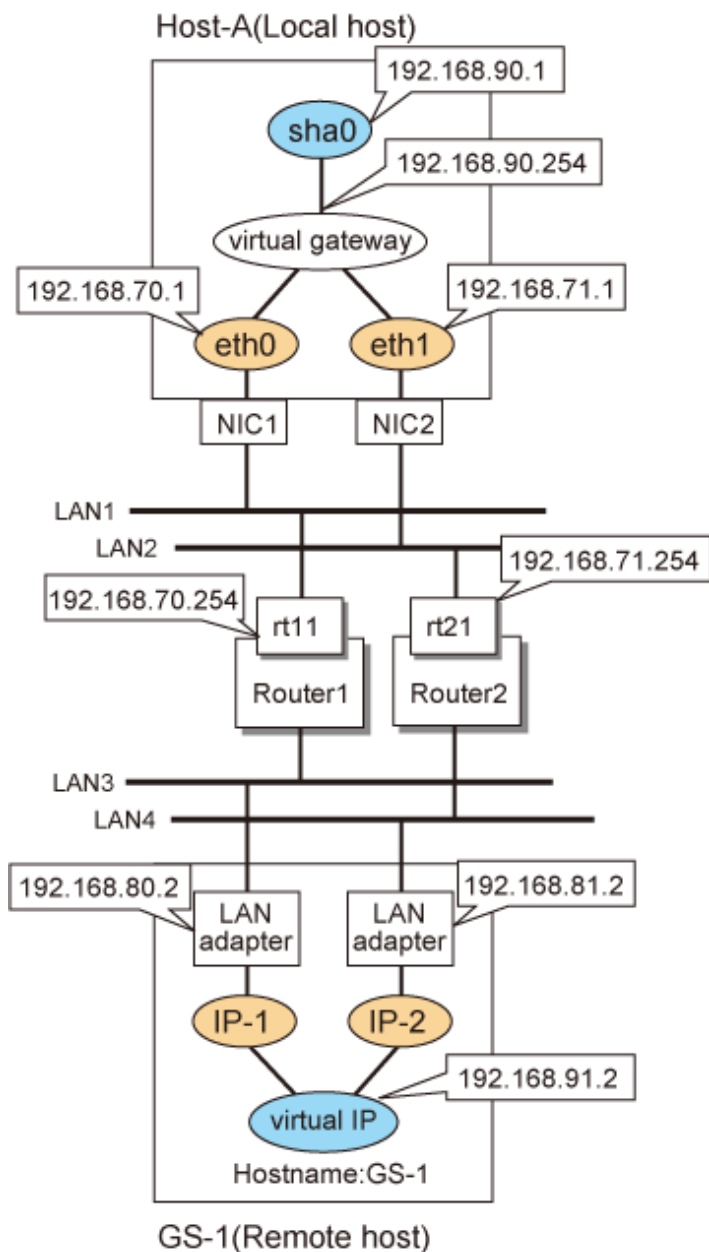
---

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

For the GS configuration, refer to GS manual.





## [HOST-A]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.70.1    host11    # HOST-A Physical IP
192.168.71.1    host12    # HOST-A Physical IP
192.168.90.1    hosta      # HOST-A Virtual IP
192.168.90.254 virgw      # Virtual gateway
192.168.70.254 rt11       # Router1
192.168.71.254 rt21       # Router2
192.168.80.2    gs11       # GS-1 Physical IP(IP-1)
192.168.81.2    gs12       # GS-1 Physical IP(IP-2)
192.168.91.2    gsa        # GS-1 Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the route information of the virtual gateway for the remote host's virtual IP address and the route information for the physical IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```
GATEWAY0=192.168.90.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.91.2 # GS-1 Virtual IP
```

- Contents of /etc/sysconfig/network-scripts/route-eth0

```
GATEWAY0=192.168.70.254 # Local router 1 on the local host
NETMASK0=255.255.255.0 # Subnet mask
ADDRESS0=192.168.80.0 # Physical IP of the remote host (network address)
```

- Contents of /etc/sysconfig/network-scripts/route-eth1

```
GATEWAY0=192.168.71.254 # Local router 2 on the local host
NETMASK0=255.255.255.0 # Subnet mask
ADDRESS0=192.168.81.0 # Physical IP of the remote host (network address)
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.90.0 -m 255.255.255.0
```

### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.90.1 -t eth0,eth1
```

### 5) Setting the Communication target monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t 192.168.70.254+192.168.80.2,  
192.168.71.254+192.168.81.2
```

### 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.90.254
```

### 7) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

## [Router setting]

Set the route information as follows for the virtual IP addresses for Route 1 and Route 2. Make sure that the router neighboring GLS is RIPv1 and the path to GS's virtual IP address is broadcast. How to set the route information depends on the type of router, so read the manual for your router for information on how to set it.

Route1	Destination: 192.168.90.1	Gateway address: 192.168.70.1
Route2	Destination: 192.168.90.1	Gateway address: 192.168.71.1

## [GS-1]

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## B.8.3 Example of the Single system (GS Hot-standby)

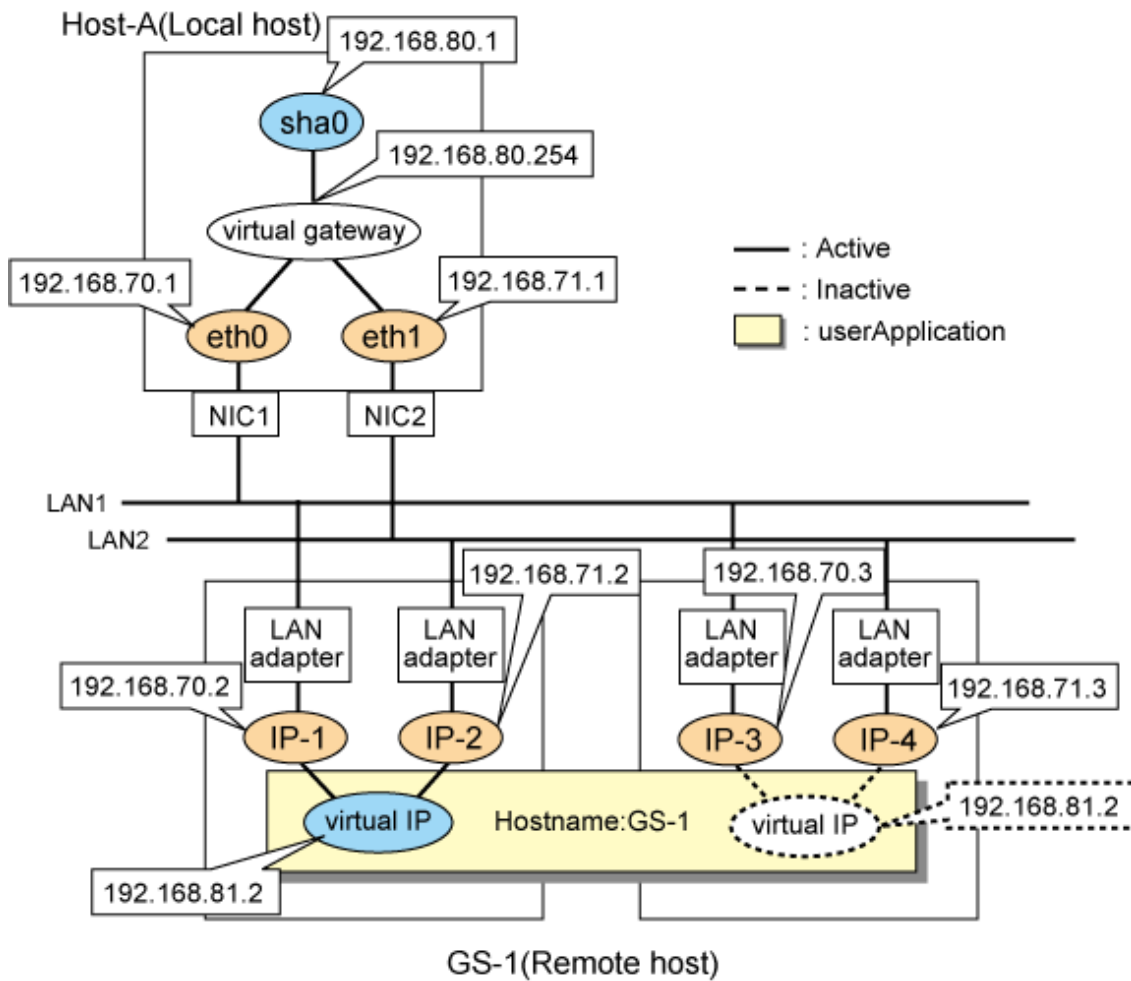
---

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

For the GS configuration, refer to GS manual.

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/hosts file.

```
192.168.70.1    host11    # HOST-A Physical IP
192.168.71.1    host12    # HOST-A Physical IP
192.168.80.1    hosta      # HOST-A Virtual IP
192.168.80.254 virgw      # Virtual gateway
192.168.70.2    gs11      # GS-1 Physical IP(IP-1)
192.168.71.2    gs12      # GS-1 Physical IP(IP-2)
192.168.70.3    gs13      # GS-1 Physical IP(IP-3)
192.168.71.3    gs14      # GS-1 Physical IP(IP-4)
192.168.81.2    gsa        # GS-1 Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
```

```
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

- 1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

- 1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```
GATEWAY0=192.168.80.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.81.2 # GS-1 Virtual IP
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.2 -t 192.168.70.2,192.168.71.2
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.2 -t 192.168.70.3,192.168.71.3
```

## 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

## 7) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

[GS-1]

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

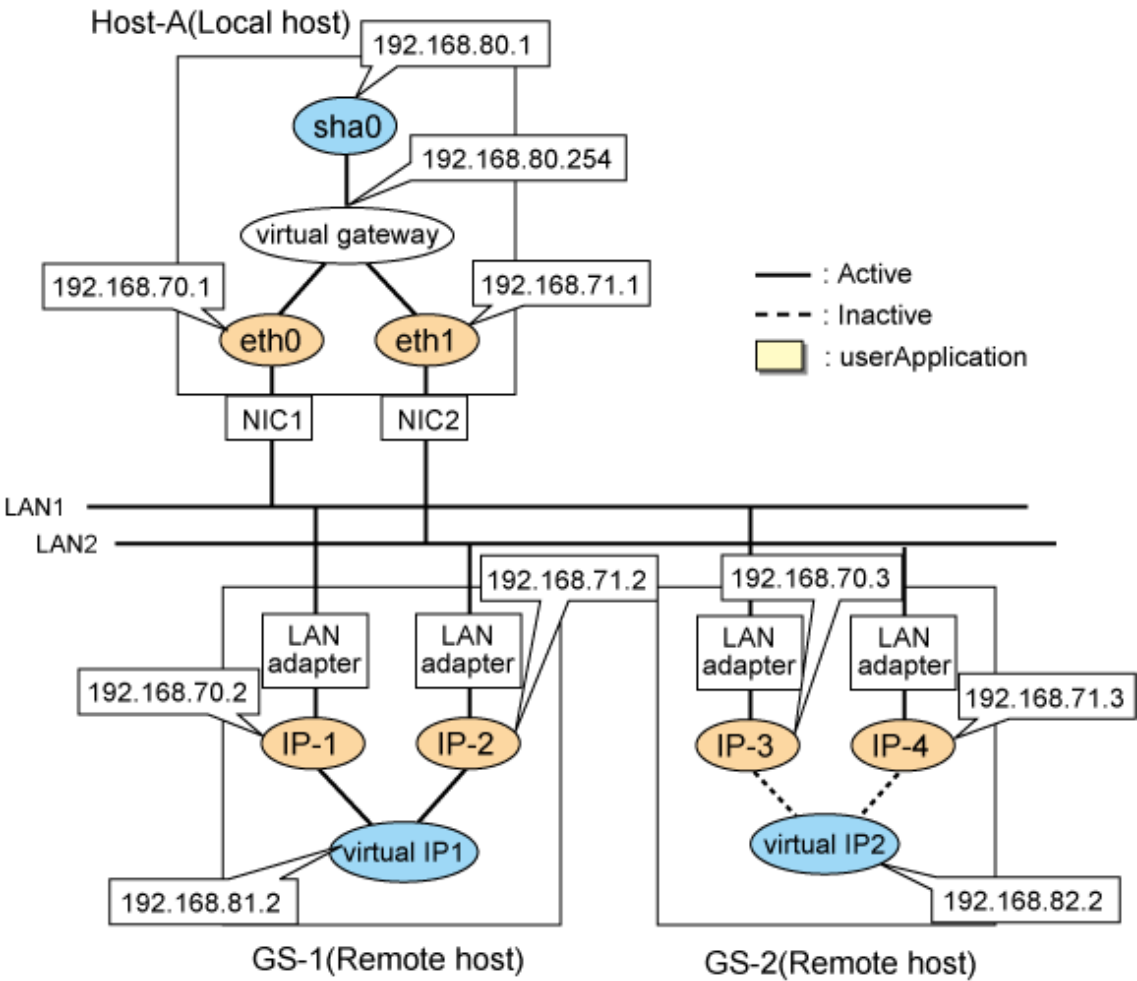
B.8.4 Example of the Single system (GS Load Sharing)

This section describes an example configuration procedure of the network shown in the diagram below.

For the network configuration other than GLS, refer to "3.2.2 Network configuration".

For the GS configuration, refer to GS manual.

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/hosts file.

192.168.70.1	host11	# HOST Physical IP
192.168.71.1	host12	# HOST Physical IP
192.168.80.1	hosta	# HOST Virtual IP
192.168.80.254	virgw	# Virtual gateway
192.168.70.2	gs11	# GS-1 Physical IP (IP-1)
192.168.71.2	gs12	# GS-1 Physical IP (IP-2)
192.168.70.3	gs23	# GS-2 Physical IP (IP-3)
192.168.71.3	gs34	# GS-2 Physical IP (IP-4)
192.168.81.2	gsa	# GS1 Virtual IP
192.168.82.2	gsb	# GS2 Virtual IP

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```
GATEWAY0=192.168.80.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.81.2 # GS-1 Virtual IP of the remote host
GATEWAY1=192.168.80.254 # Virtual gateway
NETMASK1=255.255.255.255 # Subnet mask
ADDRESS1=192.168.82.2 # GS-2 Virtual IP of the remote host
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
```

### 5) Setting the Communication target monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS1 -i 192.168.81.2 -t 192.168.70.2,192.168.71.2  
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS2 -i 192.168.82.2 -t 192.168.70.3,192.168.71.3
```

### 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

### 7) Activating of virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

## [GS]

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## B.8.5 Example of the Cluster system (1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

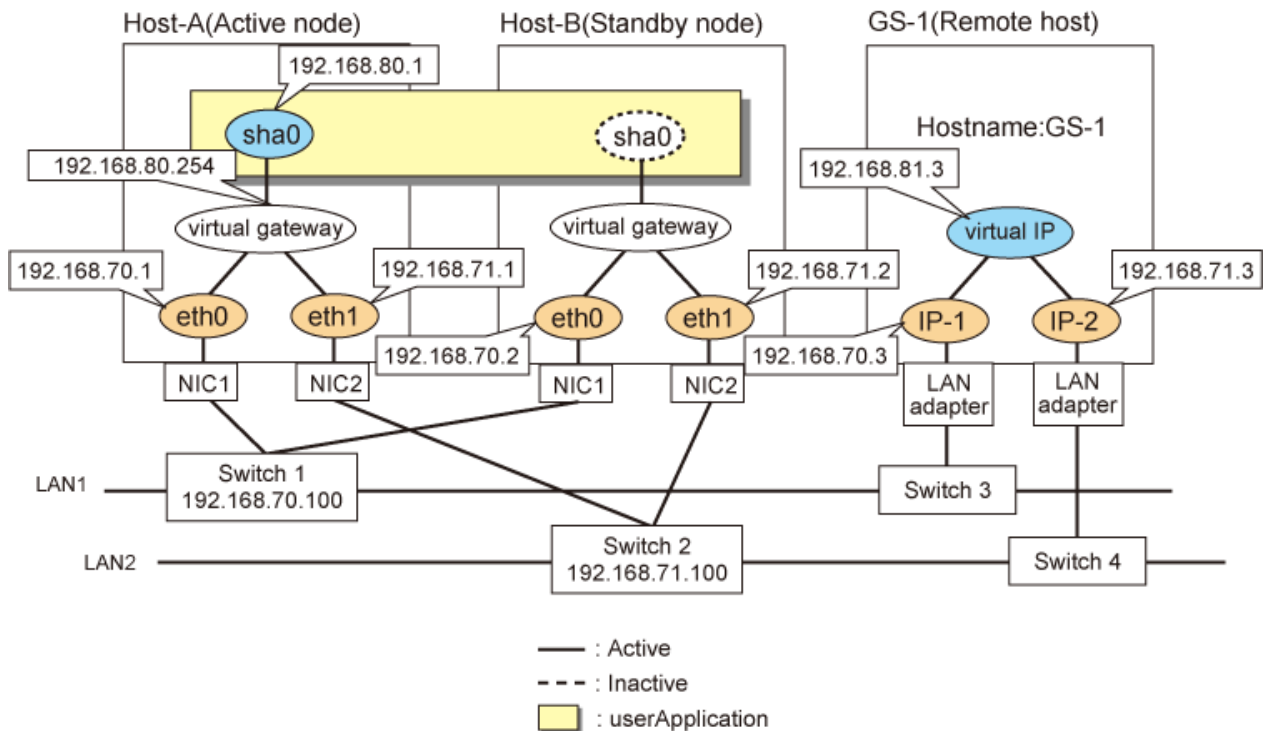
For the network configuration other than GLS, refer to "3.2.2 Network configuration".

For the GS configuration, refer to 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/hosts file.

192.168.70.1	host11	# HOST-A Physical IP
192.168.71.1	host12	# HOST-A Physical IP
192.168.70.2	host11	# HOST-B Physical IP
192.168.71.2	host12	# HOST-B Physical IP
192.168.80.1	hosta	# HOST-A/B Virtual IP(Takeover virtual IP)



```
192.168.80.254 virgw # Virtual gateway
192.168.70.3 gs11 # GS-1 Physical IP(IP-1)
192.168.71.3 gs12 # GS-1 Physical IP(IP-2)
192.168.81.3 gsa # GS-1 Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```
GATEWAY0=192.168.80.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.81.3 # GS-1 Virtual IP
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

### Setting the Remote host monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.3 -t 192.168.70.3,192.168.71.3
```

### Setting the destination cluster node monitoring information and the switches monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t  
192.168.70.2,192.168.71.2,192.168.70.100,192.168.71.100
```



### Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

## 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

## 7) Creating 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/hosts file. Defined information is the same as for HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.70.255  
IPADDR=192.168.70.2  
NETMASK=255.255.255.0  
NETWORK=192.168.70.0  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1  
BOOTPROTO=static  
HWADDR=XX:XX:XX:XX:XX:XX  
HOTPLUG=no  
BROADCAST=192.168.71.255  
IPADDR=192.168.71.2  
NETMASK=255.255.255.0  
NETWORK=192.168.71.0
```

```
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name". The information is set in the same way as for HOST-A.

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

**Setting the Remote host monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.81.3 -t 192.168.70.3,192.168.71.3
```

**Setting the destination cluster node monitoring information and the switches monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t
192.168.70.1,192.168.71.1,192.168.70.100,192.168.71.100
```



## Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

## 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
```

## 7) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After completing the procedure 7) for HOST-A and HOST-B, use the RMS Wizard to set up the cluster environment.

Select the SysNode for HOST-A and HOST-B when creating GLS resources, and then register the created GLS resources with the cluster applications.

When registering the GLS resources with the cluster applications, select the SysNode for HOST-A and HOST-B in order of the operation node and the standby node, and then register the takeover IP 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.

## [GS-1]

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## B.8.6 Example of the Cluster system on remote network(1:1 Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

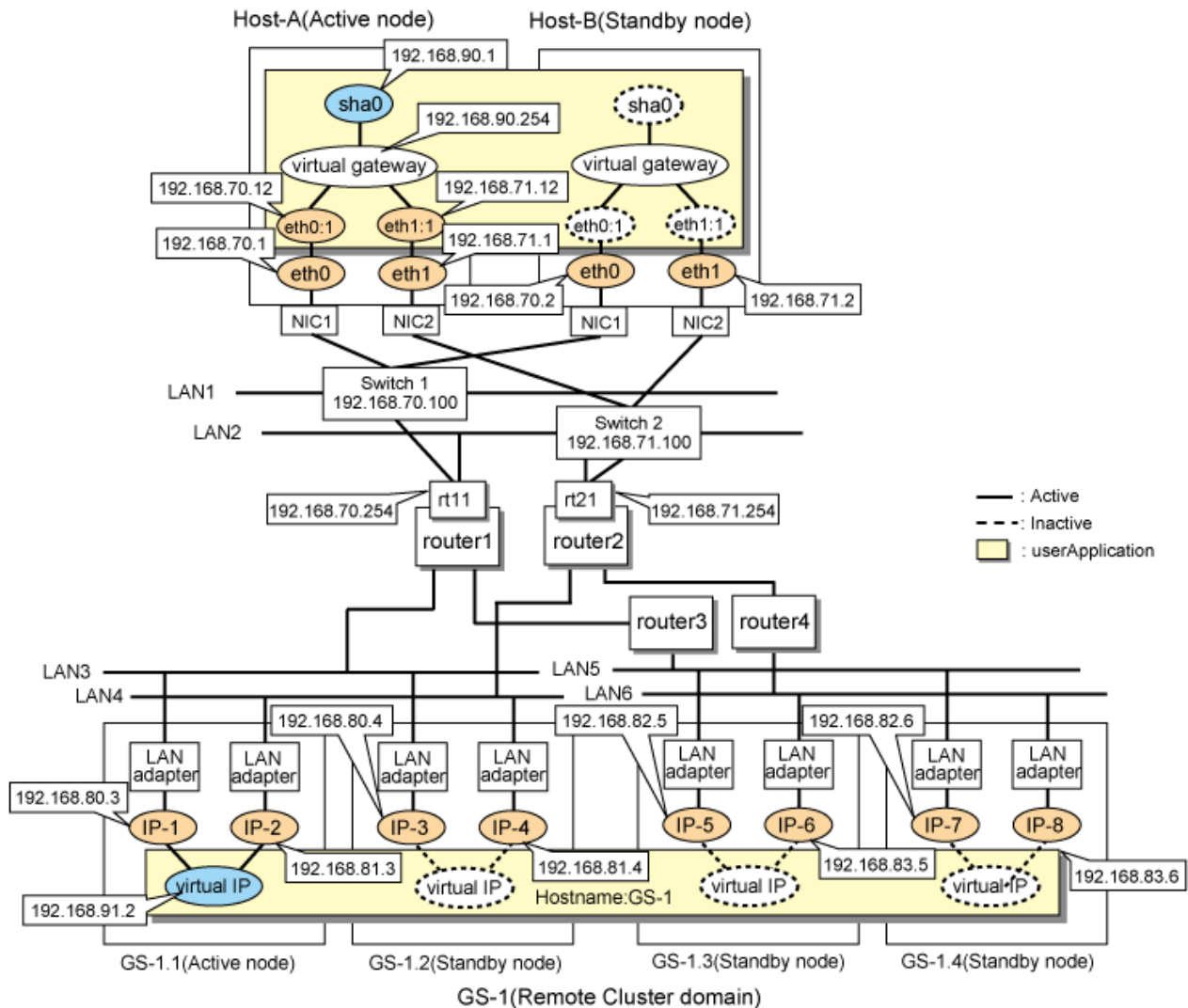
For the network configuration other than GLS, refer to "3.2.2 Network configuration".

For the GS configuration, refer to 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/hosts file.

```
192.168.70.1    host11   # HOST-A Physical IP
192.168.71.1    host12   # HOST-A Physical IP
192.168.70.2    host11   # HOST-B Physical IP
192.168.71.2    host12   # HOST-B Physical IP
192.168.70.12   host111  # HOST-A/B Logical IP
```

```

192.168.71.12    host121  # HOST- A/B Logical IP
192.168.90.1    hosta    # HOST-A/B Virtual IP(Takeover virtual IP)
192.168.90.254  virgw    # Virtual gateway
192.168.70.254  rt11     # Router1
192.168.71.254  rt21     # Router2
192.168.80.3    gs11     # GS-1 Physical IP(IP-1)
192.168.81.3    gs12     # GS-1 Physical IP(IP-2)
192.168.80.4    gs21     # GS-1 Physical IP(IP-3)
192.168.81.4    gs22     # GS-1 Physical IP(IP-4)
192.168.82.5    gs31     # GS-1 Physical IP(IP-5)
192.168.83.5    gs32     # GS-1 Physical IP(IP-6)
192.168.82.6    gs41     # GS-1 Physical IP(IP-7)
192.168.83.6    gs42     # GS-1 Physical IP(IP-8)
192.168.91.2    gsa      # GS-1 Virtual IP

```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```

DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet

```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```

GATEWAY0=192.168.90.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.91.2   # GS-1 Virtual IP

```

- Contents of /etc/sysconfig/network-scripts/route-eth0

```
GATEWAY0=192.168.70.254 # Local router 1 on the local host
NETMASK0=255.255.255.0 # Subnet mask
ADDRESS0=192.168.80.0 # Physical IP of the remote host (network address)
GATEWAY1=192.168.70.254 # Local router 1 on the local host
NETMASK1=255.255.255.0 # Subnet mask
ADDRESS1=192.168.82.0 # Physical IP of the remote host (network address)
```

- Contents of /etc/sysconfig/network-scripts/route-eth1

```
GATEWAY0=192.168.71.254 # Local router 2 on the local host
NETMASK0=255.255.255.0 # Subnet mask
ADDRESS0=192.168.81.0 # Physical IP of the remote host (network address)
GATEWAY1=192.168.71.254 # Local router 2 on the local host
NETMASK1=255.255.255.0 # Subnet mask
ADDRESS1=192.168.83.0 # Physical IP of the remote host (network address)
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.90.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.90.1 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

**Setting the Remote host monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.80.3,192.168.71.254+192.168.81.3
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.80.4,192.168.71.254+192.168.81.4
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.82.5,192.168.71.254+192.168.83.5
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.82.6,192.168.71.254+192.168.83.6
```

**Setting the destination cluster node monitoring information and the switches monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.90.1 -t
192.168.70.2,192.168.71.2,192.168.70.100,192.168.71.100
```



### Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

## 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.90.254
```

## 7) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -e 192.168.70.12,192.168.71.12
```



## Note

In the cluster configuration, if you want to connect via routers (including LANC2), specify the gateway IP address for the takeover virtual IP address in the "-e" option. Additionally, use the hanetmask command to check that the subnet mask for the gateway IP address has been set.

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined information is the same as for HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name". The information is set in the same way as for HOST-A.

### 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.90.0 -m 255.255.255.0
```

#### 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.90.1 -t eth0,eth1
```

#### 5) Setting the Communication target monitoring function

##### Setting the Remote host monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.80.3,192.168.71.254+192.168.81.3
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.80.4,192.168.71.254+192.168.81.4
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.82.5,192.168.71.254+192.168.83.5
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.2 -t
192.168.70.254+192.168.82.6,192.168.71.254+192.168.83.6
```

##### Setting the destination cluster node monitoring information and the switches monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.90.1 -t
192.168.70.1,192.168.71.1,192.168.70.100,192.168.71.100
```



#### Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

#### 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.90.254
```

#### 7) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -e 192.168.70.12,192.168.71.12
```



#### Note

In the cluster configuration, if you want to connect via routers (including LANC2), specify the gateway IP address for the takeover virtual IP address in the "-e" option. Additionally, use the hanetmask command to check that the subnet mask for the gateway IP address has been set.

### [Configuration by RMS Wizard]

#### 1) Configuration of userApplication

After completing the procedure 7) for HOST-A and HOST-B, use the RMS Wizard to set up the cluster environment.

Select the SysNode for HOST-A and HOST-B when creating GLS resources, and then register the created GLS resources with cluster applications.

When registering the GLS resources with the cluster applications, select the SysNode for HOST-A and HOST-B in order of the operation node and the standby node, and then register the takeover IP address "192.168.90.1".

#### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.



## [Router setting]

Set the route information as follows for the virtual IP addresses for Route 1 and Route 2. Make sure that the router neighboring GLS is RIPv1 and the path to GS's virtual IP address is broadcast. How to set the route information depends on the type of router, so read the manual for your router for information on how to set it.

Route1	Destination: 192.168.90.1	Gateway address: 192.168.70.12
Route2	Destination: 192.168.90.1	Gateway address: 192.168.71.12

## [GS-1]

Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## B.8.7 Example of the Cluster system (Mutual Standby)

This section describes an example configuration procedure of the network shown in the diagram below.

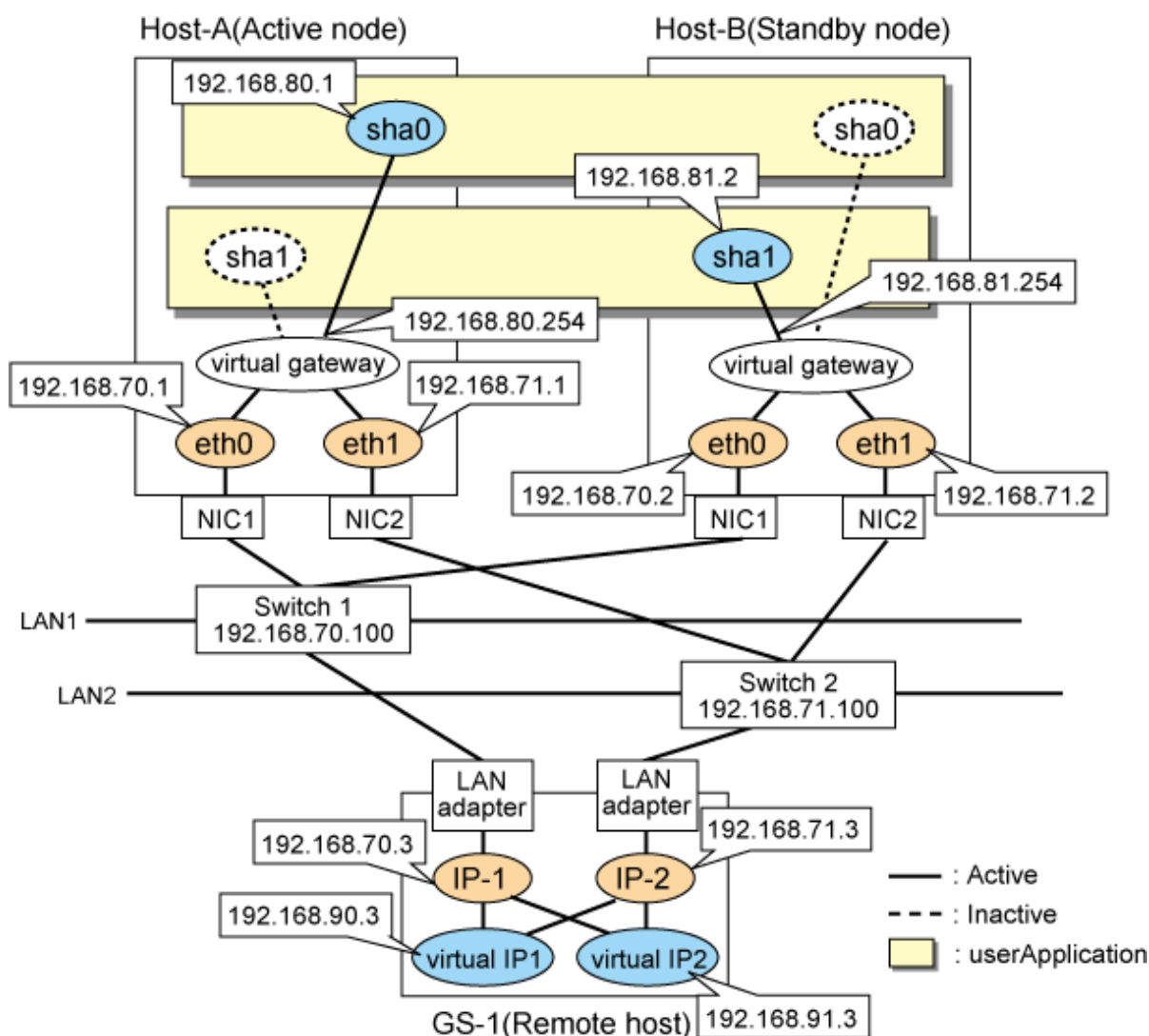
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

For the GS configuration, refer to 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/hosts file.

```
192.168.70.1    host11  # HOST-A Physical IP
192.168.71.1    host12  # HOST-A Physical IP
192.168.70.2    host11  # HOST-B Physical IP
192.168.71.2    host12  # HOST-B Physical IP
192.168.80.1    hosta    # HOST-A/B Virtual IP(Takeover virtual IP)
192.168.81.2    hostb    # HOST-A/B Virtual IP(Takeover virtual IP)
192.168.80.254  virgw    # Virtual gateway
192.168.81.254  virgw    # Virtual gateway
192.168.70.3    gs11     # GS-1 Physical IP(IP-1)
192.168.71.3    gs12     # GS-1 Physical IP(IP-2)
192.168.90.3    gsa      # GS-1 Virtual IP
192.168.91.3    gsb      # GS-1 Virtual IP
```

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



### Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name".

- Contents of /etc/sysconfig/network-scripts/route-sha0

```
GATEWAY0=192.168.80.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.90.3 # GS-1 Virtual IP
```

- Contents of /etc/sysconfig/network-scripts/route-sha1

```
GATEWAY0=192.168.81.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.91.3 # GS-1 Virtual IP
```

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.81.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.81.2 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

**Setting the Remote host monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.90.3 -t 192.168.70.3,192.168.71.3
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.3 -t 192.168.70.3,192.168.71.3
```

**Setting the destination cluster node monitoring information and the switches monitoring information:**

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.80.1 -t
192.168.70.2,192.168.71.2,192.168.70.100,192.168.71.100
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.81.2 -t
192.168.70.2,192.168.71.2,192.168.70.100,192.168.71.100
```



### Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

## 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.81.254
```

## 7) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## [HOST-B]

### 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file. Defined information is the same as for HOST-A.

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.



## Note

The following setting example (/etc/sysconfig/network-scripts/ifcfg-ethX) is for RHEL5. For details, see "[3.2.2 Network configuration](#)".

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.2
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```

1-3) When the system is RHEL, on the /etc/sysconfig/network file, define a statement which enables the network configuration.

```
NETWORKING=yes
```

1-4) Set the static route information of the virtual gateway for the remote host's virtual IP address in /etc/sysconfig/network-scripts/route-"interface name". The information is set in the same way as for HOST-A.

## 2) Reboot

Run the following command to reboot the system. After rebooting the system, verify eth0 and eth1 are active using ifconfig command.

```
/sbin/shutdown -r now
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.81.0 -m 255.255.255.0
```

## 4) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.80.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m c -i 192.168.81.2 -t eth0,eth1
```

## 5) Setting the Communication target monitoring function

Setting the Remote host monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.90.3 -t 192.168.70.3,192.168.71.3
/opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.91.3 -t 192.168.70.3,192.168.71.3
```

Setting the destination cluster node monitoring information and the switches monitoring information:

```
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.80.1 -t
192.168.70.1,192.168.71.1,192.168.70.100,192.168.71.100
/opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.81.2 -t
192.168.70.1,192.168.71.1,192.168.70.100,192.168.71.100
```



## Note

When you set the destination cluster node monitoring information and the switches monitoring information, be sure to specify the takeover IP address with the "-i" option.

### 6) Setting a virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.80.254
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.81.254
```

### 7) Creating of takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring HOST-A and HOST-B, register the created takeover virtual interface as a GIs resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## [GS-1]

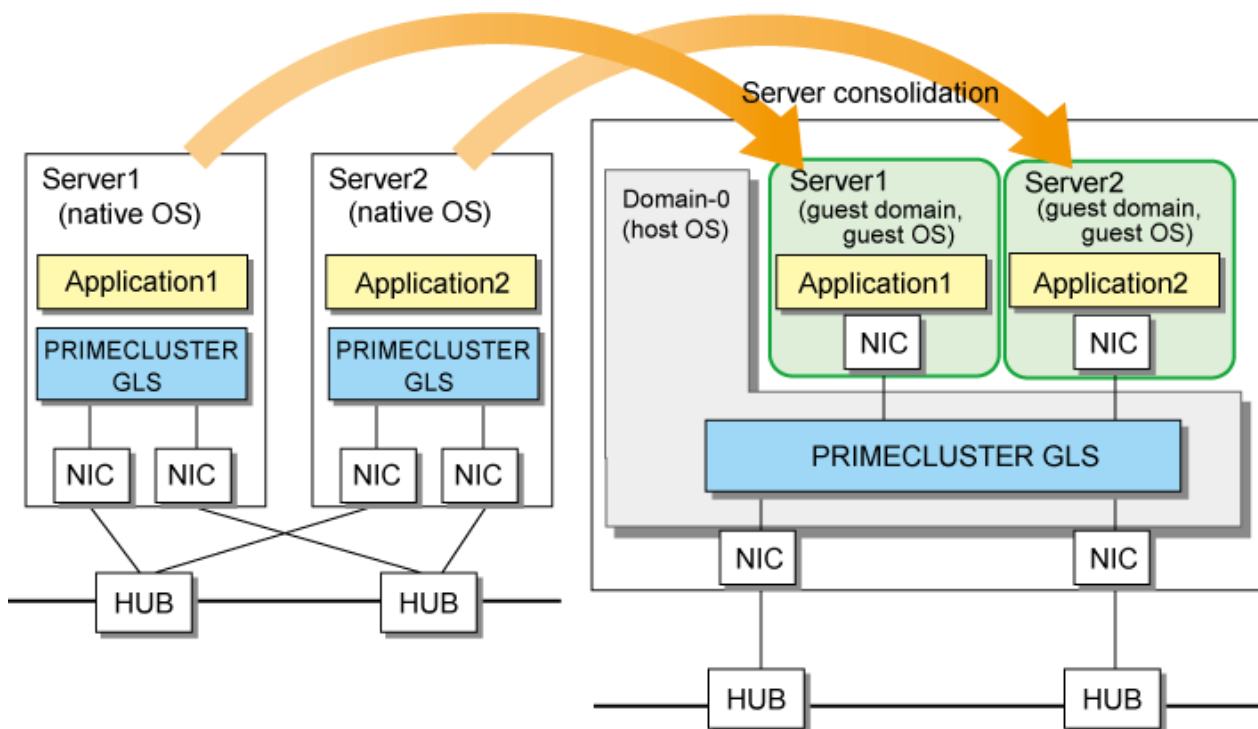
Set the information for HOST-A's physical IP address and virtual IP address. For information on how to do this, see the GS manual.

## Appendix C Operation on the Virtual Machine Function (For RHEL5)

This chapter describes the operation of GLS on the virtual machine function. For details on the virtual machine function, see the RHEL manuals.

### C.1 Virtual machine function overview

The virtual machine function is a virtual machine monitor (VMM) for running multiple operating systems at once on one server. Virtualization enables you to consolidate multiple servers on one server, which also enables you to multiplex communication links on one server, rather than one for each server.

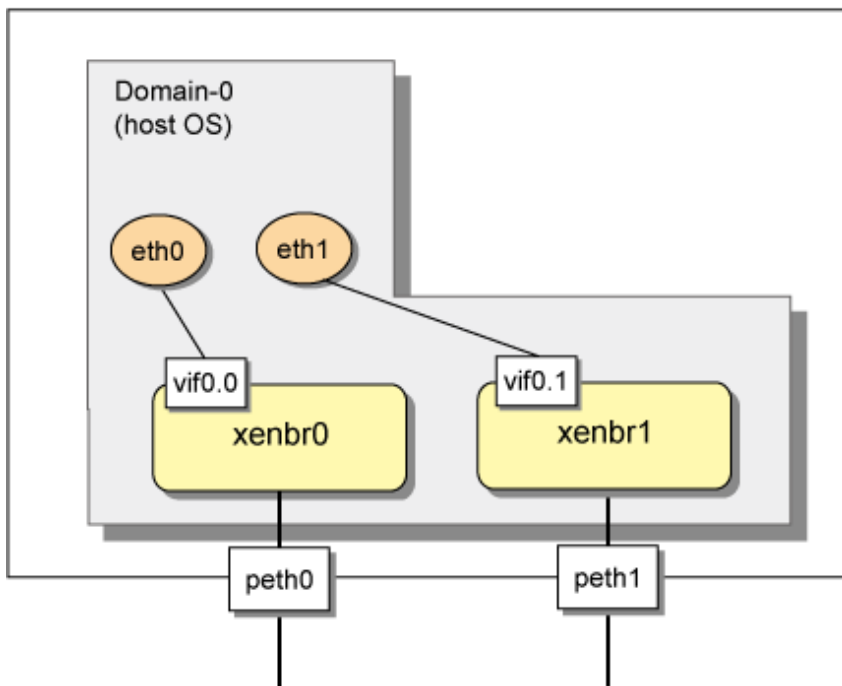


### C.2 Configuration of the virtual machine function

The virtual machine running the operating system is called a domain. The host OS, called Domain-0, is booted at system startup.

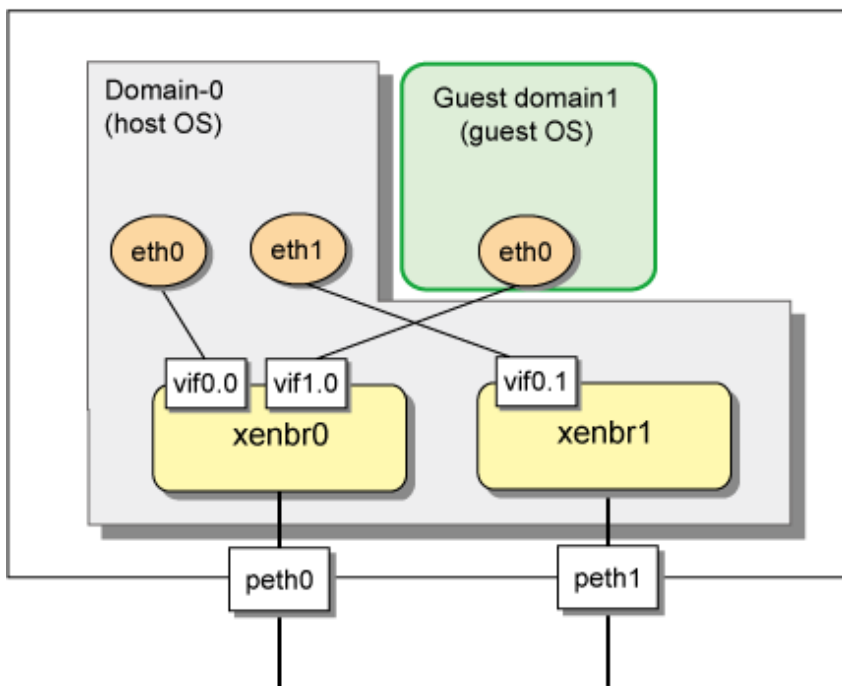
The interface, called ethX, is created so Domain-0 can access communications, and the interface vif0.X for connecting Domain-0's ethX and the server as well as the interface path for external connections are created. These are created for each NIC on the server. In addition, the virtual bridge called xenbrX is created to connect vif0.X and pethX for external connections.

## Server

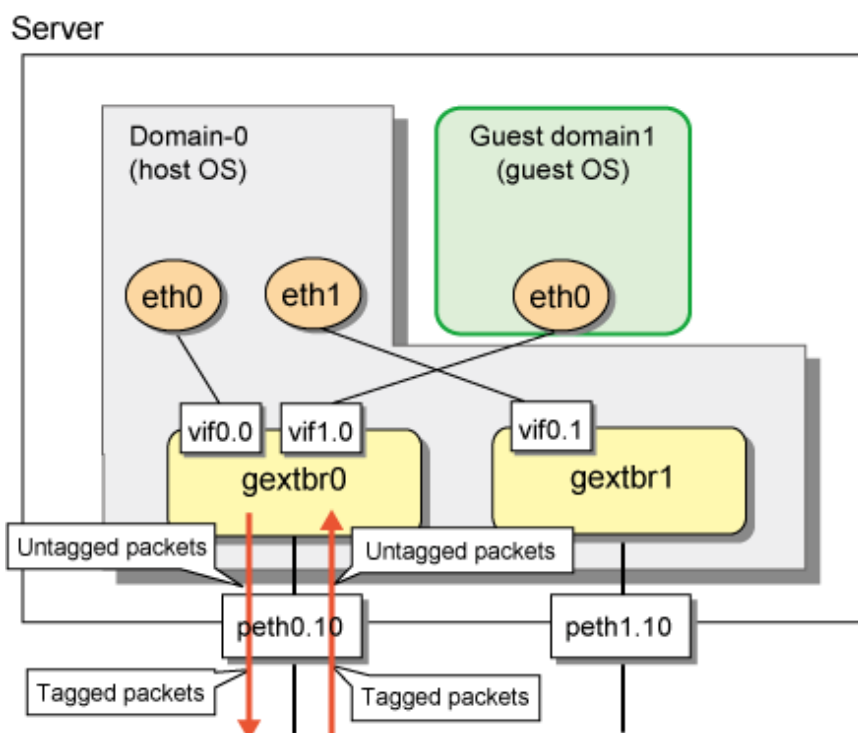


When you create a new guest domain (domain U) and boot the operating system, the interface vifU.X for connecting domain U's ethX and the server is created. In addition, vifU.X and the interface pethX for external connections are connected by the virtual bridge, enabling ethX on the guest domain to connect to the outside network.

## Server



If you use the tagged VLAN, a virtual bridge named gextbrX is created. Additionally, an interface pethX.Z (Z is an ID for the tagged VLAN) will be created for sending VLAN-tagged packets outside the server and untagging them when received.



## C.3 Virtual network design

### C.3.1 Concept of network configuration in the virtual machine function

When you use the virtual machine function, we recommend that you use the virtual machine network for the following three uses.

- Communications for administration
- Communications for public use
- Communications for backup

### C.3.2 Support set for each redundant line switching mode

GLS provides highly reliable network communications for the host OS and guest OS. The following table shows the compatibility between redundant line switching methods and domains. Select Fast switching mode if every one of the remote hosts uses Fast switching mode. Other than this mode, select NIC switching mode or Virtual NIC mode.

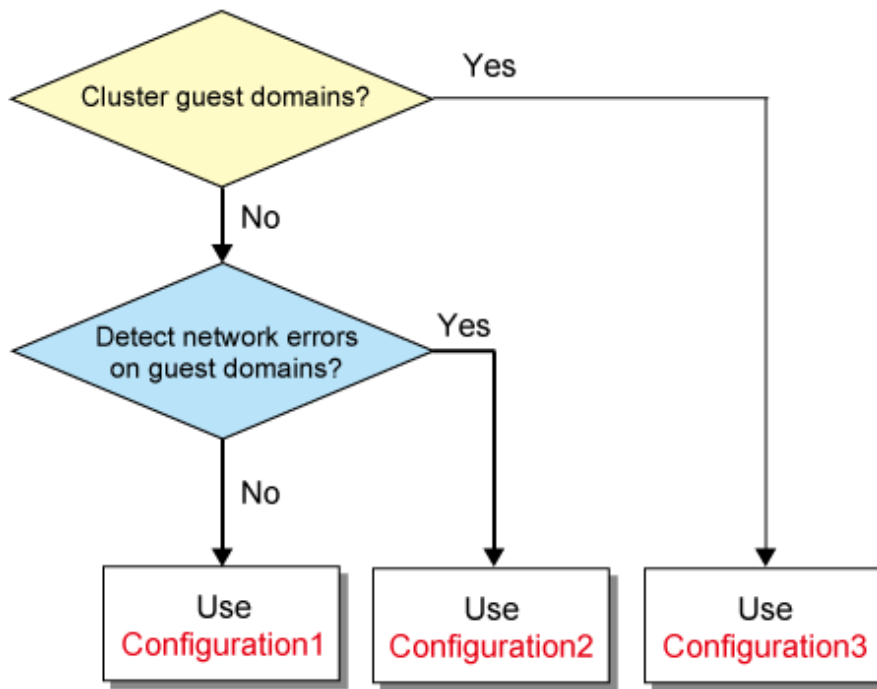
	Domain-0(host OS)	Guest domain(guest OS)
Fast switching mode	O	O
NIC switching mode	O	O
Virtual NIC mode	O	O
GS linkage mode	X	X

O: Supported X: Not supported

### C.3.3 Flow for selecting the virtual network configuration in each redundant line switching mode

Use the following flowchart to select the virtual network configuration for each redundant line switching mode.

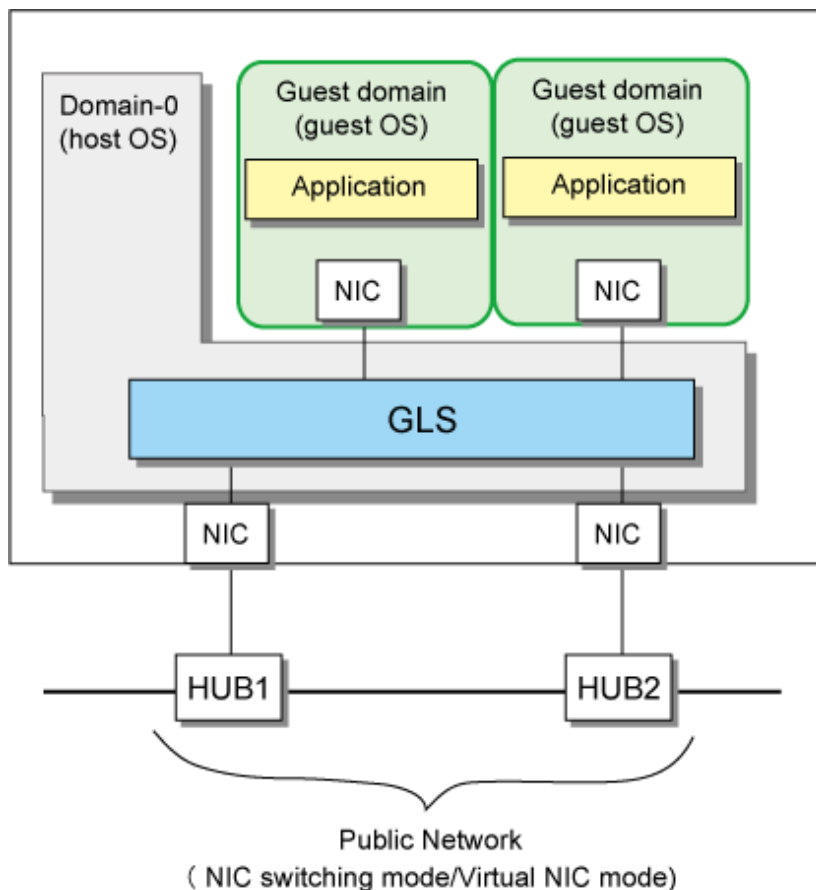




**Configuration 1: Configuration for creating a highly reliable network of guest domains using GLS on domain-0**

Use this configuration when you want guest domains to maintain communications without being aware of network failures and without clustering guest domains. Also, set the NIC switching mode or Virtual NIC mode for domain-0 (host OS).

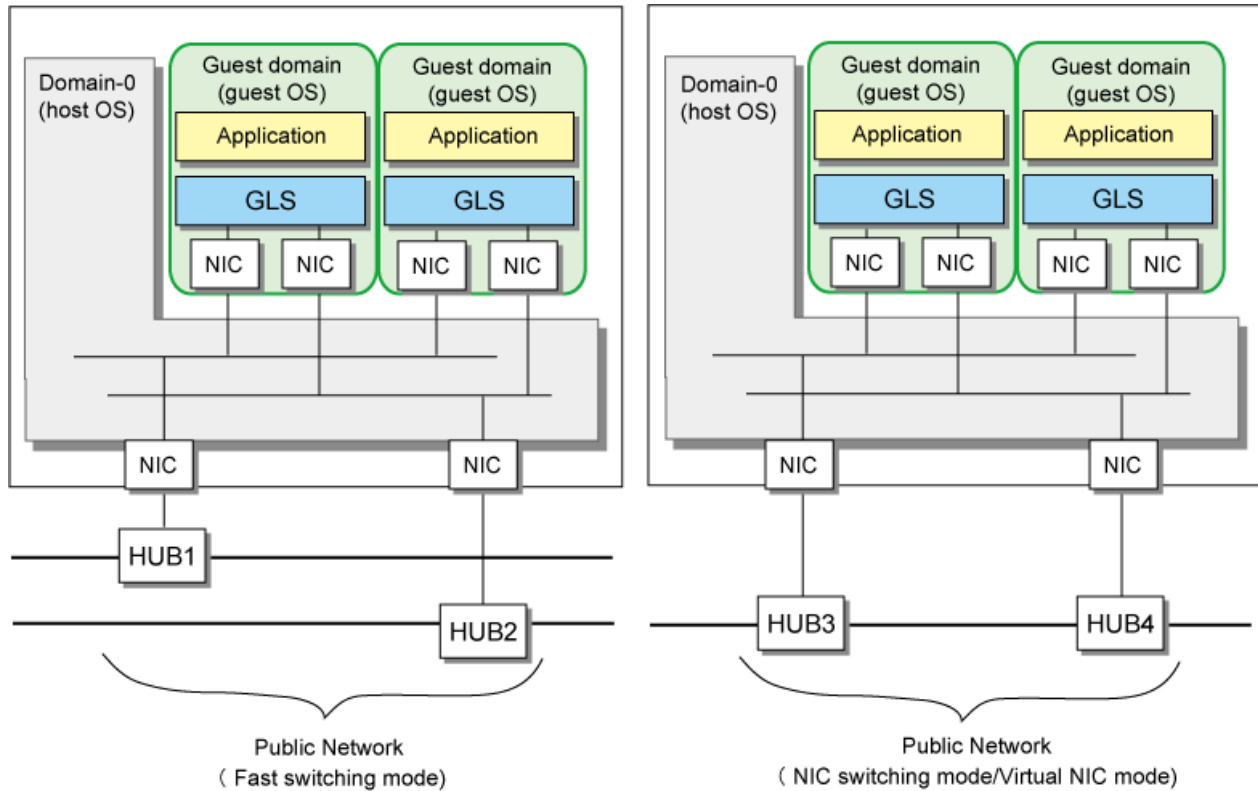
Figure C.1 Configuration 1: Configuration diagram for creating a highly reliable network of guest domains using GLS on domain-0



## Configuration 2: Configuration for creating a highly reliable network on guest domains of a single system

Use this configuration when you want to detect an error on each guest domain in the even of a network failure without clustering guest domains. Note that the Fast switching mode, NIC switching mode, or Virtual NIC mode can be set for each guest domain (guest OS) in this configuration.

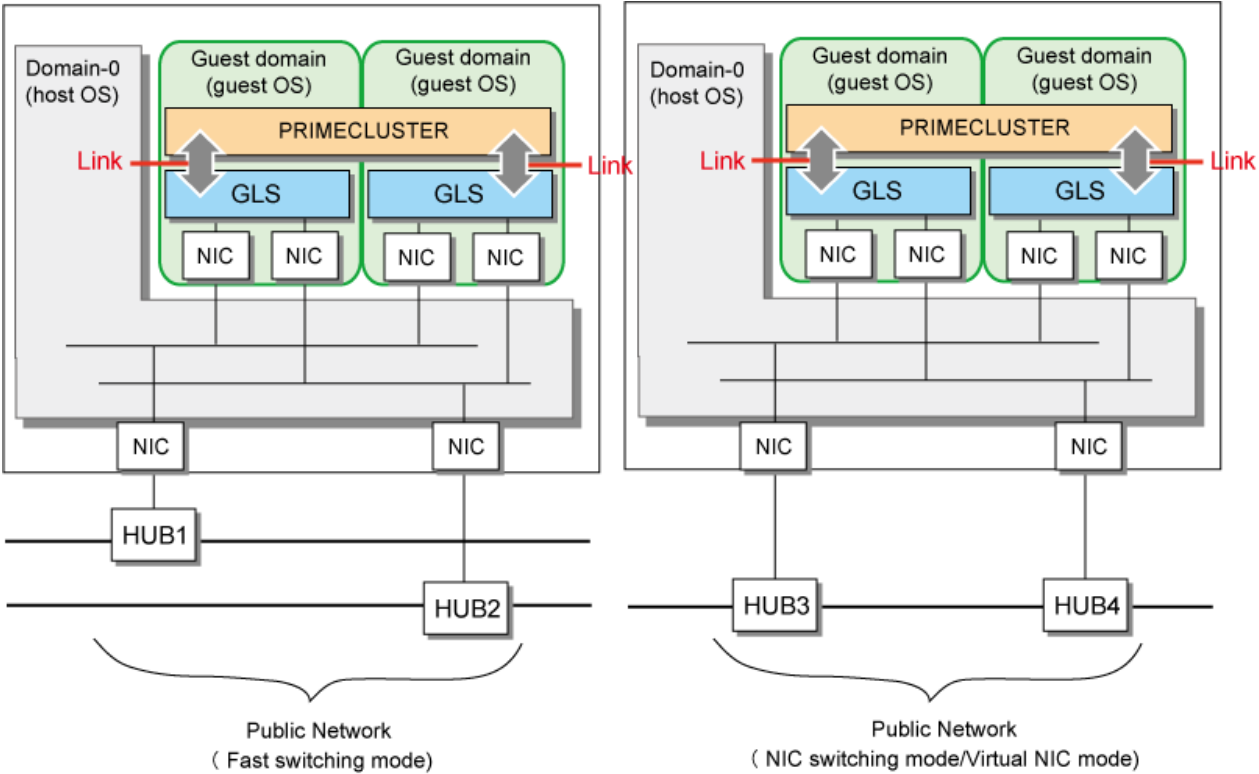
Figure C.2 Configuration 2: Configuration diagram for creating a highly reliable network on guest domains of a single system



## Configuration 3: Configuration for creating a highly reliable network on guest domains of a cluster system

Use this configuration when you want to cluster guest domains. Note that the Fast switching mode, NIC switching mode, or Virtual NIC mode can be set for each guest domain (guest OS) in this configuration.

Figure C.3 Configuration 3: Configuration diagram for creating a highly reliable network on guest domains of a cluster system



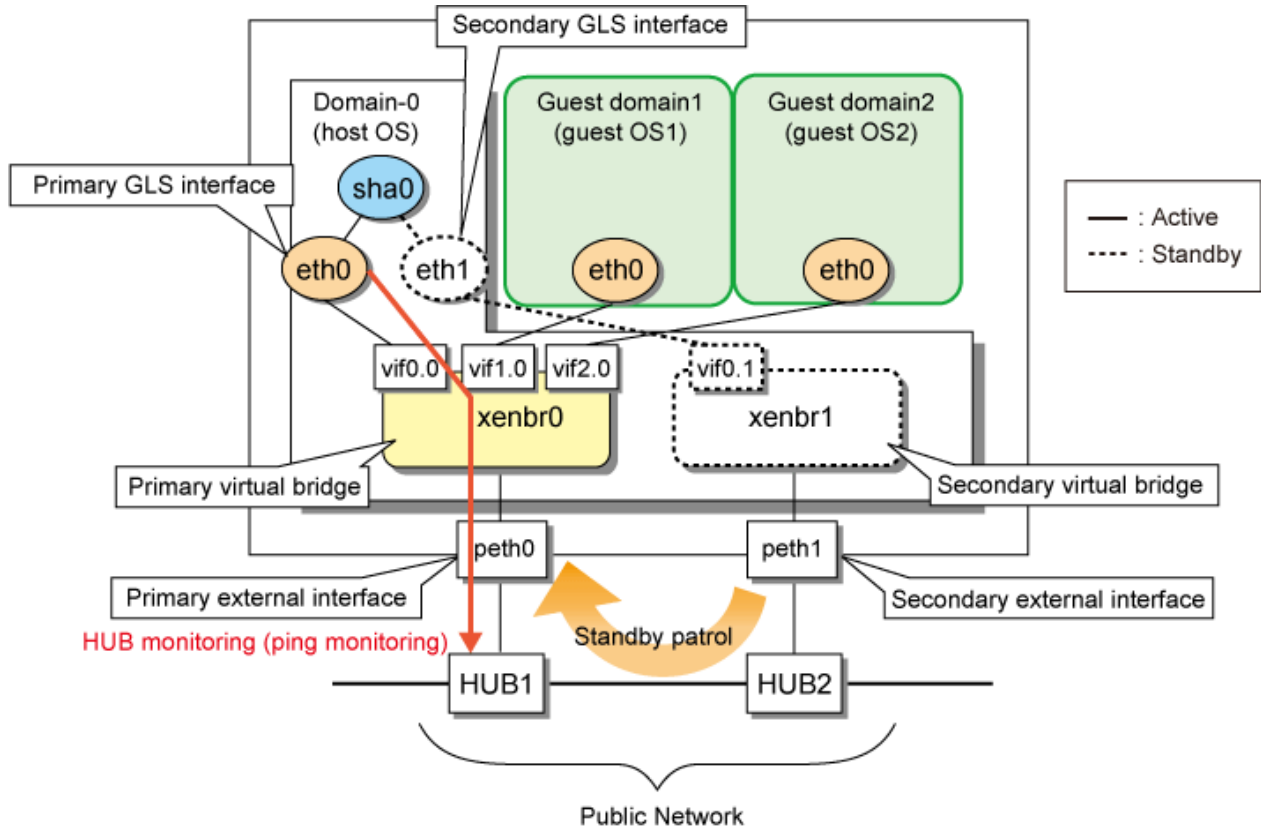
### C.3.4 Details on each configuration

#### Configuration 1: Configuration for creating a highly reliable network of guest domains using GLS on domain-0

##### NIC switching mode

Make the guest domains (guest OSes) on a single system highly reliable using GLS on domain-0 (host OS). GLS takes the configuration for multiplexing virtual bridges for network redundancy. The following illustrates the configuration.

Figure C.4 NIC switching mode



The following describes each component in the figure. Note that the name of a component is defined only in configuration 1.

Name		Descriptions
External interface	Primary external interface	An interface connecting the virtual network on the server and the external network. This interface is initially used for operation after the system startup.
	Secondary external interface	An interface connecting the virtual network on the server and the external network. This interface is initially used for standby after the system startup.
Virtual bridge	Primary virtual bridge	A bridge connected to a guest OS running applications. This bridge is continuously used for operation.
	Secondary virtual bridge	A bridge used as the path for the monitoring frame of a standby patrol. This bridge is continuously used for standby.
GLS interface	Primary GLS interface	An interface for monitoring the transfer route. This bridge is initially used for operation after the system startup.
	Secondary GLS interface	An interface for monitoring the transfer route. This bridge is initially used for standby after the system startup.

Configure the network as follows to use GLS on the virtual machine function.

- The Primary GLS interface and primary external interface are connected to the primary virtual bridge; interfaces of guest domains are connected to the primary virtual bridge.
- The secondary GLS interface and secondary external interface are connected to the secondary virtual bridge; interfaces of guest domains are not connected to the secondary virtual bridge.

To set the NIC switching mode for this configuration, see "[C.7 Examples of configuration setup \(Fast switching mode and NIC switching mode\)](#)".

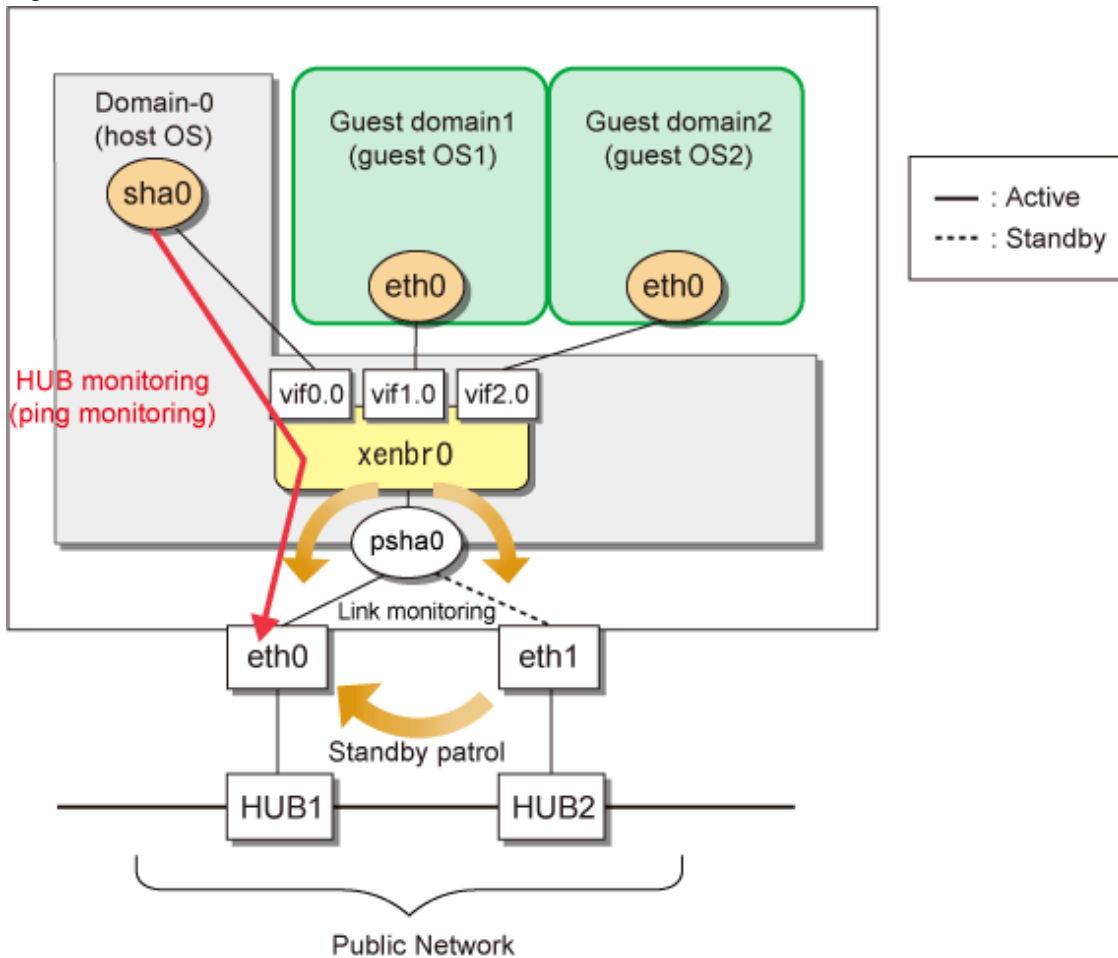
## Point

When you create a redundant administrative network or backup network, you need to design the configuration based on the same concept applied when you create a redundant public network.

### Virtual NIC mode

Make the guest domains (guest OSes) on a single system highly reliable using GLS on domain-0 (host OS). Setting bridges is required for network redundancy in GLS. Be sure to perform this step. The following illustrates the configuration.

Figure C.5 Virtual NIC mode



To set the Virtual NIC mode for this configuration, see "[C.8 Examples of configuration setup \(Virtual NIC mode\)](#)".

## Configuration 2: Configuration for creating a highly reliable network on guest domains of a single system

### Fast switching mode and Virtual NIC mode

- When using Fast switching mode

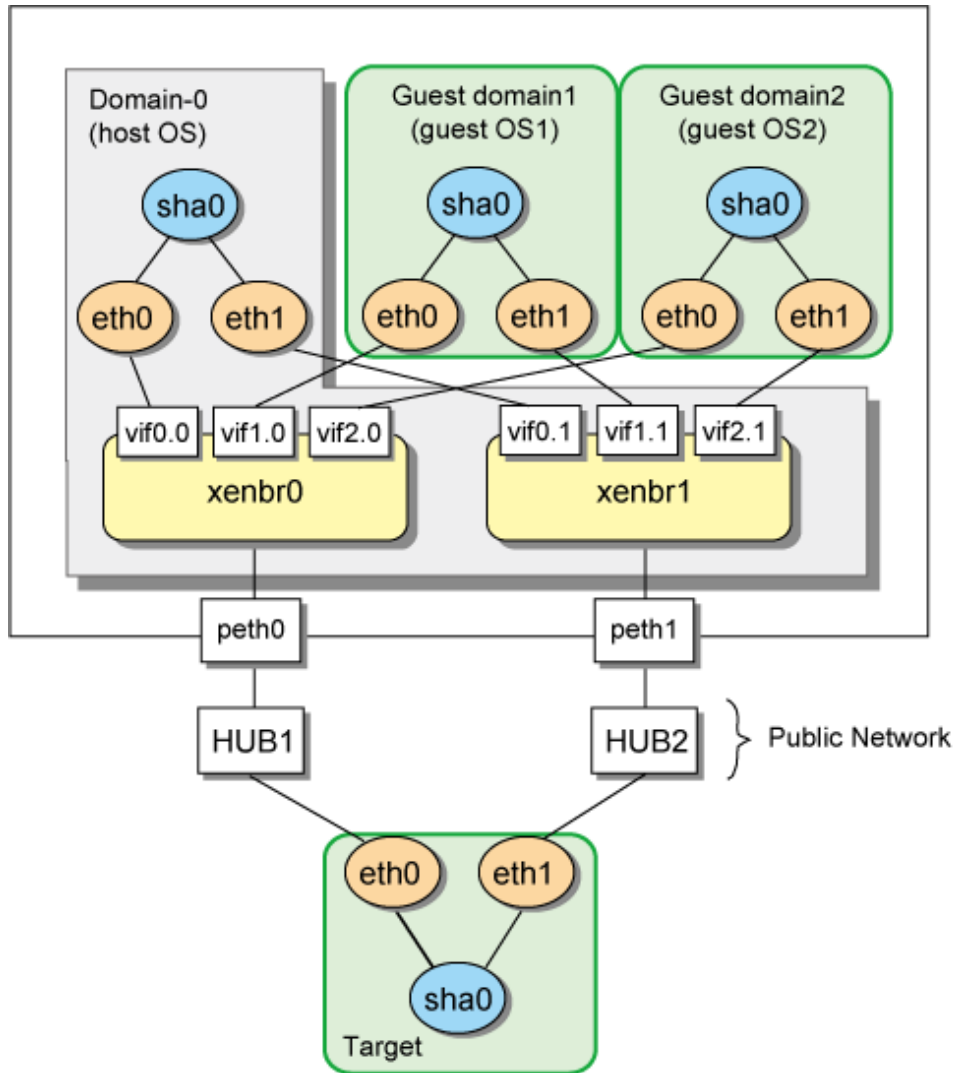
Set the Fast switching mode for the host OS (domain-0) and guest OS (guest domain). See "[B.1.1 Example of the Single system](#)" to set the Fast switching mode for the host OS and guest OS.

- When using Virtual NIC mode

Set the Virtual NIC mode only for the guest OS (guest domain). See "[B.7.1 Example of the Single system](#)" to set the Virtual NIC mode for the guest OS.

Note that GLS multiplexes virtual bridges in order to multiplex NICs. Therefore, you need to set the primary virtual bridge and secondary virtual bridge for the host OS. Be sure to perform this step.

Figure C.6 Fast switching mode and Virtual NIC mode



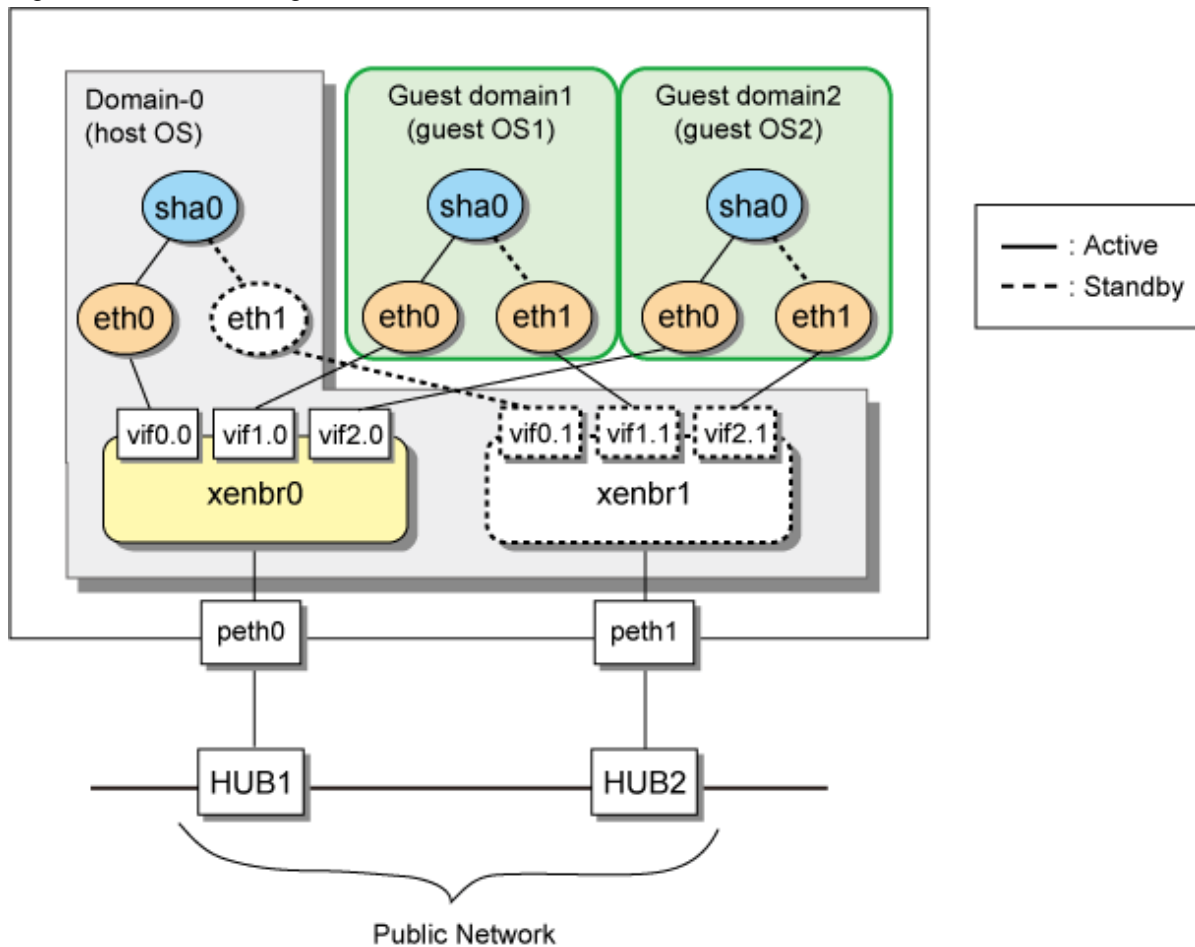
### Point

When you create a redundant administrative network or backup network, you need to design the configuration based on the same concept applied when you create a redundant public network.

### NIC switching mode

Set the NIC switching mode for the host OS (domain-0) and guest OS (guest domain). See "[B.4.1 Example of the Single system without NIC sharing](#)" to set the NIC switching mode for each OS. Note that GLS multiplexes virtual bridges in order to multiplex NICs. Therefore, you need to set the primary virtual bridge and secondary virtual bridge for the host OS. Be sure to perform this step.

Figure C.7 NIC switching mode



### Point

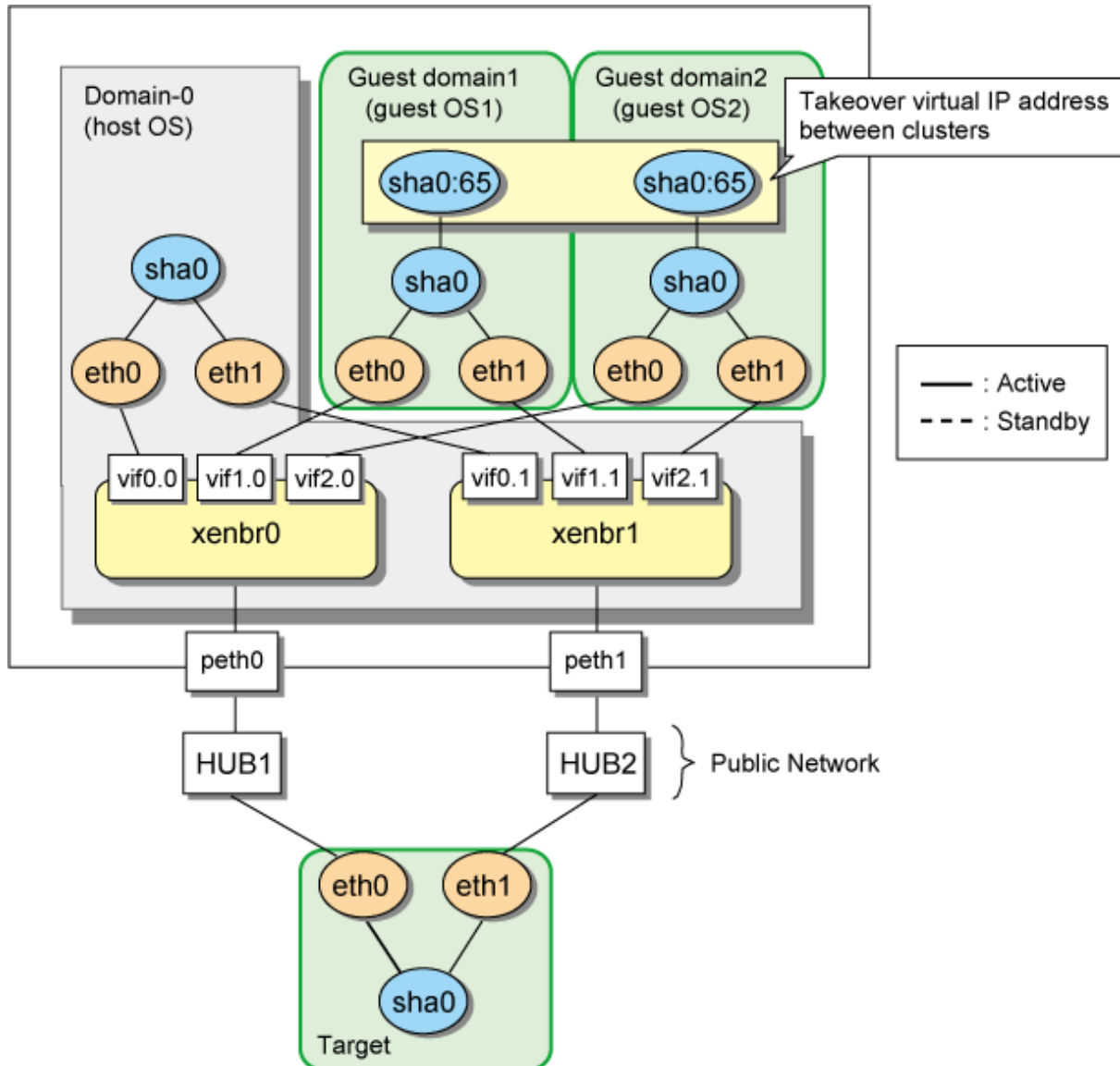
When you create a redundant administrative network or backup network, you need to design the configuration based on the same concept applied when you create a redundant public network.

## Configuration 3: Configuration for creating a highly reliable network on each guest domain of a cluster system

### Fast switching mode and Virtual NIC mode

The settings for Configuration 2 are applied to each OS (host OS and guest OS). In addition, additional cluster settings are required. See "PRIMECLUSTER Installation/Administration Guide" to perform this step.

Figure C.8 Fast switching mode and Virtual NIC mode



### Point

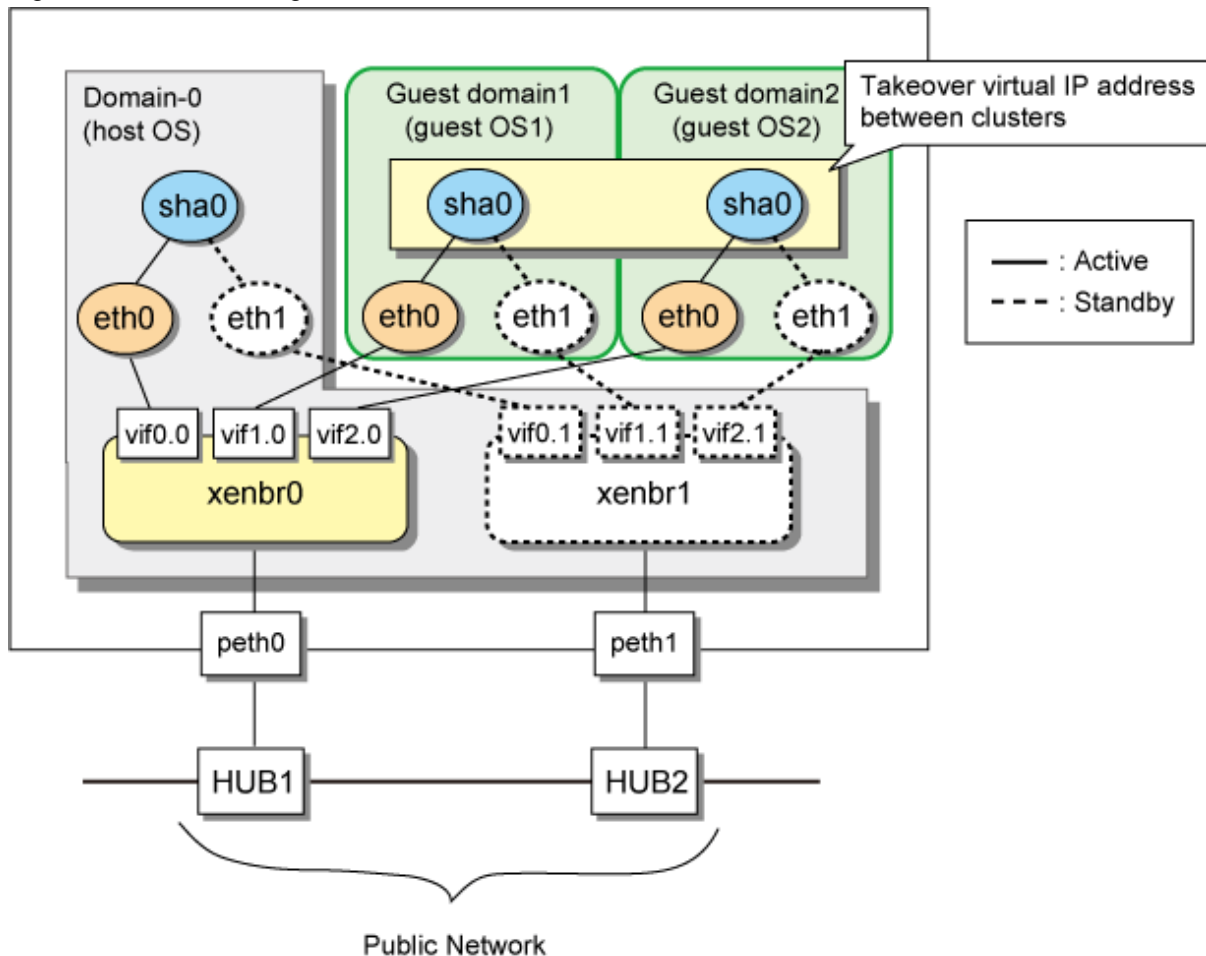
When you create a redundant administrative network or backup network, you need to design the configuration based on the same concept applied when you create a redundant public network.

### NIC switching mode

The settings for Configuration 2 are applied to each OS (host OS and guest OS). In addition, additional cluster settings are required. See "PRIMECLUSTER Installation/Administration Guide" to perform this step.



Figure C.9 NIC switching mode



#### Point

When you create a redundant administrative network or backup network, you need to design the configuration based on the same concept applied when you create a redundant public network.

## C.4 Operation of redundant line switching mode on the virtual machine function

This section describes how to monitor the GLS network for each virtual network configuration and how to switch to a normal network when a network failure occurs.

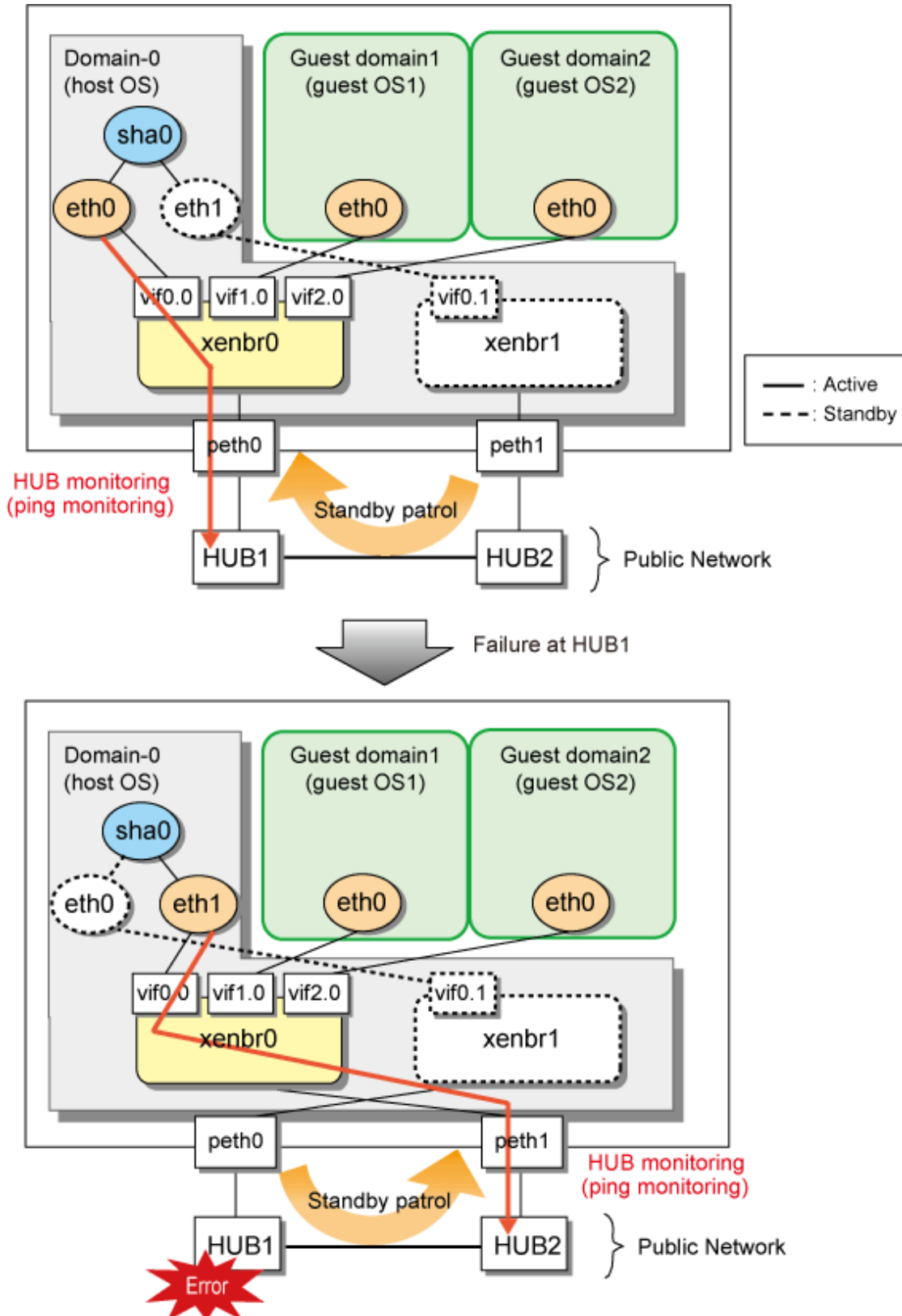
### C.4.1 Configuration for creating a highly reliable network of guest domains with GLS on domain-0 (Configuration 1)

This section describes the operation of the configuration (configuration 1) to create a highly reliable network of guest domains using GLS on domain-0.

#### NIC switching mode

If GLS on the host OS operates on the primary interface (eth0), HUB monitoring (ping monitoring) is performed for HUB1 through peth0. If a failure occurred on HUB1, GLS switches the path from the primary interface (eth0) to the secondary interface (eth1) to keep connection.

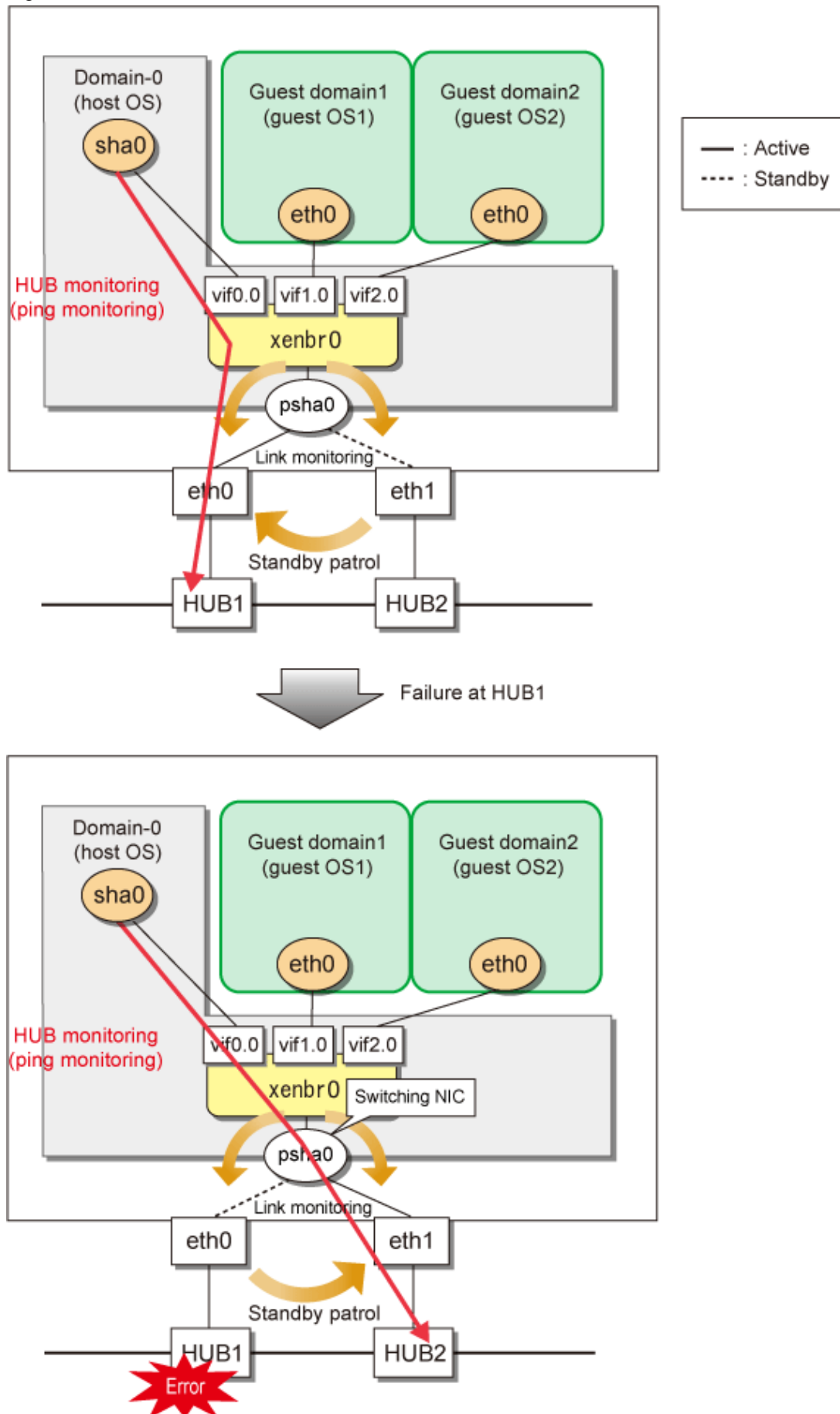
Figure C.10 NIC switching mode



#### Virtual NIC mode

If GLS on the host OS operates on the primary interface (`eth0`), HUB monitoring (ping monitoring) is performed for HUB1 through `psha0`. If a failure occurred on HUB1, GLS switches the path from the primary interface (`eth0`) to the secondary interface (`eth1`) to keep connection.

Figure C.11 Virtual NIC mode



## **C.4.2 Configuration for creating a highly reliable network on guest domains of a single system (Configuration 2)**

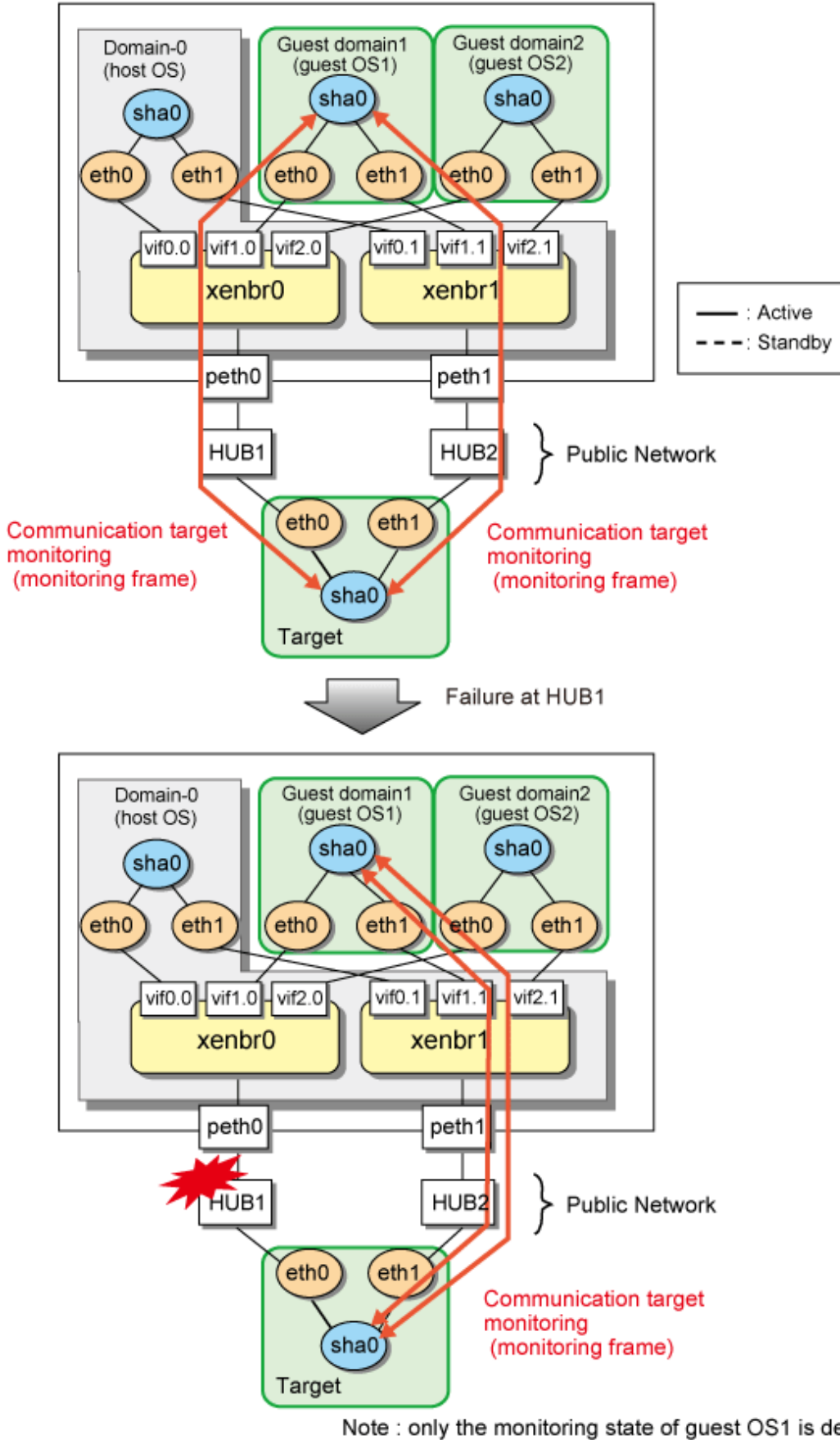
---

This section describes the operation of the configuration (configuration 2) to create a highly reliable network on guest domains of a single system.

### **Fast switching mode**

GLS on the guest OS uses eth0 and eth1 at the same time to monitor the application communications and transfer route. If a failure occurs on HUB1, GLS on the guest OS stops using eth0 and maintains communications using only eth1.

Figure C.12 Fast switching mode

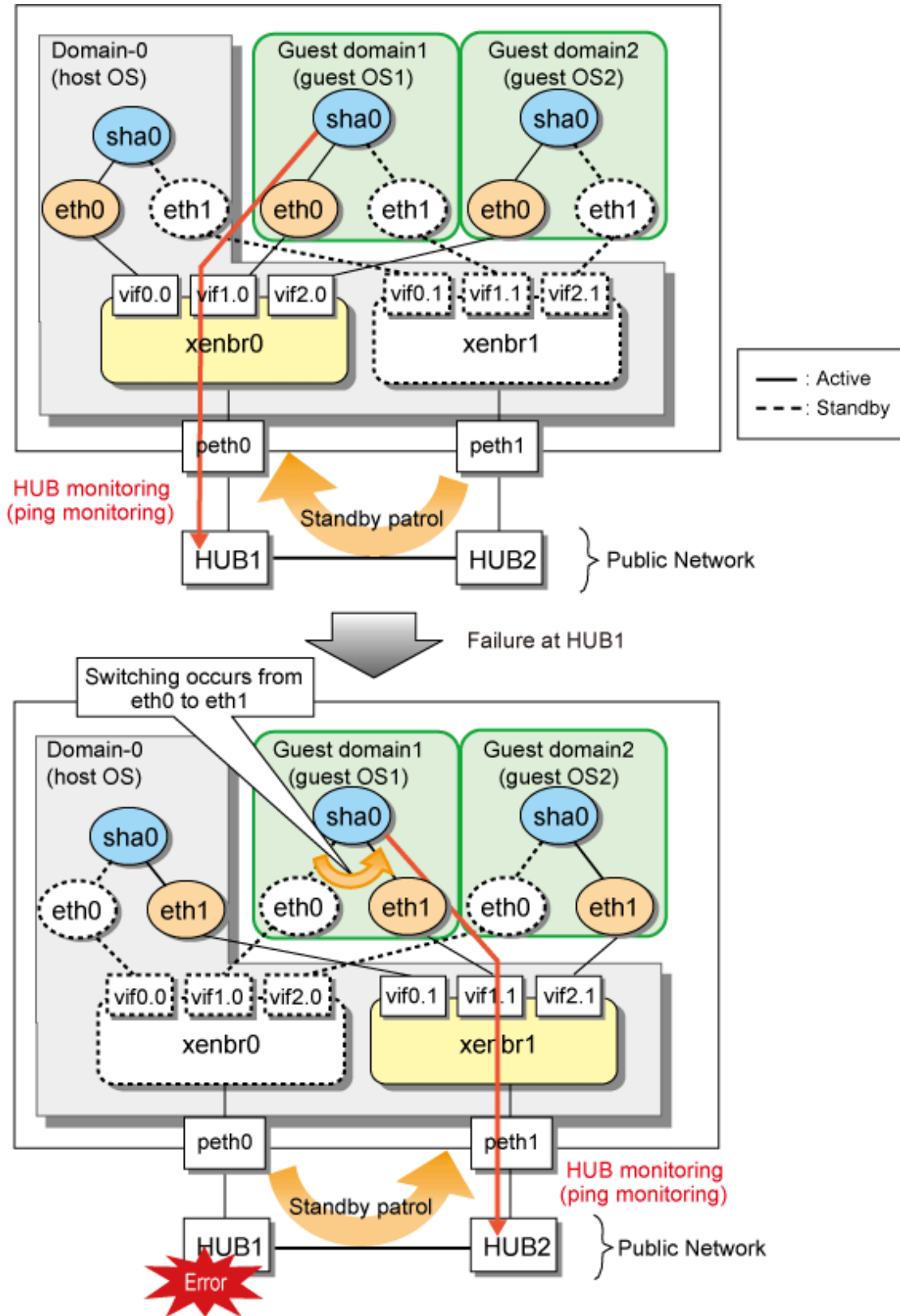


#### NIC switching mode

If GLS on the guest domain is using the primary interface (eth0), perform HUB monitoring (ping monitoring) for HUB1 via peth0. If a failure occurs on HUB1, GLS on the guest OS maintains communications by switching from the primary interface (eth0) to the secondary interface (eth1).

In addition, perform HUB monitoring (ping monitoring) for HUB 2 via peth1 after the NIC has been switched because eth1 is used for the NIC in use.

Figure C.13 NIC switching mode





## Note

With the primary interface or the secondary interface of the guest OS, a link down will not appear when a LAN cable is disconnected. Set HUB monitoring (ping monitoring), because errors cannot be detected by link status monitoring with GLS,

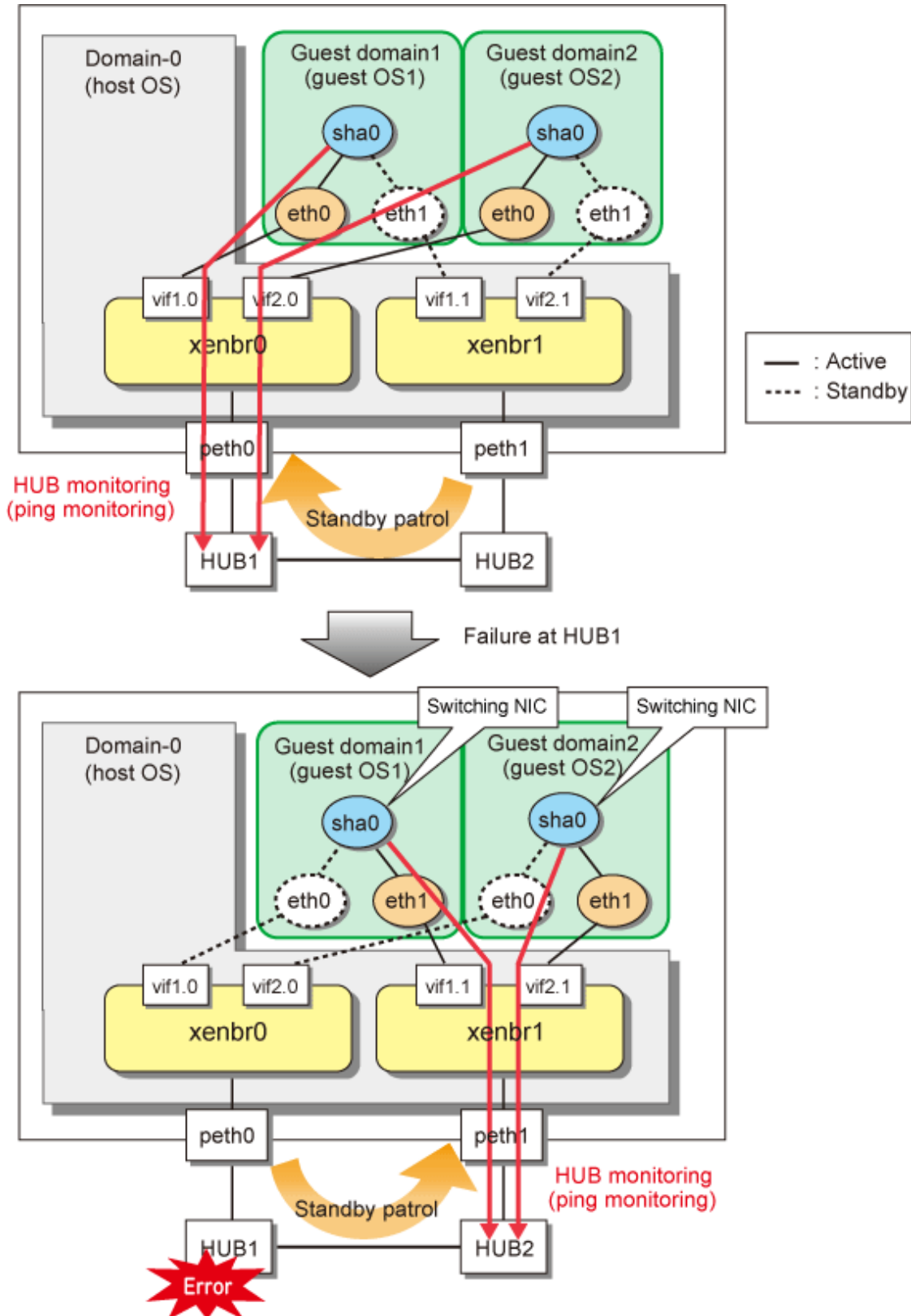
### Virtual NIC mode

If GLS on the guest domain is using the primary interface (eth0), perform HUB monitoring (ping monitoring) for HUB1 via peth0. If a failure occurs on HUB1, GLS on the guest OS maintains communications by switching from the primary interface (eth0) to the secondary interface (eth1).

In addition, perform HUB monitoring (ping monitoring) for HUB 2 via peth1 after the NIC has been switched because eth1 is used for the NIC in use.



Figure C.14 Virtual NIC mode



#### Note

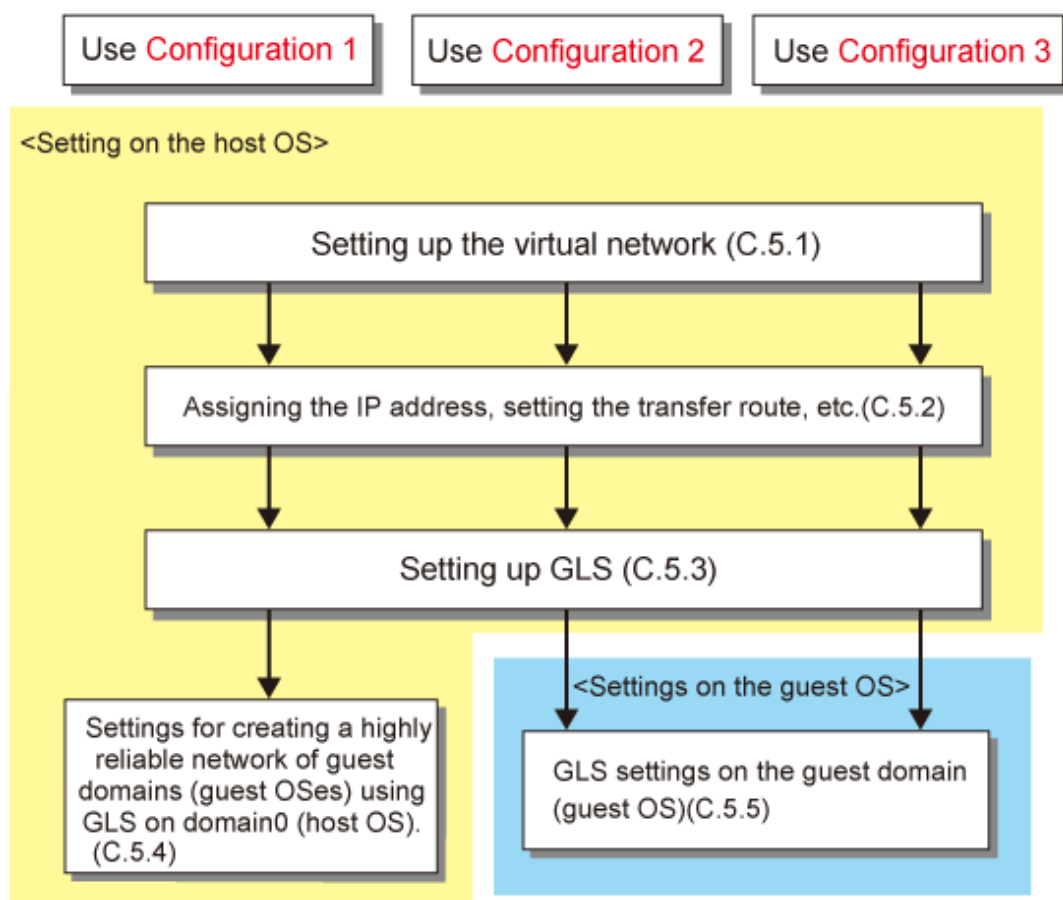
With the primary interface or the secondary interface of the guest OS, a link down will not appear when a LAN cable is disconnected. Set HUB monitoring (ping monitoring), because errors cannot be detected by link status monitoring with GLS,

### C.4.3 Configuration for creating a highly reliable network on guest domains of a cluster system (Configuration 3)

This configuration is the same as the one described in "[C.4.2 Configuration for creating a highly reliable network on guest domains of a single system \(Configuration 2\)](#)". You can maintain communications in the event of a one-sided network failure. Additionally, you can take over the virtual IP address in the event of a both-sided network failure. The failover operation is the same as when a physical server is used. For more details, see "[5.4 Operation on cluster systems](#)".

## C.5 Setting up redundant line switching mode on the virtual machine function (Fast switching mode and NIC switching mode)

The setup procedure is as follows. For setup examples, see "[C.7 Examples of configuration setup \(Fast switching mode and NIC switching mode\)](#)".



### C.5.1 Setting up the virtual network on the host OS

Set up the virtual network of the virtual machine function on the host OS. The virtual network is set only for one NIC when the operating system is installed (default). To establish a highly reliable network, set the virtual network to use multiple NICs. For details, see the RHEL manuals.

1. Create a shell script for creating the virtual bridge, and set so that GLS-specific scripts are executed in the following order.

- Creating the virtual bridge

Set so that the GLS-specific stop script (`/opt/FJSVhanet/local/sbin/hanetxen stop`) is executed before the virtual bridge is created (`op_start`) and the GLS-specific start script (`/opt/FJSVhanet/local/sbin/hanetxen start`) is executed after the virtual bridge is created.

- Deleting the virtual bridge

Set so that the GLS-specific stop script is executed before the virtual bridge is deleted (op\_stop).

The following is a setting example in which the name of the shell script to be created is network-bridge-gls.

- /etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
#   stop  : Delete virtual bridge
#   status: Display virtual bridge information

# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge
glsxenscript=/opt/FJSVhanet/local/sbin/hanetxen

# op_start:subscript for start operation #
op_start () {

    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1

}

# op_stop:subscript for stop operation #
op_stop () {
    # same operation as start
    op_start
}

case "$command" in
    start)
        # Create your virtual bridge
        $glsxenscript stop
        op_start
        $glsxenscript start
        ;;

    stop)
        # Delete virtual bridge
        $glsxenscript stop
        op_stop
        ;;

    status)
        # display virtual bridge information
        $xenscript status
        ;;

    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
esac
```

## Information

- Setting up a virtual network differs between RHEL5 and RHEL5.1. For RHEL5, set "\$xenscript \$command vifnum=X netdev=ethX" rather than "\$xenscript \$command vifnum=X".
- In "C.4.1 Configuration for creating a highly reliable network of guest domains with GLS on domain-0 (Configuration 1)", delete the line of "set -e" from the script.

2. Save the created script in "/etc/xen/scripts".

```
# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls
```

3. Register with the xend service.

Edit the "network-script" parameter in the configuration file (/etc/xen/xend-config.sxp) of the xend service. "network-bridge" is set for the "network-script" parameter. Rename it to the name of the script you created.

```
# Your default ethernet device is used as the outgoing interface,
# by default.
# To use a different one (e.g. eth1) use
#
# (network-script 'network-bridge netdev=eth1')
#
# The bridge is named xenbr0, by default. To rename the bridge, use
#
# (network-script 'network-bridge bridge=<name>')
#
# It is possible to use the network-bridge script in more
# complicated
# scenarios, such as having two outgoing interfaces, with two
# bridges, and
# two fake interfaces per guest domain. To do things like this,
# write
# yourself a wrapper script, and call network-bridge from it, as
# appropriate.
#
# (network-script network-bridge-gls)
```

## Note

If you create five virtual bridges or more, add the following setting in /etc/modprobe.conf. For details, see the RHEL manuals. The following is an example for creating six virtual bridges.

```
# options netloop nloopbacks=6
```

## C.5.2 Assigning the IP address, setting the transfer route and others (for host OS)

Set up the network for the host OS. Setting up the network is the same as when the virtual machine function is not used. For details, see "3.2.2 Network configuration" and "Appendix B Examples of configuring system environments".

## C.5.3 Setting up GLS (for host OS)

Set up networking on the host OS. You can do this in the same way as you would when no virtual machine function is used. For details, see "3.2.2 Network configuration" and "Appendix B Examples of configuring system environments".

## C.5.4 Settings for creating a highly reliable network of guest domains (guest OSes) using GLS on domain-0 (host OS)

---

Use the settings below to create highly reliable communications on guest domains using GLS on domain-0.

1. Set up GLS for the host OS. Setting up GLS is the same as when the virtual machine function is not used. For details, see "[3.3 Additional system setup](#)" and "[Appendix B Examples of configuring system environments](#)".
2. Save a script to associate the virtual machine function with GLS (ethX\_ethY) and a configuration file (ethX\_ethY.conf) for the interfaces that NIC switching mode uses. The following is a setting example in which eth0 and eth1 are bundled. It is necessary to recognize the virtual network configuration to GLS in this step.

```
# cd /etc/opt/FJSVhanet/script/xen
# cp -p eth_eth.xen.sam eth0_eth1
# cd /etc/opt/FJSVhanet/script/conf
# cp -p eth_eth.conf.sam eth0_eth1.conf
```

3. Set up a script to associate the virtual machine function with GLS (ethX\_ethY.conf). Set the primary interface's virtual bridge name in PRI\_BR=, and set the name of the external connection interface in PRI\_OUT\_IF=. In addition, set the secondary interface's virtual bridge name in SEC\_BR=, and set the name of the external connection interface in SEC\_OUT\_IF=.

```
PRI_BR=xenbr0
SEC_BR=xenbr1
PRI_OUT_IF=peth0
SEC_OUT_IF=peth1
```

## C.5.5 Setting up GLS on guest domains (guest OSes)

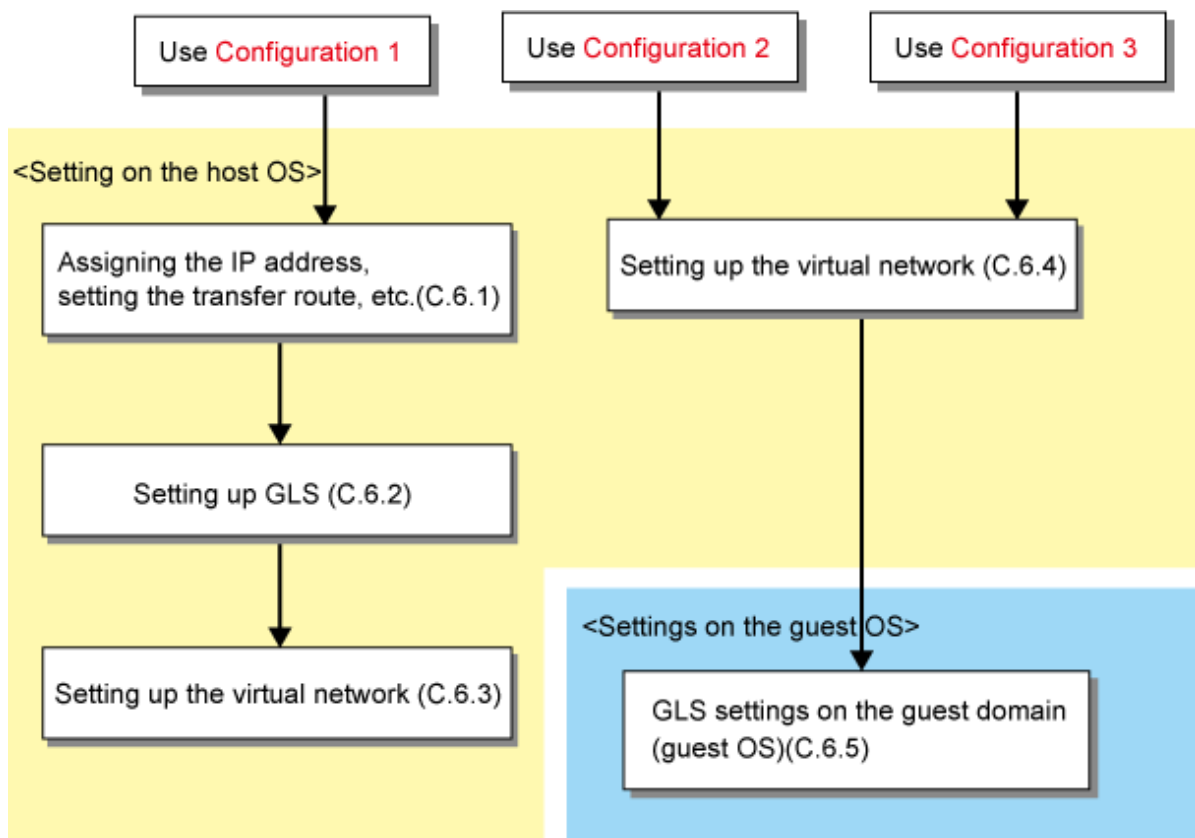
---

The settings for installing GLS on a guest OS is the same as when the virtual machine function is not used. For details, see "[3.3 Additional system setup](#)" and "[Appendix B Examples of configuring system environments](#)".

## C.6 Setting up redundant line switching mode on the virtual machine function (Virtual NIC mode)

---

The setup procedure is as follows. For setup examples, see "[C.8 Examples of configuration setup \(Virtual NIC mode\)](#)".



## C.6.1 Assigning the IP address, setting the transfer route and others (for host OS)

Set up the network for the host OS. Setting up the network is the same as when the virtual machine function is not used. For details, see ["3.2.2 Network configuration"](#) and ["Appendix B Examples of configuring system environments"](#).

## C.6.2 Setting up GLS (for host OS)

Set up GLS on the host OS. Setting up the network is the same as when the virtual machine function is not used. For details, see ["3.2.2 Network configuration"](#) and ["Appendix B Examples of configuring system environments"](#).

## C.6.3 Setting up the virtual network on the host OS (Configuration 1)

For using the configuration 1, set up the virtual network according to the following procedures.

The virtual network is set for the interface where the default gateway is specified when the operating system is installed (default).

When you want to create more than one virtual bridge, or when you create a virtual bridge for an interface where the default gateway is not specified, set up the virtual network according to the following procedures.

When you create a virtual bridge only for a virtual interface in Virtual NIC mode where the default gateway is specified, this setting is not required.

1. Create a shell script for creating the virtual bridge.



### Information

When using only Virtual NIC mode, you do not need to execute "hanetxn start/stop" because virtual interfaces in Virtual NIC mode are created under the virtual network of the virtual machine function.

The following is a setting example in which the name of the shell script to be created is network-bridge-gls.

In the example below, one virtual network is configured for the virtual interface (sha0).

/etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
#   stop  : Delete virtual bridge
#   status: Display virtual bridge information

# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge

# op_start:subscript for start operation #
op_start () {
    $xenscript $command vifnum=0 netdev=sha0
}

# op_stop:subscript for stop operation #
op_stop () {
    # same operation as start
    op_start
}

case "$command" in
    start)
        # Create your virtual bridge
        op_start
        ;;
    stop)
        # Delete virtual bridge
        op_stop
        ;;
    status)
        # display virtual bridge information
        $xenscript status
        ;;
    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
esac
```

2. Save the created script in "/etc/xen/scripts".

```
# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls
```

3. Register with the xend service.

Edit the "network-script" parameter in the configuration file (/etc/xen/xend-config.xcp) of the xend service. "network-bridge" is set for the "network-script" parameter. Rename it to the name of the script you created.

```
# Your default ethernet device is used as the outgoing interface,
by default.
# To use a different one (e.g. eth1) use
#
# (network-script 'network-bridge netdev=eth1')
#
# The bridge is named xenbr0, by default. To rename the bridge, use
#
# (network-script 'network-bridge bridge=<name>')
#
# It is possible to use the network-bridge script in more
complicated
# scenarios, such as having two outgoing interfaces, with two
bridges, and
# two fake interfaces per guest domain. To do things like this,
write
# yourself a wrapper script, and call network-bridge from it, as
appropriate.
#
(network-script network-bridge-gls)
```



## Note

If you create five virtual bridges or more, add the following setting in `/etc/modprobe.conf`. For details, see the RHEL manuals. The following is an example for creating six virtual bridges.

```
options netloop nloopbacks=6
```

## C.6.4 Setting up the virtual network on the host OS (Configuration 2 and Configuration 3)

For using the configuration 2 and the configuration 3, set up the virtual network according to the following procedures.

To create a redundant virtual network by GLS on a guest OS, you need to create two virtual bridges of the virtual machine function connected to the physical interface.

The following is an example to create the shell script for creating the virtual bridge. For details, see the RHEL manuals.

`/etc/xen/scripts/network-bridge-sample`

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
#   stop  : Delete virtual bridge
#   status: Display virtual bridge information
#
# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge

# op_start:subscript for start operation #
op_start () {
    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1
}
```



```

# op_stop:subscript for stop operation #
op_stop () {
    # same operation as start
    op_start
}

case "$command" in
    start)
        # Create your virtual bridge
        op_start
        ;;

    stop)
        # Delete virtual bridge
        op_stop
        ;;

    status)
        # display virtual bridge information
        $xenscript status
        ;;

    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
esac

```

## C.6.5 Setting up GLS on guest domains (guest OSes)

---

The settings for installing GLS on a guest OS is the same as when the virtual machine function is not used. For details, see "[3.3 Additional system setup](#)" and "[Appendix B Examples of configuring system environments](#)".

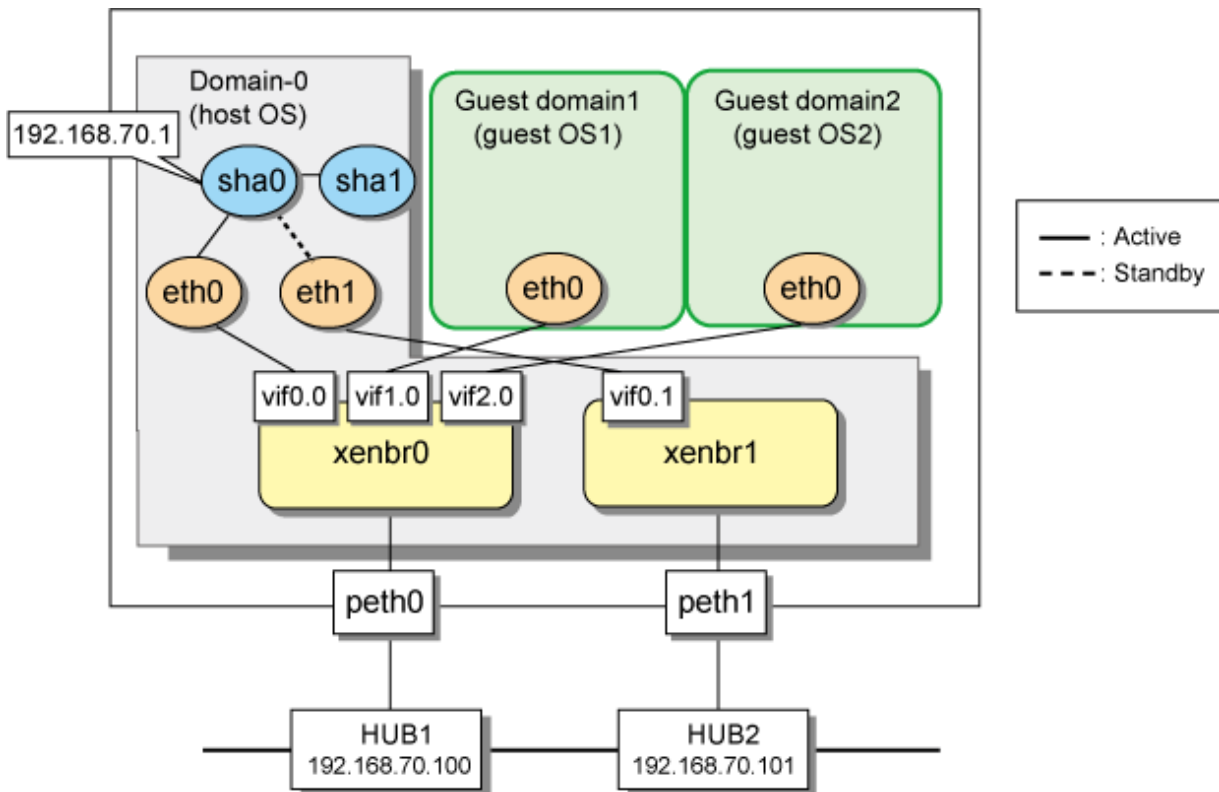
## C.7 Examples of configuration setup (Fast switching mode and NIC switching mode)

---

### C.7.1 Setup example for creating a highly reliable network of guest domains using GLS on domain-0 (Untagged VLAN and single network configuration)

---

This section describes a configuration setup example for the following network configuration.



## 1) Setting up the virtual network

1-1) Define virtual bridges (xenbr0, xenbr1). For details, see the RHEL manuals.

- Contents of /etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
#   stop  : Delete virtual bridge
#   status: Display virtual bridge information
#
# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge
glxenscript=/opt/FJSVhanet/local/sbin/hanetxen

# op_start:subscript for start operation #
op_start () {

    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1

}
# op_stop:subscript for stop operation #
op_stop () {
    # same operation as start
    op_start
}
case "$command" in
    start)
        # Create your virtual bridge
```

```

        $glxenscript stop
        op_start
        $glxenscript start
    ;;

    stop)
        # Delete virtual bridge
        $glxenscript stop
        op_stop
    ;;
    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
esac

```



## Note

In the line of "\$xenscript \$command vifnum=X netdev=ethX", specify the same value for the number (X) specified by vifnum and the number (X) of the device name (ethX) specified by netdev.

1-2) Save the script in "/etc/xen/scripts".

```

# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls

```

1-3) Register with the xend service.

- Contents of /etc/xen/xend-config.sxp

```

# Your default ethernet device is used as the outgoing interface, by
default.
# To use a different one (e.g. eth1) use
#
(omitted)
#
(network-script network-bridge-gls)

```

1-4) Edit the domain configuration file

The network interface for the guest OS should be connected to the primary virtual bridge (xenbr0) that you set in "3-1)". The following shows an example of the domain configuration file. Set the virtual bridge name in the "vif" parameter. For details on the domain configuration file, see the RHEL manuals.

- Contents of /etc/xen/domain name (domain configuration file)

```

vif=[ "mac=XX:XX:XX:XX:XX:XX,bridge=xenbr0" ]

```

## 2) Setting up the network on the host OS

2-1) Define the IP addresses and host names you use in the /etc/hosts file.

```

192.168.70.1    hosta    # virtual IP address of the host OS
192.168.70.100 swhub1   # IP address of the primary monitoring destination's HUB
192.168.70.101 swhub2   # IP address of the secondary monitoring destination's HUB

```

2-2) Type IP addresses in the /etc/sysconfig/network-scripts/ifcfg-ethX(X = 0, 1) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.2
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

2-3) Configure the /etc/sysconfig/network file to enable the network setting.

```
NETWORKING=yes
NETWORKING_IPV6=no
```

#### 2-4) Reboot

To enable the network settings for Domain-0, execute the following command and reboot the system. After rebooting the system, use the ifconfig command to check that eth0 is activated.

```
/sbin/shutdown -r now
```

### 3) Having GLS recognize the virtual network configuration

3-1) Set values in the configuration file of the virtual network.

- Contents of /etc/opt/FJSVhanet/script/conf/eth0\_eth1.conf

```
PRI_BR=xenbr0
SEC_BR=xenbr1
PRI_OUT_IF=peth0
SEC_OUT_IF=peth1
```



#### Note

Set the values in the configuration file for a virtual network for each redundant physical interface. When you name the configuration file of the virtual network, put an underscore between the names of the redundant physical interfaces, and ".conf" at the end. Other forms of names are invalid. In addition, only alphanumeric characters and periods can be used in the string after the "=" for each setting. If you use characters other than the above, the setting will be invalid.

3-2) Copy the script for switching virtual networks to enable the redundant line control function.

```
cd /etc/opt/FJSVhanet/script/xen
cp -p eth_eth.xen.sam eth0_eth1
```



## Note

Create the script for associating the virtual machine function with GLS for each redundant physical interface. When you name the script file for associating the virtual machine function with GLS, put an underscore between the names of the redundant physical interfaces. Other forms of names are invalid.

### 4) Setting the redundant line switching mode

#### 4-1) Setting subnet masks

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

#### 4-2) Setting the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```



## Note

Make sure to set the same physical IP address that has been set in /etc/sysconfig/network-scripts/ifcfg-eth0 as the physical IP address to be specified in the '-i' option.

#### 4-3) Setting HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

#### 4-4) Setting the standby patrol

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

#### 4-5) Activating the virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

#### 4-6) Starting HUB monitoring

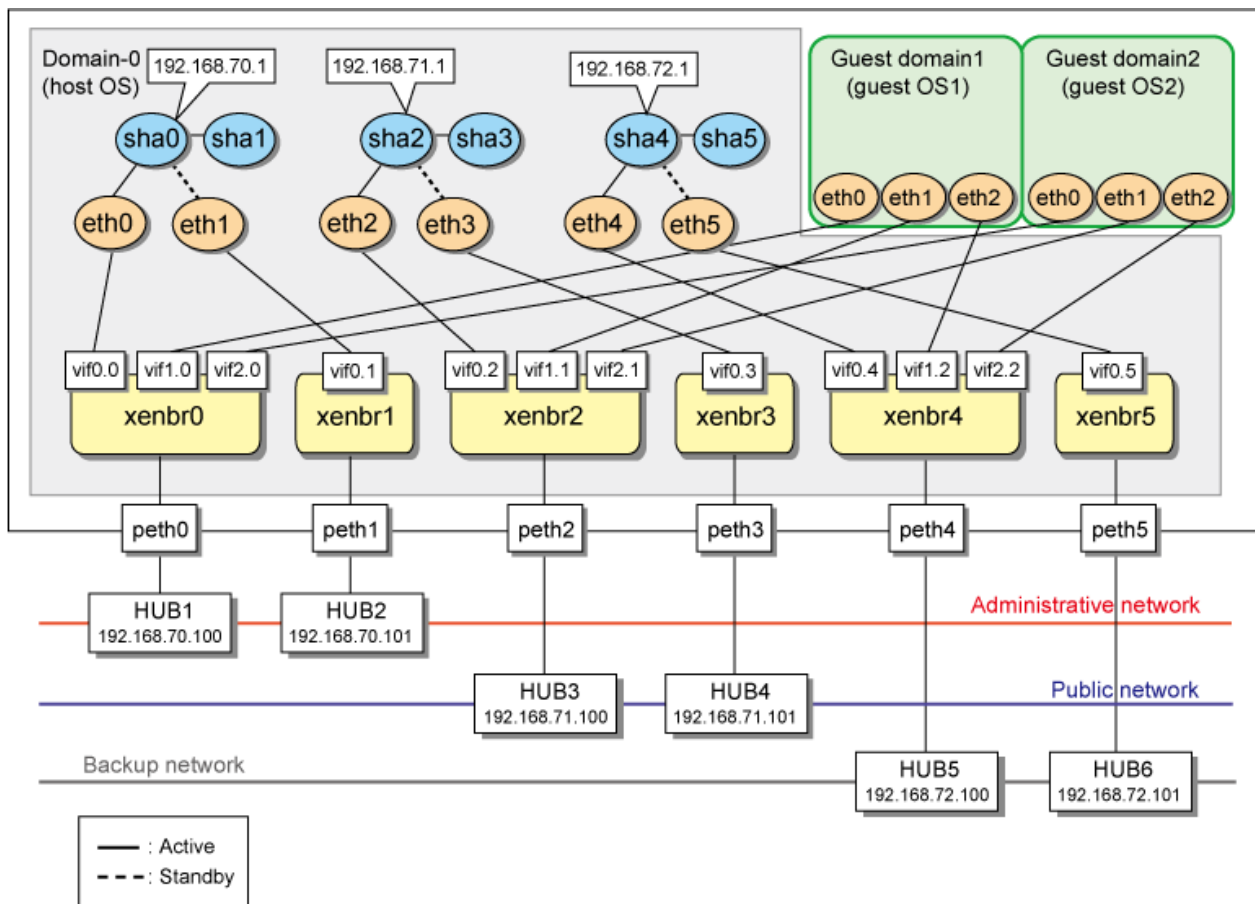
```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 5) Setting up a guest OS

Set up an IP address. Edit the "/etc/sysconfig/network-scripts/ifcfg-ethX" file as you would for the host OS.

## C.7.2 Setup example for creating a highly reliable guest domains using GLS on domain-0 (Untagged VLAN and multiple network configuration)

This section describes a configuration setup example in which communications for administration, public use, and backup are established on different networks for the virtual machine function.



## 1) Setting up virtual networks on the host OS

1-1) Define virtual bridges (xenbr0, xenbr1, xenbr2, xenbr3, xenbr4, xenbr5). For details, see the RHEL manuals.

- Contents of /etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
# stop : Delete virtual bridge
# status: Display virtual bridge information
#
# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge
glsxenscript=/opt/FJSVhanet/local/sbin/hanetxen

# op_start:subscript for start operation #
op_start () {

    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1
    $xenscript $command vifnum=2 netdev=eth2
    $xenscript $command vifnum=3 netdev=eth3
    $xenscript $command vifnum=4 netdev=eth4
    $xenscript $command vifnum=5 netdev=eth5
}

# op_stop:subscript for stop operation #
```

```

op_stop () {
    # same operation as start
    op_start
}
case "$command" in
    start)
        # Create your virtual bridge
        $glxenscript stop
        op_start
        $glxenscript start

        ;;

    stop)
        # Delete virtual bridge
        $glxenscript stop
        op_stop

        ;;
    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1

esac

```



## Note

In the line of "\$xenscript \$command vifnum=X netdev=ethX", specify the same value for the number (X) specified by vifnum and the number (X) of the device name (ethX) specified by netdev.

1-2) Save the script in "/etc/xen/scripts".

```

# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls

```

1-3) Register with the xend service.

- Contents of /etc/xen/xend-config.sxp

```

# Your default ethernet device is used as the outgoing interface, by
default.
# To use a different one (e.g. eth1) use
#
(omitted)
#
(network-script network-bridge-gls)

```

1-4) Edit the domain configuration file

The network interface for the guest OS should be connected to the primary virtual bridge (xenbr0) that you set in "3-1)". The following shows an example of the domain configuration file. Set the virtual bridge name in the "vif" parameter. For details on the domain configuration file, see the RHEL manuals.

- Contents of /etc/xen/domain name (domain configuration file)

```

vif=[ "mac=XX:XX:XX:XX:XX:XX,bridge=xenbr0", "mac=YY:YY:YY:YY:YY:YY,bridge=xenbr2",
"mac=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ,bridge=xenbr4" ]

```



## Note

If you create five virtual bridges or more, add the following setting in /etc/modprobe.conf. For details, see the RHEL manuals. The following is an example for creating six virtual bridges.

```
# options netloop nloopbacks=6
```

## 2) Setting up the network on the host OS

2-1) Define the IP addresses and host names you use in the /etc/hosts file.

```
192.168.70.1    hosta    # virtual IP address of the host OS
192.168.71.1    hostb    # physical IP address of the host OS
192.168.72.1    hostc    # virtual IP address of the host OS
192.168.70.100 swhub1   # IP address of the primary monitoring destination's HUB
192.168.70.101 swhub2   # IP address of the secondary monitoring destination's HUB
192.168.71.100 swhub3   # IP address of the primary monitoring destination's HUB
192.168.71.101 swhub4   # IP address of the secondary monitoring destination's HUB
192.168.72.100 swhub5   # IP address of the primary monitoring destination's HUB
192.168.72.101 swhub6   # IP address of the secondary monitoring destination's HUB
```

2-2) Type IP addresses in the /etc/sysconfig/network-scripts/ifcfg-ethX(X = 0,1,2,3,4,5) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.71.255
IPADDR=192.168.71.1
NETMASK=255.255.255.0
NETWORK=192.168.71.0
ONBOOT=yes
TYPE=Ethernet
```



- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth4

```
DEVICE=eth4
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.72.255
IPADDR=192.168.72.1
NETMASK=255.255.255.0
NETWORK=192.168.72.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth5

```
DEVICE=eth5
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

2-3) Configure the /etc/sysconfig/network file to enable the network setting.

```
NETWORKING=yes
NETWORKING_IPV6=no
```

## 2-4) Reboot

To enable the network setting for Domain-0, 1 and 2, execute the following command and reboot the system. After rebooting the system, use the ifconfig command to check that eth0 is activated.

```
/sbin/shutdown -r now
```

## 3) Having GLS recognize the virtual network configuration

3-1) Set these values in the configuration file for the virtual networks.

- Contents of /etc/opt/FJSVhanet/script/conf/eth0\_eth1.conf

```
PRI_BR=xenbr0
SEC_BR=xenbr1
PRI_OUT_IF=peth0
SEC_OUT_IF=peth1
```

- Contents of /etc/opt/FJSVhanet/script/conf/eth2\_eth3.conf

```
PRI_BR=xenbr2
SEC_BR=xenbr3
PRI_OUT_IF=peth2
SEC_OUT_IF=peth3
```

- Contents of /etc/opt/FJSVhanet/script/conf/eth4\_eth5.conf

```
PRI_BR=xenbr4
SEC_BR=xenbr5
PRI_OUT_IF=peth4
SEC_OUT_IF=peth5
```

## Note

Set the values in the configuration file for the virtual network for each redundant physical interface. When you name the configuration file of a virtual network, put an underscore between the names of the redundant physical interfaces, and ".conf" at the end. Other forms of names are invalid. In addition, only alphanumeric characters and periods can be used in the string after the "=" for each setting. If you use characters other than the above, the setting will be invalid.

- 3-2) Create the script to associate the virtual machine function with GLS to enable the redundant line control function.

```
cd /etc/opt/FJSVhanet/script/xen
cp -p eth_eth.xen.sam eth0_eth1
cp -p eth_eth.xen.sam eth2_eth3
cp -p eth_eth.xen.sam eth4_eth5
```

## Note

Create the script to associate the virtual machine function with GLS for each redundant physical interface. When you name the script file for associating the virtual machine function with GLS, put an underscore between the names of the redundant physical interfaces, and ".conf" at the end. Other forms of names are invalid.

### 4) Setting the redundant line switching mode

- 4-1) Setting subnet masks

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.71.0 -m 255.255.255.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.72.0 -m 255.255.255.0
```

- 4-2) Setting virtual interfaces

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m e -i 192.168.71.1 -t eth2,eth3
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha4 -m e -i 192.168.72.1 -t eth4,eth5
```

## Note

Make sure to set the same physical IP address set in /etc/sysconfig/network-scripts/ifcfg-ethX for the physical IP address to be specified with the '-i' option.

- 4-3) Setting 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 sha2 -p 192.168.71.100,192.168.71.101 -b off
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha4 -p 192.168.72.100,192.168.72.101 -b off
```

- 4-4) Setting the standby patrol

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha3 -m p -t sha2
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha5 -m p -t sha4
```

- 4-5) Activating virtual interfaces

/opt/FJSVhanet/usr/sbin/strhanet

4-6) Starting HUB monitoring

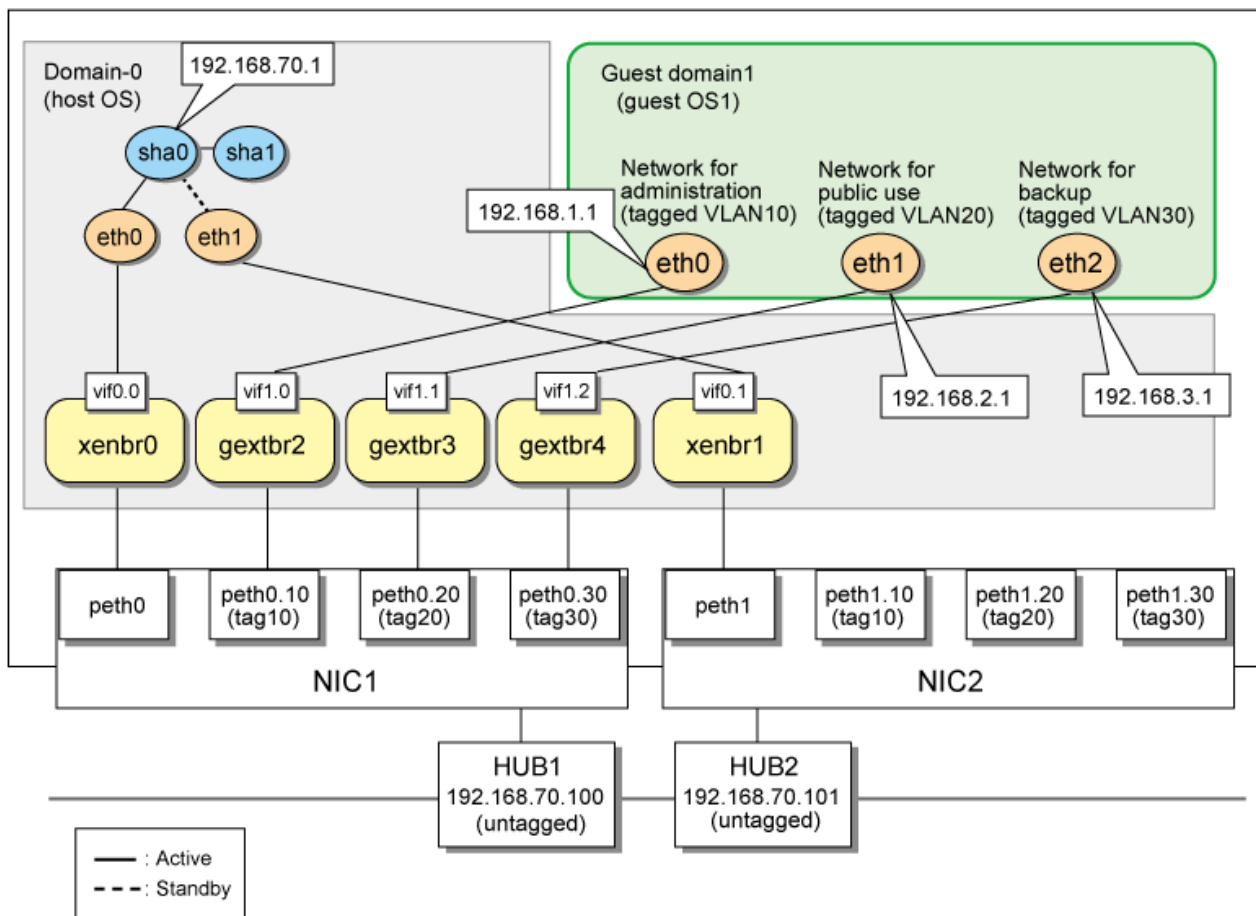
/opt/FJSVhanet/usr/sbin/hanetpoll on

### 5) Setting up the guest OS

Set up an IP address. Edit the "/etc/sysconfig/network-scripts/ifcfg-ethX" file as you would for the host OS.

## C.7.3 Setup example for creating a highly reliable domains using GLS on domain-0 (Tagged VLAN and multiple network configuration)

The following shows an example of using each LAN (administrative LAN, public LAN, and backup LAN) of a guest OS on one physical network by using the tagged VLAN



### 1) Setting up the virtual network

1-1) Define virtual bridges (xenbr0, xenbr1, gextbr2-4). For details, see the RHEL manuals.

- Contents of /etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
# stop : Delete virtual bridge
# status: Display virtual bridge information
#
# Exit if anything goes wrong
```

```

#set -e

command=$1

glxsenscript=/opt/FJSVhanet/local/sbin/hanetxen
xenscript=/etc/xen/scripts/network-bridge
xenscriptgext=/etc/xen/scripts/gext-network-bridge

# op_start:subscript for start operation #
op_start () {
    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1

    vconfig add peth0 10
    vconfig add peth0 20
    vconfig add peth0 30
    vconfig add peth1 10
    vconfig add peth1 20
    vconfig add peth1 30

    $xenscriptgext $command extnum=2 netdev=peth0.10
    $xenscriptgext $command extnum=3 netdev=peth0.20
    $xenscriptgext $command extnum=4 netdev=peth0.30
}

# op_stop:subscript for stop operation #
op_stop () {
    $xenscript $command vifnum=0 netdev=eth0
    $xenscript $command vifnum=1 netdev=eth1

    $xenscriptgext $command extnum=2 netdev=peth0.10
    $xenscriptgext $command extnum=3 netdev=peth0.20
    $xenscriptgext $command extnum=4 netdev=peth0.30

    vconfig rem peth0.10
    vconfig rem peth0.20
    vconfig rem peth0.30
    vconfig rem peth1.10
    vconfig rem peth1.20
    vconfig rem peth1.30
}

case "$command" in
    start)
        # Create your virtual bridge
        $glxsenscript stop
        op_start
        $glxsenscript start
        ;;
    stop)
        # Delete virtual bridge
        $glxsenscript stop
        op_stop
        ;;
    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
esac

```



## Note

In the line of "\$xenscript \$command vifnum=X netdev=ethX", specify the same value for the number (X) specified by vifnum and the number (X) of the device name (ethX) specified by netdev.

1-2) Save the created script in "/etc/xen/scripts".

```
# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls
```

1-3) Register with the xend service

- Contents of /etc/xen/xend-config.sxp

```
# Your default ethernet device is used as the outgoing interface, by
default.
# To use a different one (e.g. eth1) use
#
(omitted)
#
(network-script network-bridge-gls)
```

1-4) Edit the domain configuration file

The network interface for the guest OS should be connected to the primary virtual bridge (xenbr0) that you set in "3-1)". The following shows an example of the domain configuration file. Set the virtual bridge name in the "vif" parameter. For details on the domain configuration file, see the RHEL manuals.

- Contents of /etc/xen/domain name (domain configuration file)

```
vif=[ "mac=XX:XX:XX:XX:XX:XX,bridge=gextbr2", "mac=YY:YY:YY:YY:YY:YY,bridge=gextbr3",
      "mac=ZZ:ZZ:ZZ:ZZ:ZZ:ZZ,bridge=gextbr4" ]
```

## 2) Setting up the network for the host OS

2-1) Define the IP address and hostname to be used in the /etc/hosts file.

```
192.168.70.1    hosta    # Virtual IP address of the host OS
192.168.70.100 swhub1   # IP address of the primary monitoring destination HUB
192.168.70.101 swhub2   # IP address of the secondary monitoring destination HUB
```

2-2) Type the IP address in the /etc/sysconfig/network-scripts/ifcfg-ethX (X represents 0,1) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
BROADCAST=192.168.70.255
IPADDR=192.168.70.1
NETMASK=255.255.255.0
NETWORK=192.168.70.0
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
```

2-3) Configure the /etc/sysconfig/network file to enable the network settings.

```
NETWORKING=yes
NETWORKING_IPV6=no
```

2-4) Activate VLAN of the operating system.

```
NETWORKING=yes
VLAN=yes
```

2-5) Reboot

To enable the network settings of domain-0, execute the following command and reboot the system. After reboot, use the "ifconfig" command to check that eth0 has been activated.

```
/sbin/shutdown -r now
```

### 3) Having GLS recognize the virtual network configuration

3-1) Create the configuration file for the virtual network.

- Content of /etc/opt/FJSVhanet/script/conf/eth0\_eth1.conf

```
PRI_BR=xenbr0
SEC_BR=xenbr1
PRI_OUT_IF=peth0
SEC_OUT_IF=peth1
GEXTBR0=gextbr2
GEXTBR_PRI_OUT_IF0=peth0.10
GEXTBR_SEC_OUT_IF0=peth1.10
GEXTBR1=gextbr3
GEXTBR_PRI_OUT_IF1=peth0.20
GEXTBR_SEC_OUT_IF1=peth1.20
GEXTBR2=gextbr4
GEXTBR_PRI_OUT_IF2=peth0.30
GEXTBR_SEC_OUT_IF2=peth1.30
```



#### Note

Set the values in the configuration file for the virtual network for each redundant physical interface. When you name the configuration file of the virtual network, put an underscore between the names of the redundant physical interfaces, and ".conf" at the end. Other forms of names are invalid. In addition, only alphanumeric characters and periods can be used in the string after the "=" for each setting. If you use characters other than the above, the setting will be invalid.

3-2) Copy the script for switching virtual networks to enable the redundant line control function.

```
cd /etc/opt/FJSVhanet/script/xen
cp -p eth_eth.xen.sam eth0_eth1
```



## Note

Create the script for associating the virtual machine function with GLS for each redundant physical interface. When you name the script file for associating the virtual machine function with GLS, put an underscore between the names of the redundant physical interfaces, and ".conf" at the end. Other forms of names are invalid.

### 4) Setting the redundant line switching mode

#### 4-1) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

#### 4-2) Setting the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```



## Note

The physical IP address to be specified in the "-i" option should be identical to the physical IP address that has been set in /etc/sysconfig/network-scripts/ifcfg-eth0.

#### 4-3) Setting HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

#### 4-4) Setting the standby patrol

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

#### 4-5) Activating the virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

#### 4-6) Starting HUB monitoring

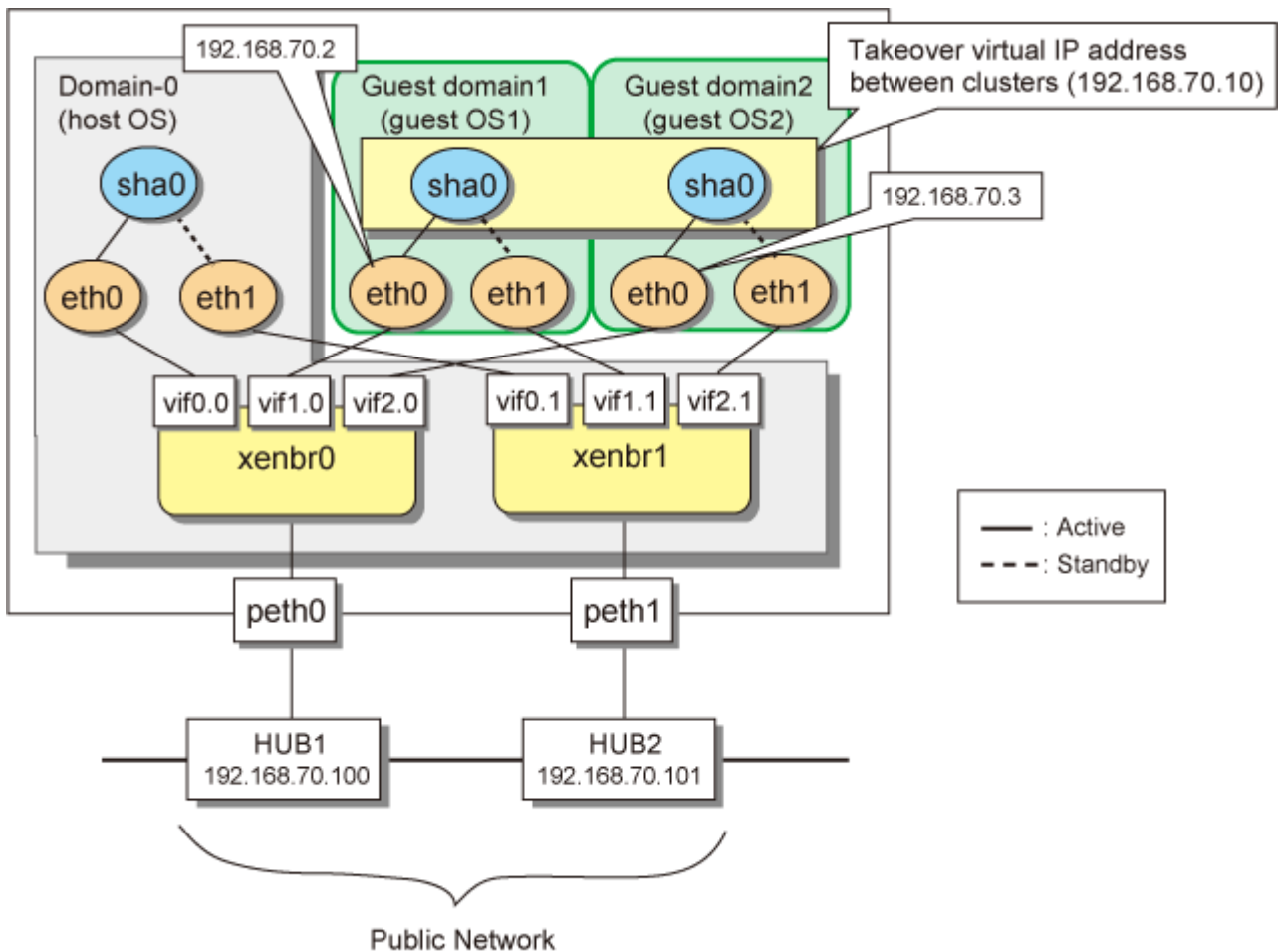
```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

### 5) Setting up the guest OS

Set up an IP address. Edit the "/etc/sysconfig/network-scripts/ifcfg-ethX" file as you would for the host OS.

## C.7.4 Setup example for achieving high reliability using GLS on each guest domain of a cluster system

This section describes a configuration setup example for the following network configuration.



### [Setting up domain-0 (host OS)]

The GLS for the host is the same as the one described in "[B.4.1 Example of the Single system without NIC sharing](#)". Note that you do not need to create the settings to have GLS recognize the virtual network configuration.

### [Setting up the guest domain1 (active node)]

Setting up GLS is the same as for "[B.4.7 Example of the Cluster system \(1:1 Standby\)](#)".

### [Setting up the guest domain2 (standby node)]

Setting up GLS is the same as for "[B.4.7 Example of the Cluster system \(1:1 Standby\)](#)".

### [Setting up the cluster interconnect]

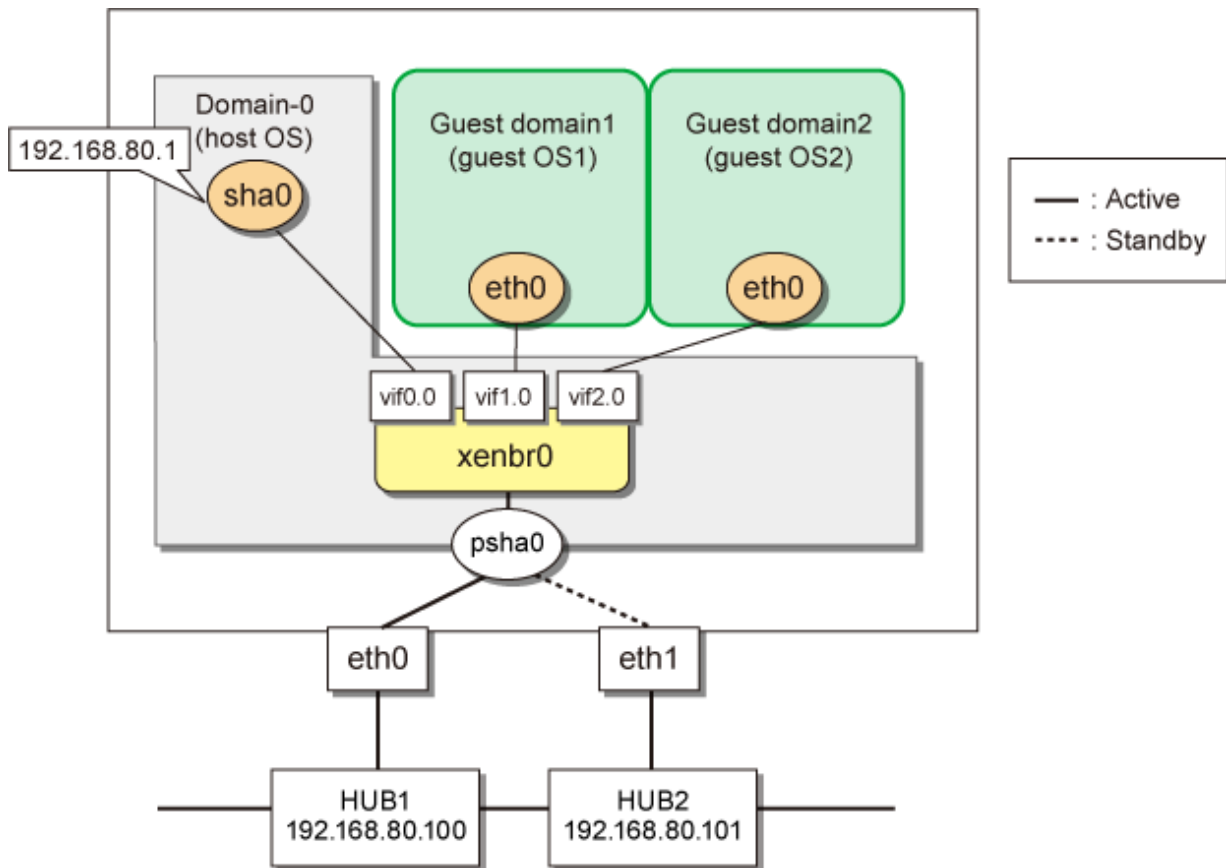
For information on the settings of the virtual switch required for connecting clusters, see "PRIMECLUSTER Installation/Administration Guide".

## C.8 Examples of configuration setup (Virtual NIC mode)

### C.8.1 Setup example for creating a highly reliable network of guest domains using GLS on domain-0 (Untagged VLAN and single network configuration)

This section describes a configuration setup example for the following network configuration.





## 1) Setting up the network on the host OS

1-1) Define the IP addresses and host names you use in the /etc/hosts file.

```
192.168.80.1 hosta      # virtual IP address of the host OS
192.168.80.100 swhub1 # IP address of the primary monitoring destination's HUB
192.168.80.101 swhub2 # IP address of the secondary monitoring destination's HUB
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Configure the /etc/sysconfig/network file to enable the network setting.

```
NETWORKING=yes
```

## 2) Setting the redundant line switching mode

### 2-1) Setting the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 2-2) Setting an IP address and a subnet mask

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
```

### 2-3) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

## 3) Setting up the virtual network

### 3-1) Define the virtual bridge (xenbr0). For details, see the RHEL manuals.

- Contents of /etc/xen/scripts/network-bridge-gls

```
#!/bin/sh
#
# Sample of Create/Delete virtual bridge
#
# $1 start : Create virtual bridge
# stop : Delete virtual bridge
# status: Display virtual bridge information

# Exit if anything goes wrong
#set -e

command=$1
xenscript=/etc/xen/scripts/network-bridge

# op_start:subscript for start operation #
op_start () {
    $xenscript $command vifnum=0 netdev=sha0
}

# op_stop:subscript for stop operation #
op_stop () {
    # same operation as start
    op_start
}

case "$command" in
    start)
        # Create your virtual bridge
        op_start
        ;;
    stop)
        # Delete virtual bridge
        op_stop
        ;;
    status)
        # display virtual bridge information
```

```

        $xenscript status
    ;;
    *)
        echo "Unknown command: $command" >&2
        echo 'Valid commands are: start, stop, status' >&2
        exit 1
    esac

```

3-2) Save the created script in "/etc/xen/scripts".

```

# cp network-bridge-gls /etc/xen/scripts
# cd /etc/xen/scripts
# chmod +x network-bridge-gls

```

3-3) Register with the xend service

- Contents of /etc/xen/xend-config.sxp

```

# Your default ethernet device is used as the outgoing interface, by default.
# To use a different one (e.g. eth1) use
#
(omitted)
#
(network-script network-bridge-gls)

```

3-4) Edit the domain configuration file

The network interface for the guest OS should be connected to the primary virtual bridge (xenbr0) that you set in "3-1)". The following shows an example of the domain configuration file. Set the virtual bridge name in the "vif" parameter. For details on the domain configuration file, see the RHEL manuals.

- Contents of /etc/xen/domain name (domain configuration file)

```

vif=[ "mac=XX:XX:XX:XX:XX:XX,bridge=xenbr0" ]

```

3-5) Reboot

To enable the network settings for Domain-0, execute the following command and reboot the system. After rebooting the system, use the ifconfig command to check that sha0 is activated.

```

/sbin/shutdown -r now

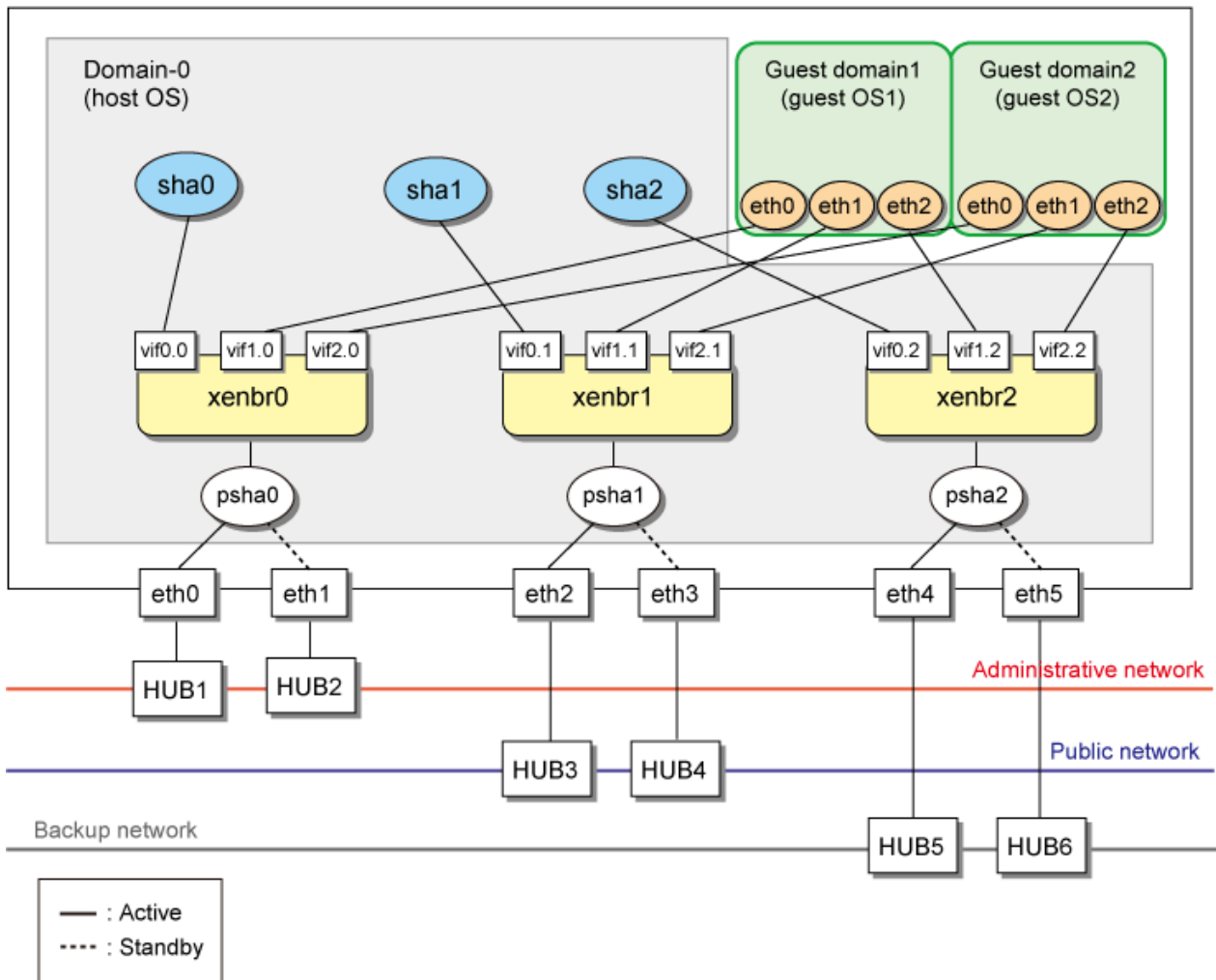
```

#### 4) Setting up a guest OS

Set up an IP address. Edit the "/etc/sysconfig/network-scripts/ifcfg-ethX" file as you would for the host OS.

## C.8.2 Setup example for creating a highly reliable guest domains using GLS on domain-0 (Untagged VLAN and multiple network configuration)

This section describes a configuration setup example in which communications for administration, public use, and backup are established on different networks for the virtual machine function.



### [Setting up domain-0 (host OS)]

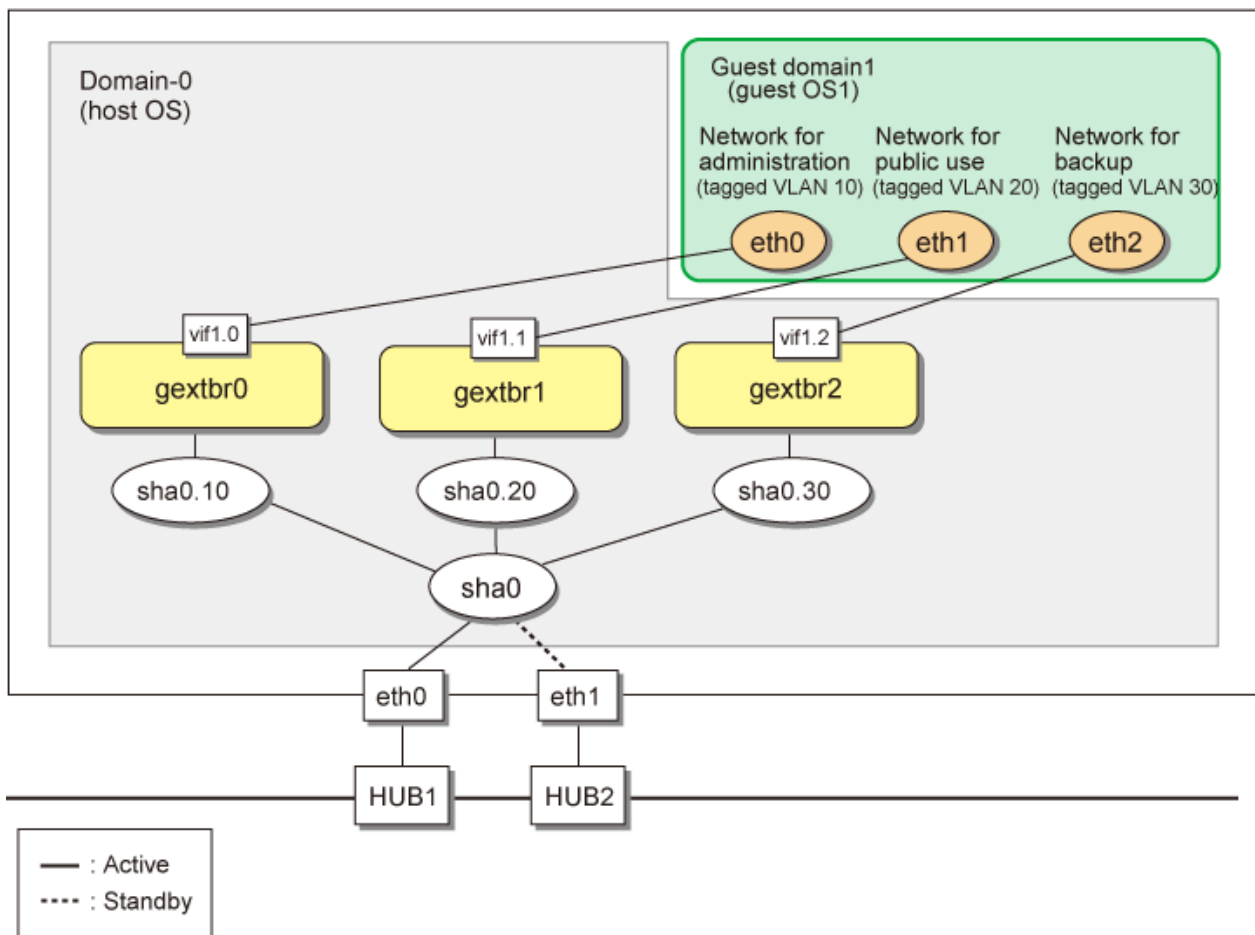
The GLS for the host is the same as the one described in "[C.8.1 Setup example for creating a highly reliable network of guest domains using GLS on domain-0 \(Untagged VLAN and single network configuration\)](#)". Set up the virtual bridge (xenbrX) for each virtual interface (shaX).

### [Setting up each guest OS]

Set up an IP address. Edit the `/etc/sysconfig/network-scripts/ifcfg-ethX` file as you would for the host OS.

## C.8.3 Setup example for creating a highly reliable domains using GLS on domain-0 (Tagged VLAN and multiple network configuration)

The following shows an example of using each LAN (administrative LAN, public LAN, and backup LAN) of a guest OS on one physical network by using the tagged VLAN.



### [Setting up domain-0 (host OS)]

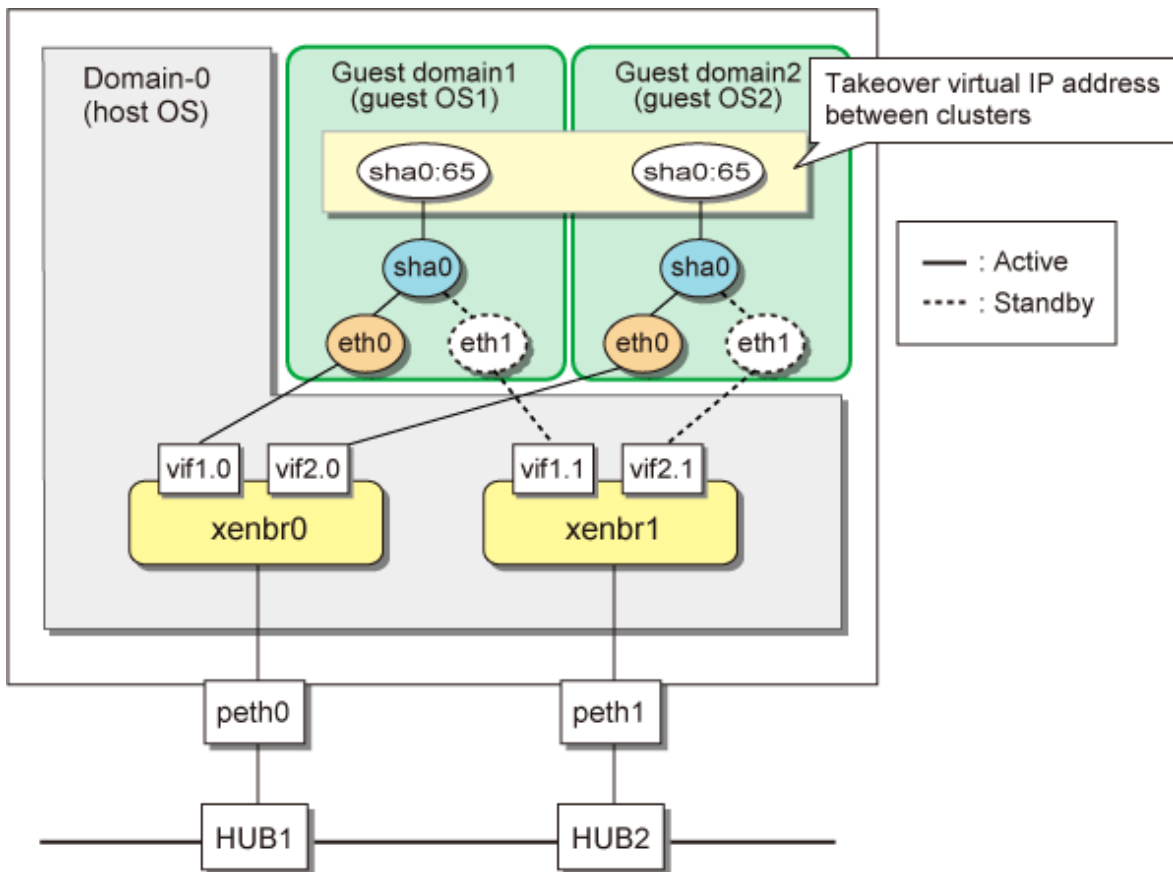
For setting up GLS, see "[B.7.2 Configuring virtual interfaces with tagged VLAN](#)". Set up the virtual bridge (`gextbrX`) for each tagged VLAN interface (`shaX.Y`).

### [Setting up each guest OS]

Set up an IP address. Edit the `/etc/sysconfig/network-scripts/ifcfg-ethX` file as you would for the host OS.

## C.8.4 Setup example for achieving high reliability using GLS on each guest domain of a cluster system

This section describes a configuration setup example for the following network configuration.



### [Setting up domain-0 (host OS)]

On the host OS, set up the virtual bridge (xenbrX) for the physical interface (ethX).

### [Setting up the guest domain1 (active node)]

Setting up GLS is the same as for "[B.7.3 Example of the Cluster system \(1:1 Standby\)](#)".

### [Setting up the guest domain2 (standby node)]

Setting up GLS is the same as for "[B.7.3 Example of the Cluster system \(1:1 Standby\)](#)".

### [Setting up the cluster interconnect]

For information on the settings of the virtual switch required for connecting clusters, see "[PRIMECLUSTER Installation/Administration Guide](#)".

## Appendix D Operation on the Virtual Machine Function (for RHEL6)

This chapter describes the operation of GLS on the virtual machine function. For details on the virtual machine function, see the RHEL manuals.

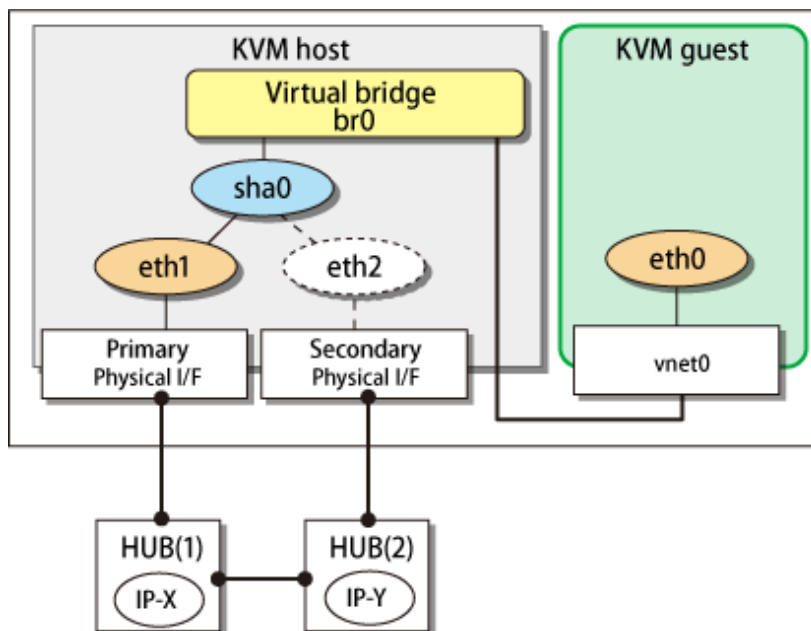
### D.1 Virtual Machine Function Overview

For the overview of virtual machines, see "[C.1 Virtual machine function overview](#)".

### D.2 Configuration of the Virtual Machine Function

In KVM environments, the hypervisor (KVM host) is embedded in the Linux kernel, and virtual machines (KVM guests) run as Linux processes. Network connections from KVM guests are made over the virtual bridge (br0) that is configured on the KVM host.

To this virtual bridge, a virtual interface (sha0) or a physical interface of GLS is connected for communication with external networks. Moreover, a virtual NIC (vnet0) is generated at the connection of the virtual bridge to the KVM guest. KVM guests communicate with external networks via these elements.



### D.3 Virtual Network Design in Virtual Machine Function

#### D.3.1 Concept of network configuration in the virtual machine function

With the virtual machine function, we recommend that you use the virtual machine network separately for each of the following three purposes. For details, see the RHEL manuals.

- Communications for administration
- Communications for public use
- Communications for backup

### D.3.2 Support set for each redundant line switching mode

GLS provides highly reliable network communications for KVM hosts (host OS) and guest domains (guest OS). The following table shows the compatibility between redundant line switching methods and domains. Select Fast switching mode if every one of the remote hosts uses Fast switching mode. Other than this mode, select Virtual NIC mode.

	KVM host (host OS)	KVM guest (guest OS)
Fast switching mode	O (Connection with a virtual bridge: X)	O
NIC switching mode	O (Connection with a virtual bridge: X)	O
Virtual NIC mode	O	O
GS linkage mode	O (Connection with a virtual bridge: X)	O

O: Supported X: Not supported

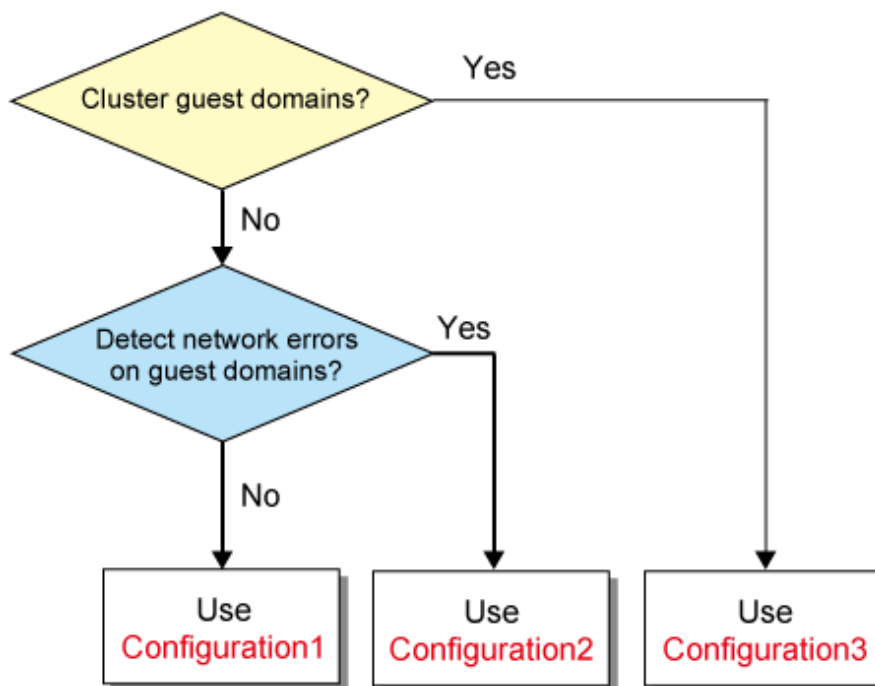


#### Note

When bundling the interface that was created by SR-IOV, use the NIC switching mode.

### D.3.3 Flow for selecting the virtual network configuration in each redundant line switching mode

Use the following flowchart to select the virtual network configuration for each redundant line switching mode.



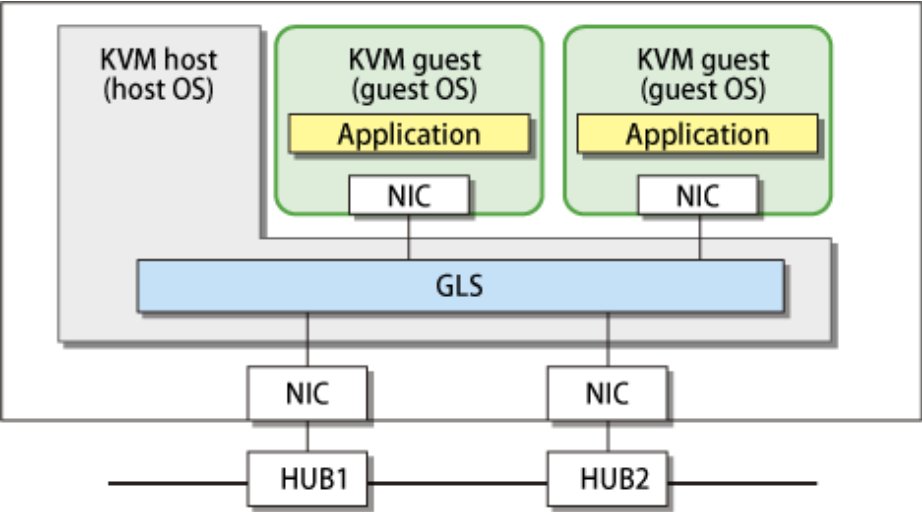
### D.3.4 Details on each configuration

#### Configuration 1: Configuration for creating a highly reliable network of KVM guests on the KVM host

This configuration is useful if KVM guests are not clustered but you want to maintain communication without being aware of KVM guest (guest OS) failures when a network failure has occurred. The KVM host (host OS) is set to the Virtual NIC mode.



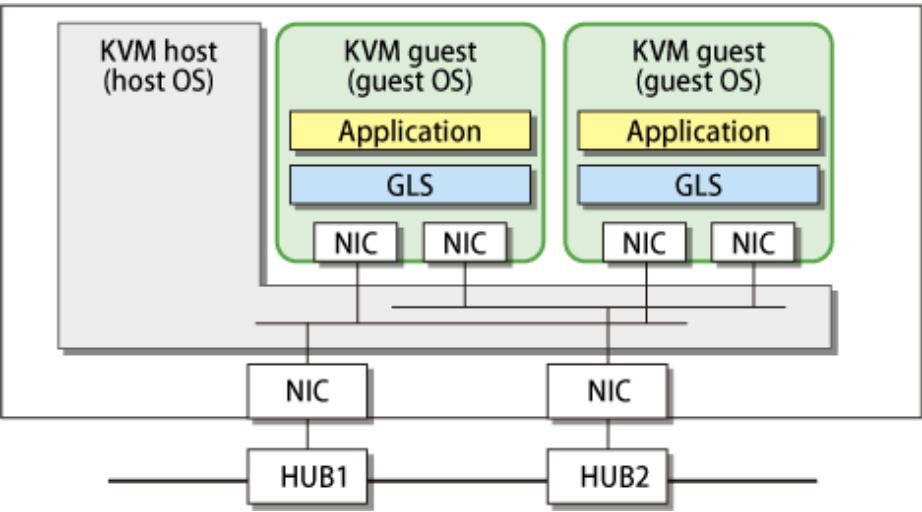
Figure D.1 Configuration 1: Configuration diagram for creating a highly reliable network of KVM guests on the KVM host



**Configuration 2: Configuration for creating a highly reliable network on KVM guests in a single system**

This configuration is useful if KVM guests are not clustered and you want to detect failures on each KVM guest when a network failure has occurred. In this configuration, each KVM guest (guest OS) can be set to either the Fast switching mode, the NIC switching mode, or the Virtual NIC mode.

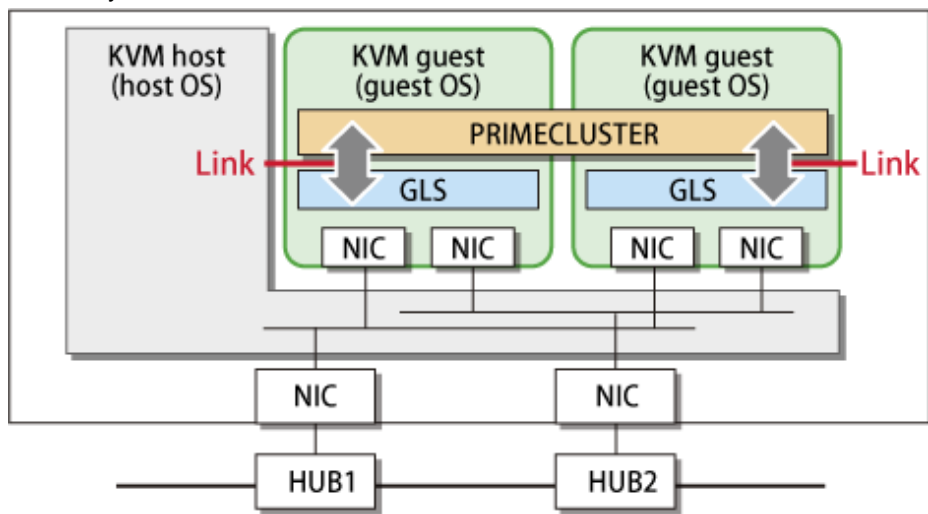
Figure D.2 Configuration 2: Configuration diagram for creating a highly reliable network on KVM guests in a single system



**Configuration 3: Configuration for creating a highly reliable network on each KVM guest in a cluster system**

This configuration is useful if KVM guests are clustered. In this configuration, each KVM guest (guest OS) can be set to either the Fast switching mode, the NIC switching mode, or the Virtual NIC mode.

Figure D.3 Configuration 3: Configuration diagram for creating a highly reliable network on each KVM guest in a cluster system



## D.4 Operation of Redundant Line Switching Mode on the Virtual Machine Function

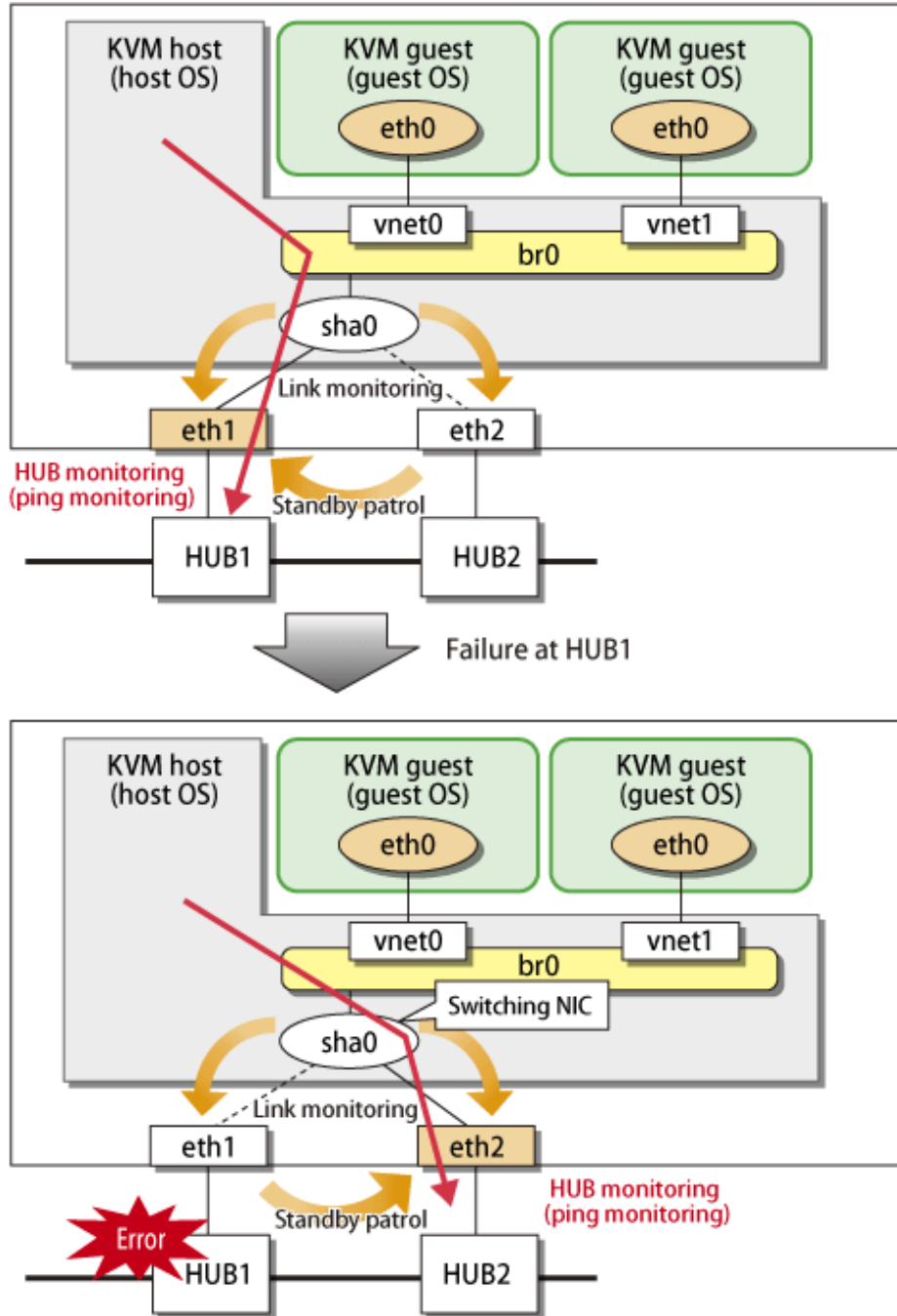
This section describes how to monitor the GLS network for each virtual network configuration and how to switch to a normal network when a network failure occurs.

### D.4.1 Configuration for creating a highly reliable network of KVM guests on the KVM host (Configuration 1)

This section describes the operation of the configuration (configuration 1) to create a highly reliable network of KVM guests on the KVM host.

If GLS on the KVM host operates on the primary interface (eth1), HUB monitoring (ping monitoring) is performed for HUB1 through eth1. If a failure occurred on HUB1, GLS switches the path from the primary interface (eth1) to the secondary interface (eth2) to keep connection.

Figure D.4 Configuration for creating a highly reliable network of KVM guests on the KVM host (Configuration 1)



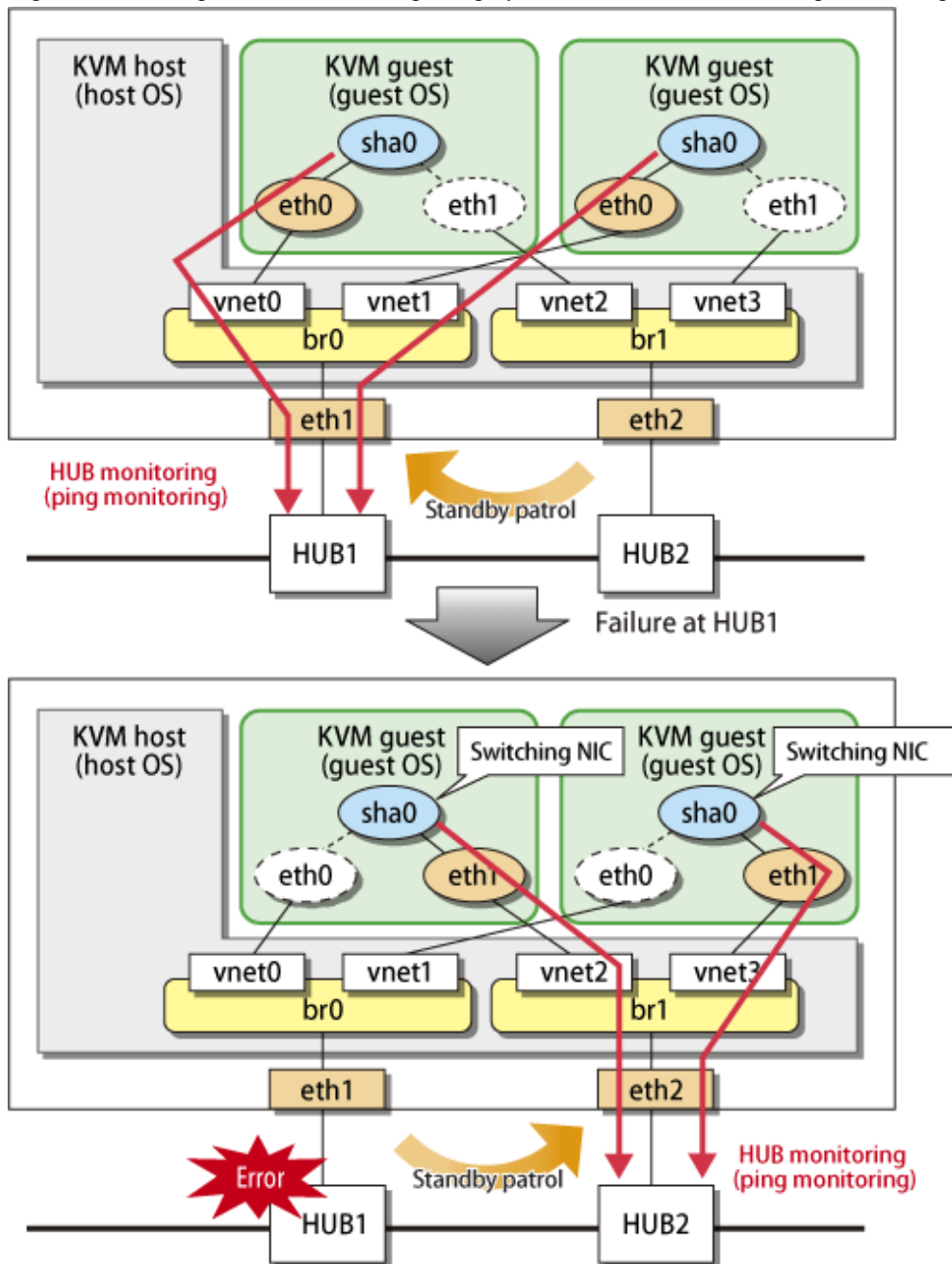
## D.4.2 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2)

This section describes the operation of the configuration (configuration 2) to create highly reliable communications on KVM guests of a single system.

If GLS on the KVM guest is using the primary interface (`eth0`), perform HUB monitoring (ping monitoring) for HUB1 via the virtual bridge (`br0`) and physical NIC (`eth1`) on the KVM host. If a failure occurs on HUB1, GLS on the guest OS maintains communications by switching from the primary interface (`eth0`) to the secondary interface (`eth1`).

In addition, perform HUB monitoring (ping monitoring) for HUB 2 via `br1` and `eth2` on the KVM host after the NIC has been switched because `eth1` is used for the NIC in use.

Figure D.5 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2)

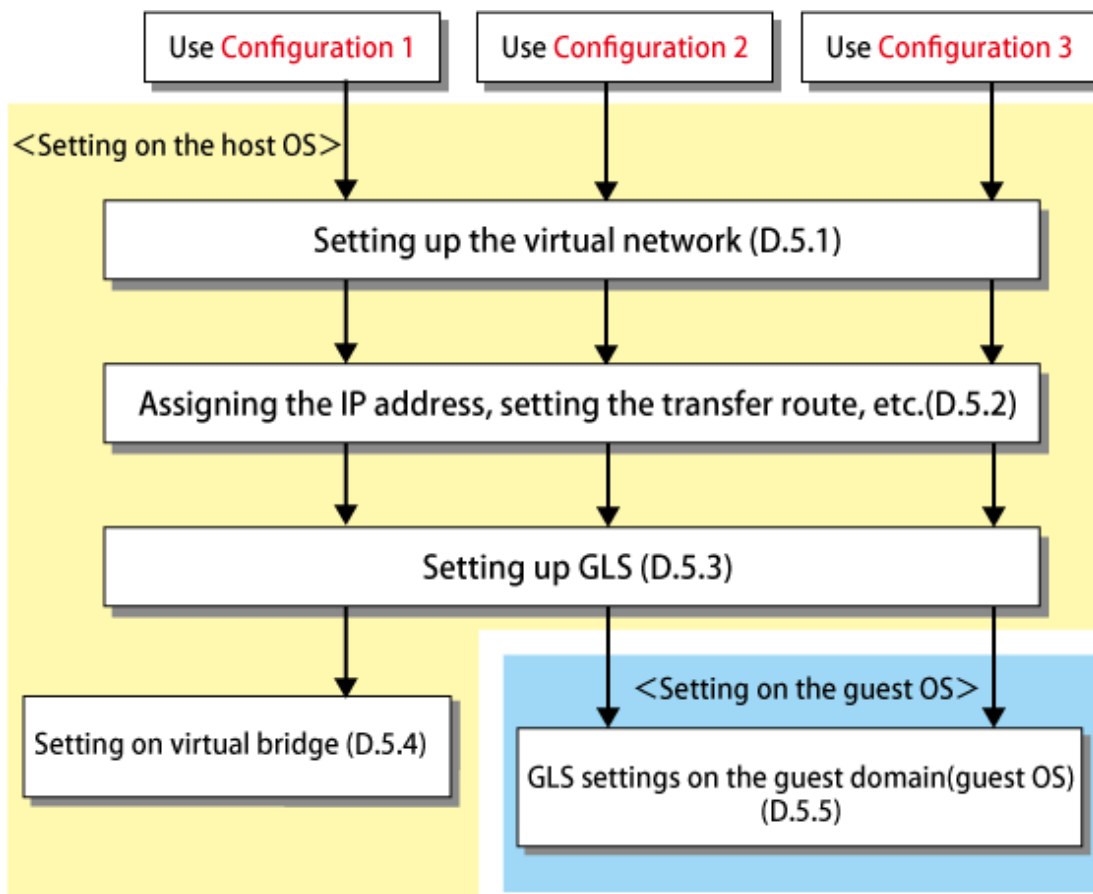


### D.4.3 Configuration for creating a highly reliable network on each KVM guest of a cluster system (Configuration 3)

This configuration is the same as the one described in "[D.4.2 Configuration for creating a highly reliable network on KVM guest a single system \(Configuration 2\)](#)". You can maintain communications in the event of a one-sided network failure. Additionally, you can take over the virtual IP address in the event of a both-sided network failure. The failover operation is the same as when a physical server is used.

## D.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function

The setup procedure is as follows. For setup examples, see "[D.6 Examples of Configuration Setup](#)".



## D.5.1 Setting up the virtual network on the host OS

For creating a highly reliable network of guest OSes (KVM guests) on the host OS (KVM host), it is required to set up a virtual interface in the Virtual NIC mode and connect it to a virtual bridge. For details on setting a virtual bridge, see the RHEL manuals.

## D.5.2 Assigning the IP address, setting the transfer route and others (for host OS)

Set up the network for the host OS. Setting up the network is the same as when the virtual machine function is not used. For details, see "[3.2.2 Network configuration](#)" and "[Appendix B Examples of configuring system environments](#)".

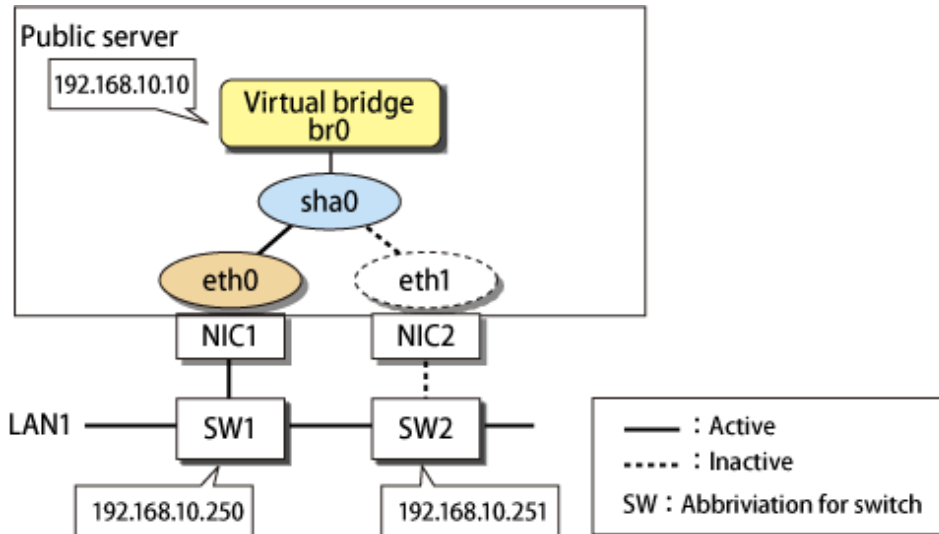
## D.5.3 Setting up GLS (for host OS)

Set up networking on the host OS. You can do this in the same way as you would when no virtual machine function is used. For details, see "[3.2.2 Network configuration](#)" and "[Appendix B Examples of configuring system environments](#)".

## D.5.4 Sample configurations for the virtual bridge

This section provides sample configurations for a virtual bridge based on the network configuration shown below.

Figure D.6 For setting the IP address to the virtual bridge (br0)



### Adding the settings for the virtual bridge

- 1) Create the settings for the virtual interface.
- 2) If the virtual interface is activated, deactivate it.

```
# /opt/FJSVhanet/usr/sbin/stphanet -n sha0
```

- 3) Create a new interface setting file.

```
# /bin/touch /etc/sysconfig/network-scripts/ifcfg-br0
```

- 4) Define IP address and other settings for the virtual bridge.

- Contents of /etc/sysconfig/network-scripts/ifcfg-br0

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=static
IPADDR=192.168.10.10
NETMASK=255.255.255.0
ONBOOT=yes
DELAY=0
```

- 5) Edit the setting file for the virtual interface.

Delete "IPADDR", "NETMASK", and similar statements related to the IP address.  
In addition, add the statement of "BRIDGE=br0".

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
BRIDGE=br0
```

- 6) Activate the virtual interface.

```
# /sbin/ifup sha0
```

- 7) Activate the virtual bridge.

```
# /sbin/ifup sha0
```

## Deleting the settings for the virtual bridge

- 1) Deactivate the virtual bridge.

```
# /sbin/ifdown br0 boot
```

- 2) Deactivate the virtual interface and dismantle the virtual bridge.

```
# /sbin/ifdown sha0 boot
```

- 3) Delete the manually created interface setting file.

```
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-br0
```

- 4) Edit the setting file for the virtual interface.

Delete the statement of "BRIDGE=br0".

In addition, add statements of "IPADDR", "NETMASK" related to the IP address as necessary.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.10.10
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

- 5) Activate the virtual interface.

```
# /opt/FJShanet/usr/sbin/strhanet -n sha0
```

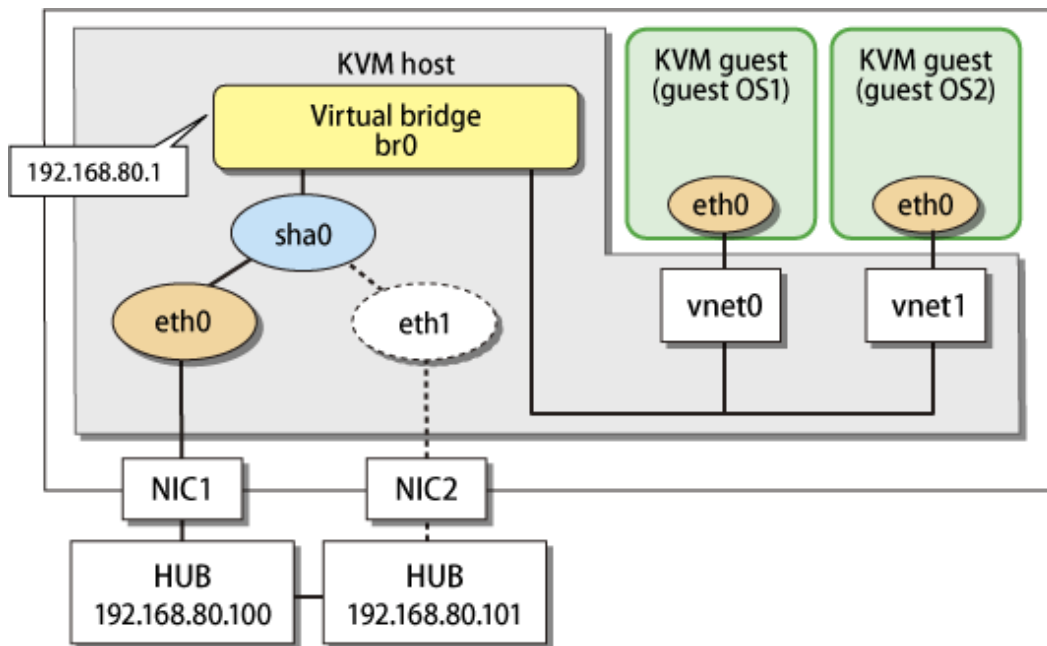
## D.5.5 Setting up GLS on guest domains (guest OSes)

The settings for installing GLS on a guest OS is the same as when the virtual machine function is not used. For details, see "[3.3 Additional system setup](#)" and "[Appendix B Examples of configuring system environments](#)".

## D.6 Examples of Configuration Setup

### D.6.1 Setup example for creating a highly reliable network of guest domains on KVM hosts (Untagged VLAN)

This section describes a configuration setup example for the following network configuration.



### 1) Setting up the system

1-1) Define the IP addresses and host names you use in the /etc/hosts file.

```
192.168.80.1    hosta    # virtual IP address of the KVM host
192.168.80.100 shhub1   # IP address of the primary monitoring destination's HUB
192.168.80.101 shhub2   # IP address of the secondary monitoring destination's HUB
```

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX files (X is 0,1) as follows:

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Configure the /etc/sysconfig/network file to enable the network setting.

```
NETWORKING=yes
```

### 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting the virtual bridge

Create /etc/sysconfig/network-scripts/ifcfg-br0 as a new interface setup file for the virtual bridge.



- Contents of /etc/sysconfig/network-scripts/ifcfg-br0

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=static
IPADDR=192.168.80.1
NETMASK=255.255.255.0
ONBOOT=yes
DELAY=0
```

#### 4) Setting a virtual interface

Define the virtual bridge name (BRIDGE=br0) of the connection target in the /etc/sysconfig/network-scripts/ifcfg-sha0 file. In addition, delete the statements related to the IP address ("IPADDR" and "NETMASK").

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
BRIDGE=br0
```

#### 5) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 6) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

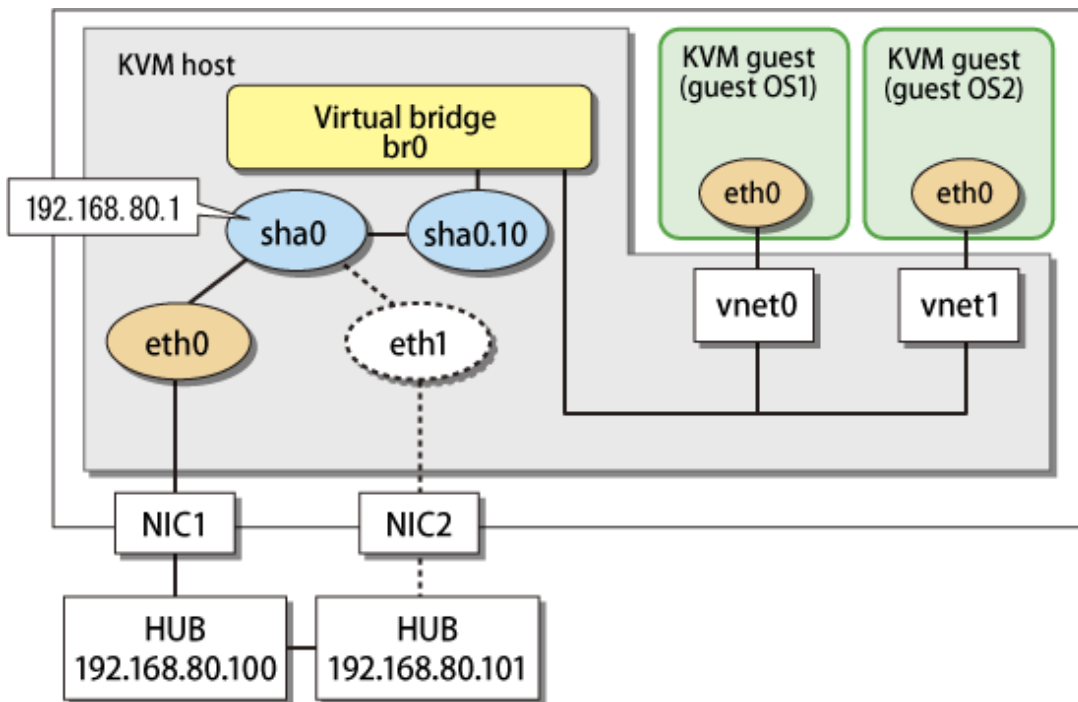
#### 7) Setting a guest OS

Edit the /etc/sysconfig/network-scripts/ifcfg-eth0 file to configure the IP address.

## D.6.2 Setup example for creating a highly reliable network of guest domains on KVM hosts (Tagged VLAN)

---

This section describes a configuration setup example for the following network configuration.



## 1) Setting up the system

1-1) Define IP addresses and hostnames in /etc/hosts file.

```
192.168.80.1    hosta    # virtual IP address of the KVM host
192.168.80.100 swhub1   # IP address of the primary monitoring destination's HUB
192.168.80.101 swhub2   # IP address of the secondary monitoring destination's HUB
```

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX files (X is 0,1) as follows:

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
DEVICETYPE=hanet
```

1-3) Configure the /etc/sysconfig/network file to enable the network and tagged VLAN settings.

```
NETWORKING=yes
VLAN=yes
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting the virtual bridge

Create /etc/sysconfig/network-scripts/ifcfg-br0 as a new interface setup file for the virtual bridge.

- Contents of /etc/sysconfig/network-scripts/ifcfg-br0

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=static
ONBOOT=yes
DELAY=0
```

#### 4) Setting a virtual interface

Define an IP address or a subnet mask in /etc/sysconfig/network-scripts/ifcfg-sha0 file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0

```
DEVICE=sha0
IPADDR=192.168.80.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

#### 5) Adding tagged VLAN interfaces

To add tagged VLAN interfaces sha0.10 on the virtual interface sha0, add the /etc/sysconfig/network-scripts/ifcfg-sha0.10 file. In addition, define the virtual bridge name (BRIDGE=br0) of the connection target.

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.10

```
DEVICE=sha0.10
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
BRIDGE=br0
```

#### 6) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 7) Reboot

Run the following command to reboot the system.

```
/sbin/shutdown -r now
```

## D.6.3 Setup example for achieving high reliability using GLS on each guest domain of a cluster system

This section describes a configuration setup example for the following network configuration.

When migrate the cluster systems on the existing physical servers to the KVM guests, use this configuration.

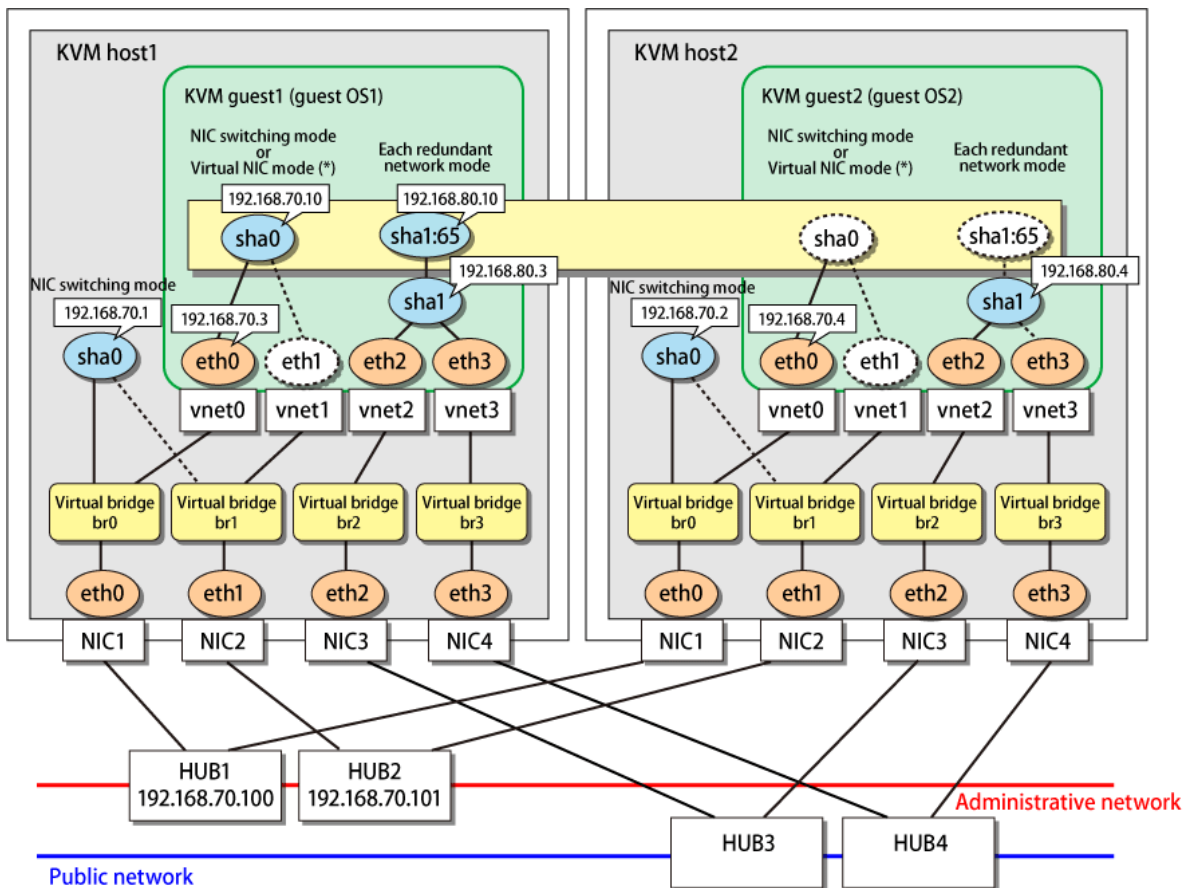
To configure GLS with a redundant NIC on KVM guests, KVM hosts need to have virtual bridges for each NIC on KVM guests. In addition, to connect to KVM hosts from the administrative LAN, bundle two virtual bridges by NIC switching mode.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



\* The figure above shows an example for NIC switching mode. For Virtual NIC mode, sha0 is always activated on both nodes in the cluster, and 192.168.70.3 and 192.168.70.4 are assigned. The takeover IP, 192.168.70.10, is assigned to sha0:65.

## [Setting up the KVM host1]

### 1) Setting up the system

1-1) Define the IP addresses and host names you use in the /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A Virtual IP
192.168.70.2    hostb    # HOST-B Virtual IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101 swhub2   # Secondary HUB IP
```

1-2) Edit /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file as follows.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br0
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br1
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
DEVICE=eth2
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br2
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
DEVICE=eth3
BOOTPROTO=static
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br3
```

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file.

```
NETWORKING=yes
```

## 2) Setting the virtual bridge

Create /etc/sysconfig/network-scripts/ifcfg-brX (X is 0,1,2,3) as a new interface setup file for the virtual bridge.

- Contents of /etc/sysconfig/network-scripts/ifcfg-br0

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=static
IPADDR=192.168.70.1
NETMASK=255.255.255.0
ONBOOT=yes
DELAY=0
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-br1

```
DEVICE=br1
TYPE=Bridge
BOOTPROTO=static
ONBOOT=yes
DELAY=0
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-br2

```
DEVICE=br2
TYPE=Bridge
BOOTPROTO=static
```

```
ONBOOT=yes  
DELAY=0
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-br3

```
DEVICE=br3  
TYPE=Bridge  
BOOTPROTO=static  
ONBOOT=yes  
DELAY=0
```

### 3) Reboot

Run the following command to reboot the system. After rebooting the system, verify ethX (X is 0,1,2,3) and brX (X is 0,1,2,3) are active using ifconfig command.

```
/sbin/shutdown -r now
```

### 4) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 5) Creating of virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t br0,br1
```



### Note

The physical IP address to be specified in the "-i" option should be identical to the physical IP address that has been set in /etc/sysconfig/network-scripts/ifcfg-br0.

### 6) Setting HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 7) Setting the standby patrol

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 8) Activating the virtual interface

```
/opt/FJSVhanet/usr/sbin/strhanet
```

### 9) Starting HUB monitoring

```
/opt/FJSVhanet/usr/sbin/hanetpoll on
```

## [Setting up the KVM host2]

### 1) Setting up the system

1-1) Define the IP addresses and host names you use in the /etc/hosts file. Defined content is same as KVM host1.

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1,2,3) file. Defined content is same as KVM host1 other than the value of HWADDR.

1-3) Define a statement to enable the network configuration in /etc/sysconfig/network file. Defined content is same as KVM host1.

### 2) Setting the virtual bridge

Edit the /etc/sysconfig/network-scripts/ifcfg-brX (X is 0,1,2,3) file. Defined content is same as KVM host1 other than the value of IPADDR.

### 3) Reboot

Run the following command to reboot the system. After rebooting the system, verify ethX (X is 0,1,2,3) and brX (X is 0,1,2,3) are active using ifconfig command.

```
/sbin/shutdown -r now
```

#### 4) Setting up GLS

Settings other than addresses specified by the -i option of the hanetconfig command are the same as those of KVM host1.

Perform steps from 4) to 9) described in [Setting up the KVM host1].

#### [Setting up the KVM host1]

Setting up GLS is the same as for physical servers. For the administrative LAN, set up Virtual NIC mode or NIC switching mode.

#### [Setting up the KVM host2]

Setting up GLS is the same as for physical servers. For the administrative LAN, set up Virtual NIC mode or NIC switching mode.

#### [Configuration by RMS Wizard]

##### 1) Configuration of userApplication

After configuring KVM host1 and KVM host2, register the created takeover virtual interface (sha0:65) as a GLS resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

##### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

### D.6.4 Setup example for creating a highly reliable network of guest domains on KVM hosts in a cluster system

---

This section describes a configuration setup example for the following network configuration.

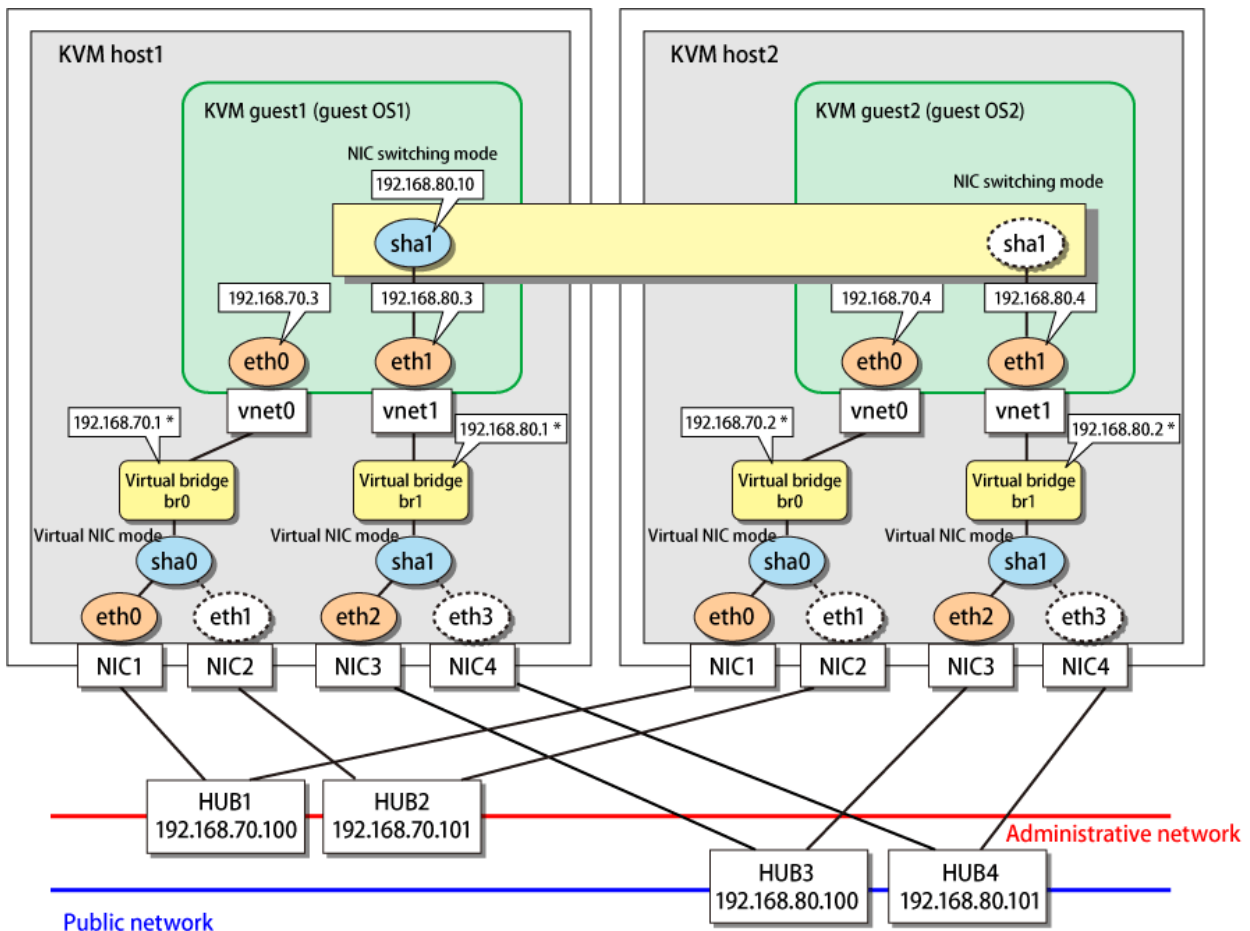
Make a redundant network on KVM hosts. To link up with the cluster system, install GLS on KVM guests. In addition to the cluster system, select this configuration when consolidating various servers to KVM guests.

For the network configuration other than GLS, refer to "[3.2.2 Network 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.



\* For Virtual NIC mode, configurations in which no IP addresses are assigned to virtual bridges can be used. In this case, error detection and switching are performed by the link status monitoring function.

### [Setting up the KVM host1 and KVM host2]

Setting up GLS is the same as for "D.6.1 Setup example for creating a highly reliable network of guest domains on KVM hosts (Untagged VLAN)". Set up virtual bridges (br0 and br1) on virtual interfaces (sha0 and sha1) on KVM host1.

### [Setting up the KVM host1 and KVM host2]

Setting up GLS is the same as for "B.4.13 Example of the Cluster system (NIC non-redundant)". However, you need to change parameters for HUB monitoring. This is to prevent NIC switching mode in KVM guests from detecting an error of the entire communication path before Virtual NIC mode in KVM hosts switches the communication.

The longest detection time in Virtual NIC mode (Link up waiting period of HUB monitoring) < The shortest detection time in NIC switching mode (Error detection time of HUB monitoring)

The table below shows the default values for each mode.

Mode	Item	Setting value	Error detection time	
Virtual NIC mode	Link up waiting period	45	47 sec	(3 sec x 15 times + 2 sec)
NIC switching mode	Error detection time	5 x 5	22 sec	(5 x (5 - 1) + 2 sec)

For parameters for HUB monitoring, set the values so that the shortest detection time in NIC switching mode (22 seconds) becomes longer than the longest detection time (47 seconds) in Virtual NIC mode.



For example, to change the parameters for NIC switching mode to 52 seconds, set as follows:

```
/opt/FJSVhanet/usr/sbin/hanetpoll off
```

```
/opt/FJSVhanet/usr/sbin/hanetpoll on -c 11
```

Mode	Item	Setting value	Error detection time	
Virtual NIC mode	Link up waiting period	45	47 sec	(3 sec x 15 times + 2 sec)
NIC switching mode	Error detection time	5 x 11	52 sec	(5 x (11 - 1) + 2 sec)



## Point

.....

In Virtual NIC mode, the network monitoring is performed by 5 times at intervals of 3 seconds after starting the operation. However, just after the monitoring started, error detection will be pended until the waiting time for linkup (45 seconds) elapses. Therefore, the longest detection time in Virtual NIC mode is required to be estimated by the linkup waiting time.

.....

## [Configuration by RMS Wizard]

### 1) Configuration of userApplication

After configuring KVM host1 and KVM host2, register the created takeover virtual interface as a Gls resource to create a cluster application. Use RMS Wizard to set up the cluster configuration. For details, see "PRIMECLUSTER Installation and Administration Guide".

### 2) Starting of userApplication

After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## Appendix E Operation on VMware

This chapter describes the operation of GLS on VMware. For details on VMware, see the manuals for VMware.

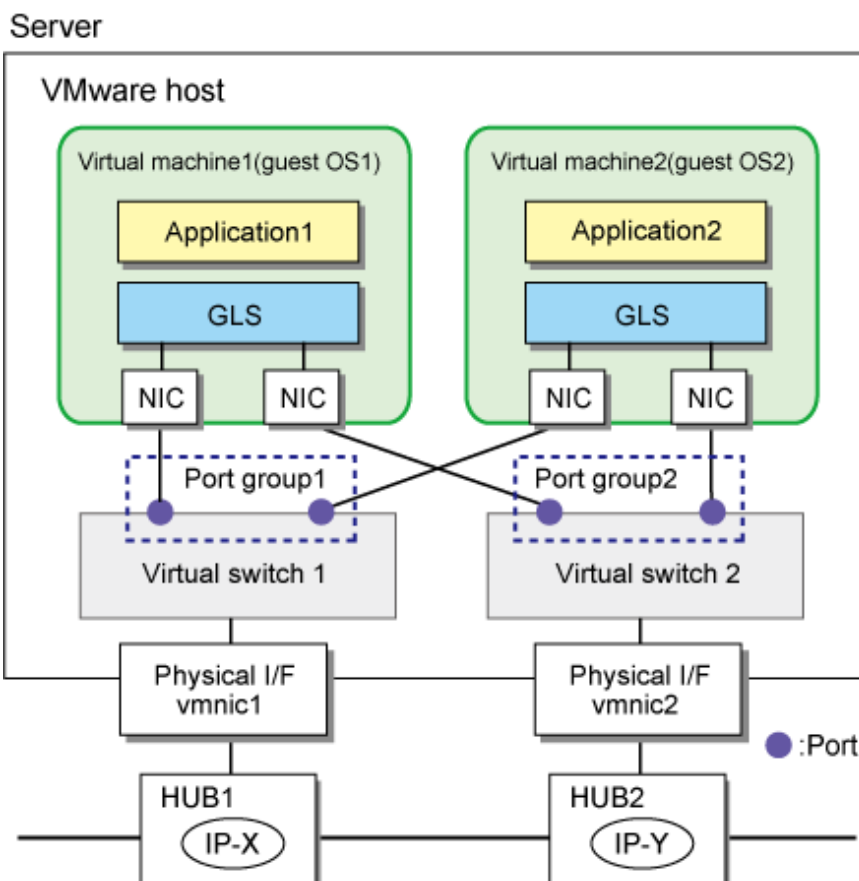
### E.1 VMware Overview

VMware is a product offered by VMware, Inc., which achieves server virtualization. Server virtualization enables you to consolidate multiple servers on one server.

### E.2 Configuration of VMware

In a VMware environment, servers on which applications operate are consolidated into a guest OS of VMware as a virtual machine. NICs of a guest OS are connected to ports on the virtual switch on the VMware host. A guest OS communicate with external devices via this virtual switch. Ports on the virtual switch are managed by VMware as a port group.

GLS operates on a guest OS of VMware. A redundant network can be provided by bundling the ports on the virtual switch.



### E.3 Virtual Network Design in VMware

#### E.3.1 Concept of network configuration in VMware

For a virtual network required for VMware, see the manuals for VMware.

To make a redundant network by using GLS on a guest OS of VMware, ports bundled by GLS must be connected to different virtual switches. Therefore, as many virtual switches as ports bundled by GLS are required.



## Note

When using the virtual NIC mode, set [Accept] for [Promiscuous Mode] under [Security] for each virtual switch in VMware.

## E.3.2 Support set for each redundant line switching mode

GLS provides highly reliable network communications for guest OSes. The following table shows the compatibility between redundant line switching methods and guest OSes.

Note that it is not possible to install GLS on the VMware host.

	Guest OS
Fast switching mode	O
NIC switching mode	O
Virtual NIC mode	O
GS linkage mode	O

O: Supported X: Not supported



## Note

- When using the virtual NIC mode, specify the MAC address to the virtual interface configuration file by using SHAMACADDR. For details, see "[3.3.3 Virtual NIC mode](#)."
- When using the virtual NIC mode on a VMware guest OS, a tagged VLAN interface is not usable. For a tagged VLAN connection, set the VLAN ID for a port group of VMware.
- When bundling the interface that was created by SR-IOV, use the NIC switching mode.

## E.4 Operation of Redundant Line Switching Mode on VMware

This section describes how to monitor the GLS network for the virtual network configuration of VMware and how to switch to a normal network when a network failure occurs.

### E.4.1 Configuration for creating a highly reliable network on guest OSes in a single system

This section describes the operation of the configuration to create a highly reliable network using guest OSes of VMware.

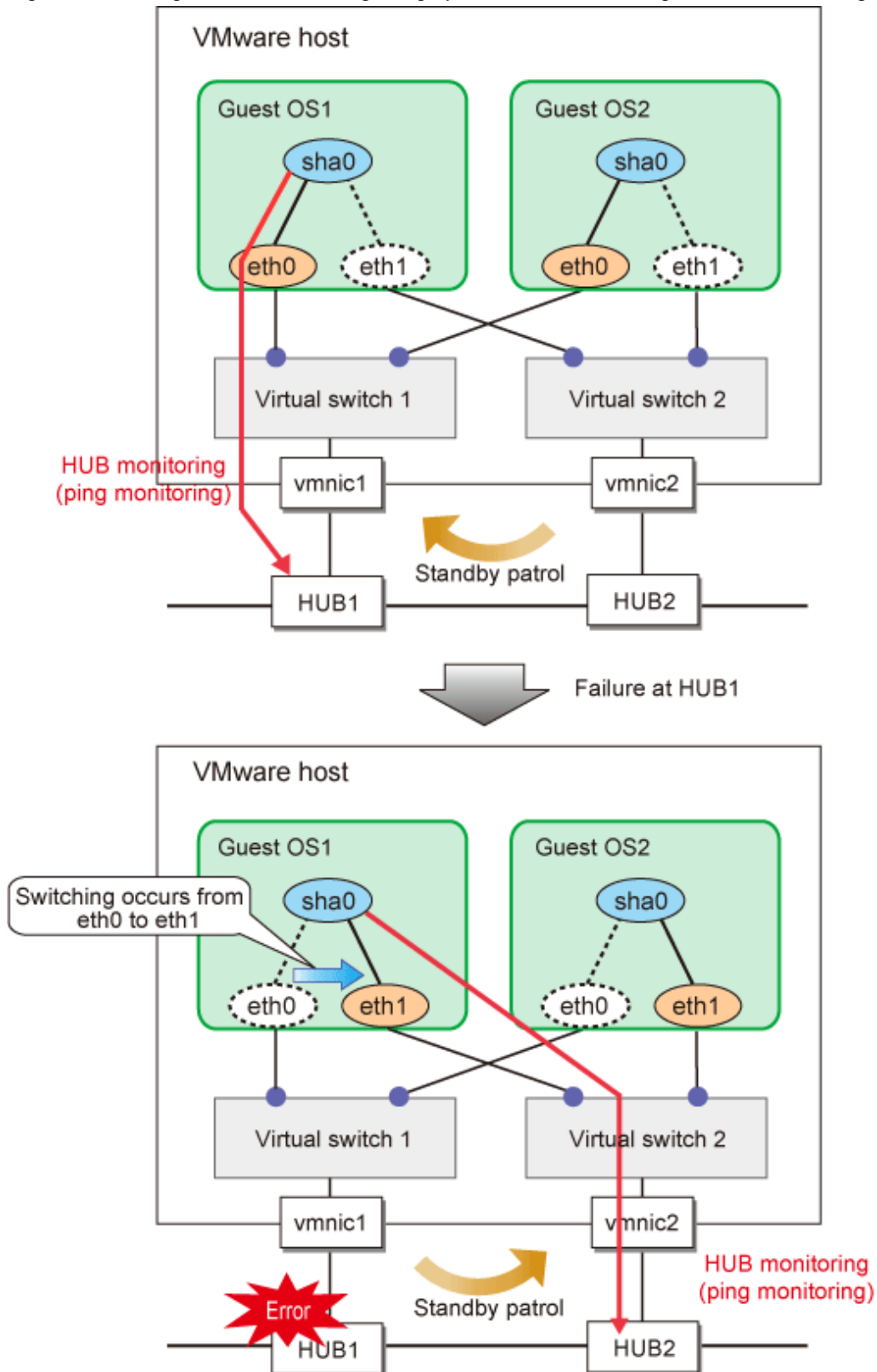
For the operation of GLS in VMware, there is no difference from the operation on a physical server.

NIC switching mode is provided as an example in this section.

#### NIC switching mode

GLS on a guest OS performs HUB monitoring (ping monitoring) for HUB1 placed outside the server. If a failure occurred on HUB1, GLS switches the path from the primary interface (eth0) to the secondary interface (eth1) to keep connection. In addition, vmnic2 becomes the active NIC after the connection is switched to eth1. Then, HUB monitoring (ping monitoring) is performed for HUB2 via the virtual switch 2 and the active NIC (vmnic2).

Figure E.1 Configuration for creating a highly reliable network on guest OSes in a single system



## E.4.2 Configuration for creating a highly reliable network on guest OSes in a cluster system

This configuration is the same as the one described in "[E.4.1 Configuration for creating a highly reliable network on guest OSes in a single system](#)". You can maintain communications in the event of a one-sided network failure. Additionally, you can take over the virtual IP address in the event of a both-sided network failure. The failover operation is the same as when a physical server is used.

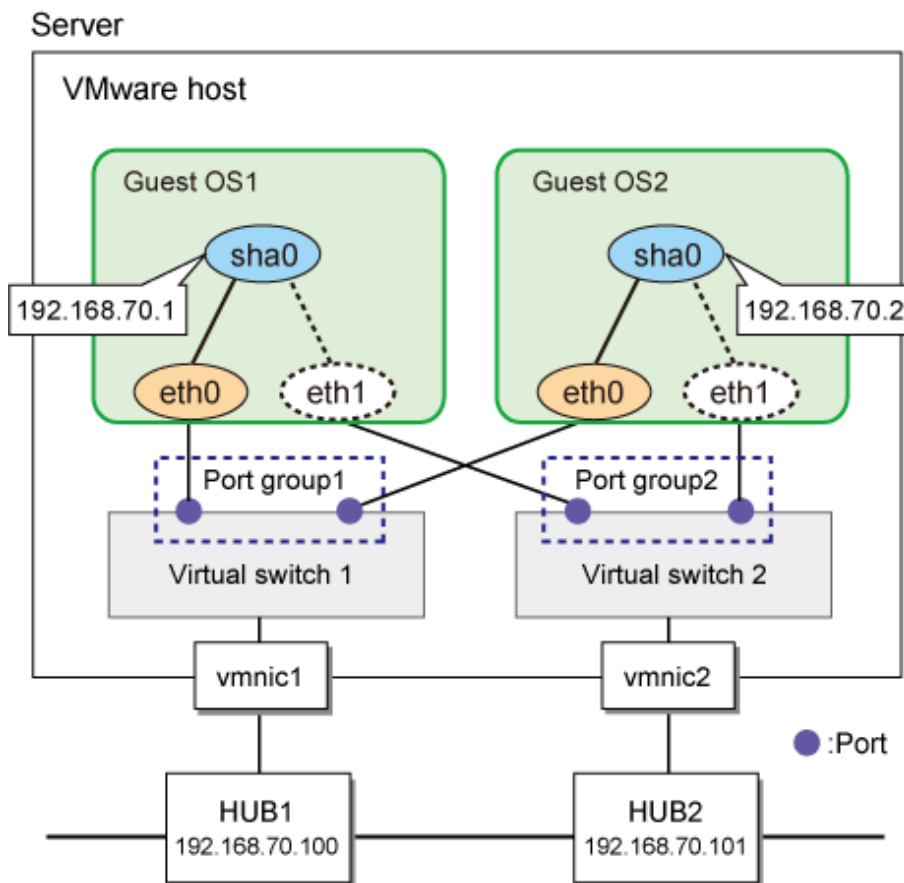
## E.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function

According to the manuals for VMware, configure guest OSes or virtual switches. After installing GLS on guest OSes, perform the same procedure as that of physical servers for configuration.

## E.6 Examples of Configuration Setup

### E.6.1 Setup example for creating a highly reliable network of guest OSes

This section describes a configuration setup example for the following network configuration.



#### [Setting up VMware host]

Set up each interface of guest OSes so that they are connected to ports of different virtual switches.

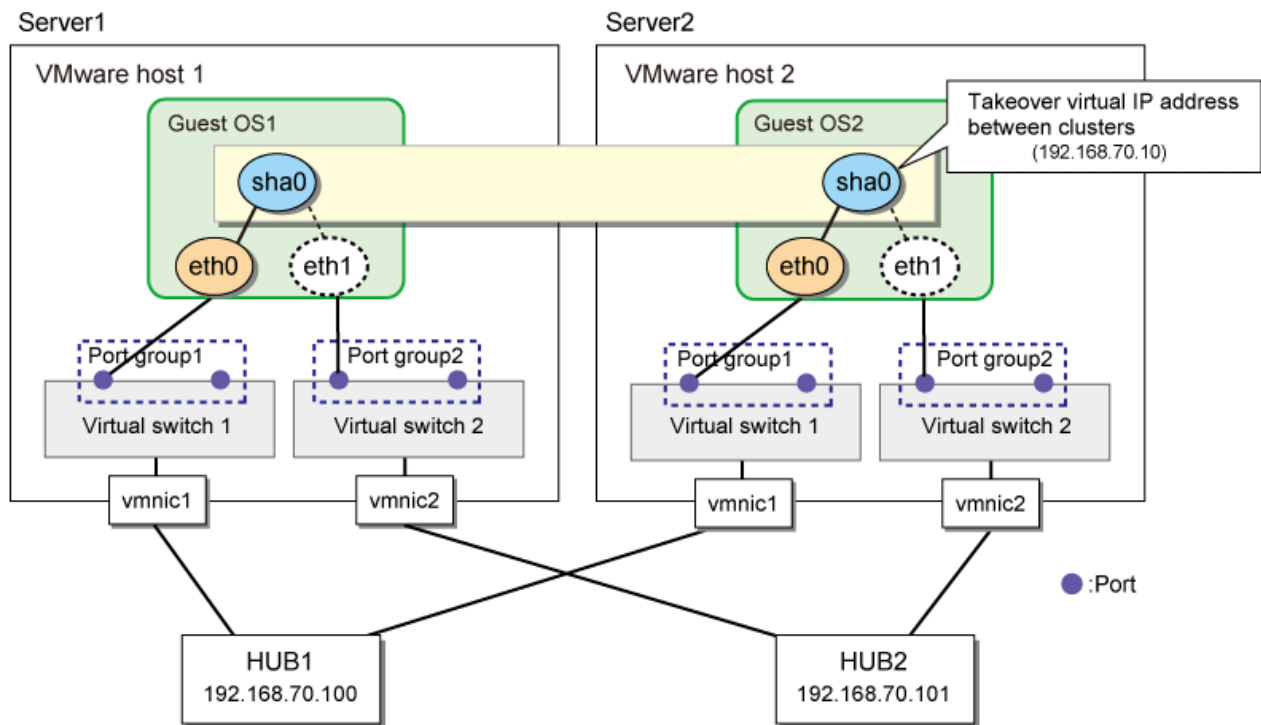
When using the virtual NIC mode, set [Accept] for [Promiscuous Mode] under [Security] for each virtual switch in VMware.

#### [Setting up the guest OS1 and the guest OS2]

Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

## E.6.2 Setup example for creating a highly reliable network of guest OSes in a cluster system

This section describes a configuration setup example for the following network configuration.



### [Setting up VMware host]

Set up each interface of guest OSes so that they are connected to ports of different virtual switches.

### [Setting up the guest OS1 (active node)]

Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

### [Setting up the guest OS2 (active node)]

Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

## Appendix F Trouble shooting

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.

### F.1 Communication as expected cannot be performed (Common to IPv4 and IPv6)

#### F.1.1 The route information set by a route command is deleted

**Symptom:**

The static route information set by a route add command is deleted.

**Corrective action:**

The static route information configured with "route add" command may be deleted when activating/inactivating the interface and detecting failure on the transfer path.

When routing daemon is not used, define the static route information on the OS configuration file (/etc/sysconfig/network-scripts/route-ethX). When using the routing daemon, define the static route information on the routing daemon configuration file.

For details regarding this configuration, refer to "[3.2.2 Network configuration](#)".

#### F.1.2 Automatic address configuration lags behind for IPv6

**Symptom:**

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.

**Corrective action:**

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 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 operating NIC and standby NIC or modify the router setting so that a router transmits the router advertisement message within a few minutes interval.

#### F.1.3 Communication is not switched in the event of HUB monitoring error in Virtual NIC mode

**Symptom:**

In an environment where Virtual NIC mode is used, the communication is not switched even when the switch of HUB monitoring (ping monitoring) is turned off.

**Corrective action:**

Check the monitoring status of the standby patrol by the "dspathmon" command. If the monitoring status is ACTIVE, the standby patrol function is operating normally. Therefore, switching of the communication does not occur.

```
# /opt/FJSVhanet/usr/sbin/dsppathmon

Status Name VLAN Primary Target/Secondary Target Patrol
+-----+-----+-----+-----+-----+-----+
ON sha0 u/t 192.168.70.100(FAIL)/192.168.70.101(WAIT) ACTIVE
```

In Virtual NIC mode, if both HUB monitoring and the standby patrol fail, switching of the communication occurs. By combining different two monitoring methods, unnecessary communications are suppressed

Examples for "when the communication is not switched" and "when the communication is switched" are shown below.

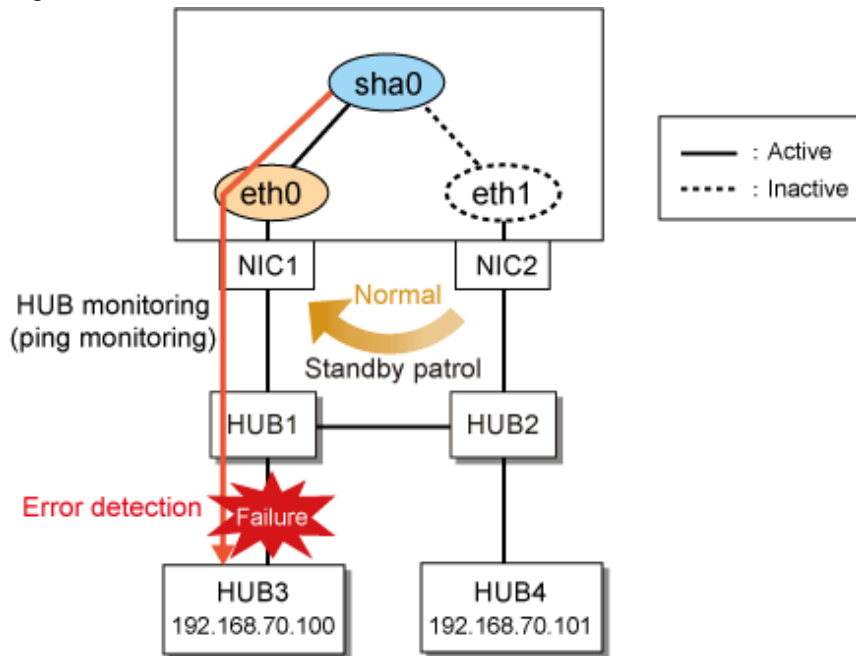


## Example

### When the communication is not switched

In the case of [Figure F.1 When the communication is not switched](#), HUB monitoring fails, but the standby patrol is normal. In this case, switching of the communication does not occur even if the communication is switched from eth0 to eth1, because the communication with HUB3 is not available.

Figure F.1 When the communication is not switched



## Example

### When the communication is switched

In the case of [Figure F.2 When the communication is switched \(1\)](#) and [Figure F.3 When the communication is switched \(2\)](#), both HUB monitoring and the standby patrol fail. In this case, the communication with HUB3 becomes available by switching the communication from eth0 to eth1.



Figure F.2 When the communication is switched (1)

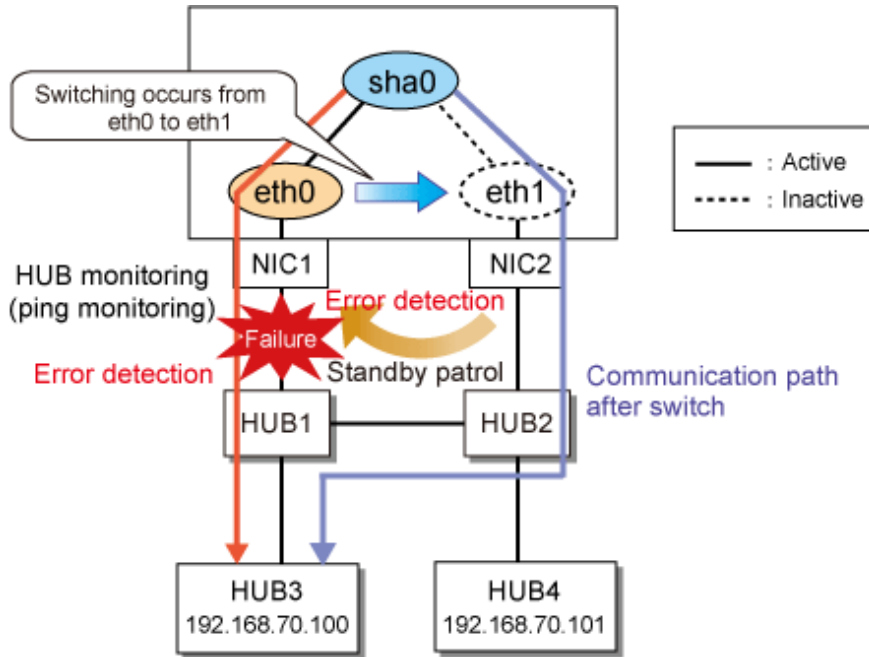
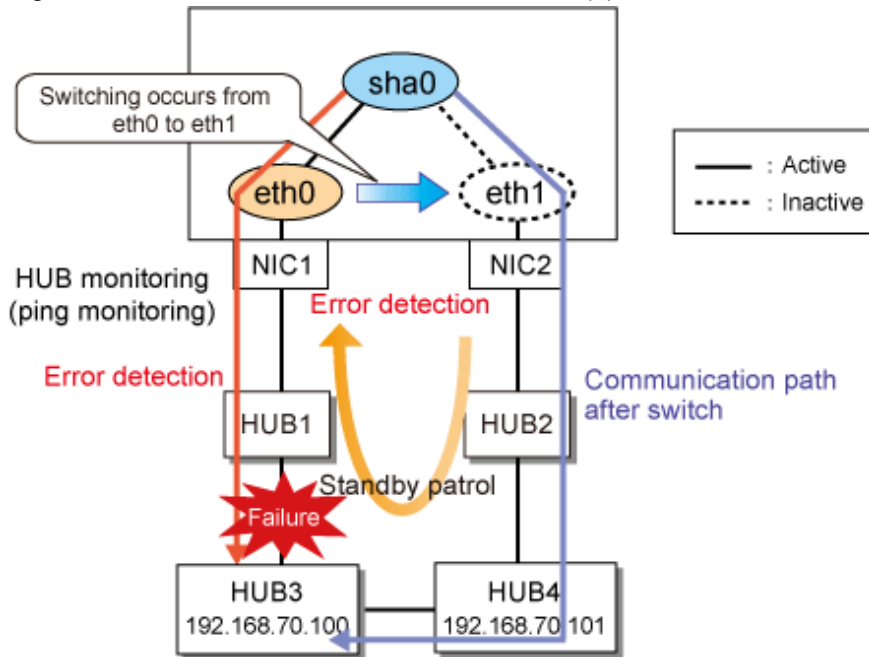


Figure F.3 When the communication is switched (2)



## F.2 Virtual interface or the various functions of Redundant Line Control Function cannot be used

### F.2.1 An interface of NIC switching mode is not activated

#### Symptom:

The following message is output and activation of an interface fails.

```
hanet: ERROR: 85700: polling information is not defined. Devname = sha0(0)
```

#### Corrective action:

In NIC switching mode, switching interfaces inside a node and between nodes are 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. It is necessary to set the monitor-to information by a hanetpoll create command. When the monitor-to information is not set, a takeover IP address is not activated either. Activation of a service fails in cluster operation.

When using a logical address takeover function, and also when sharing a physical interface, it is 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.

## F.2.2 It does not failback at the time of the restoration detection by standby patrol in NIC switching mode

---

#### Symptom:

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.
(shal)
```

#### Corrective action:

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 be displayed 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.

## F.2.3 Error detection message displays for standby patrol in NIC switching mode

---

#### Symptom:

The following message is output and activation of an interface fails.

```
hanet: WARNING: 87500: standby interface failed.
```

#### Corrective action:

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 (IEE802.1Q 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.

## F.3 Failure occurs during operation (Common to both Single and Cluster system)

### F.3.1 Error messages(870) and corresponding actions for HUB monitoring

#### Symptom:

The following messages (\*1) are output to the system log, and the switch of NIC occurs.

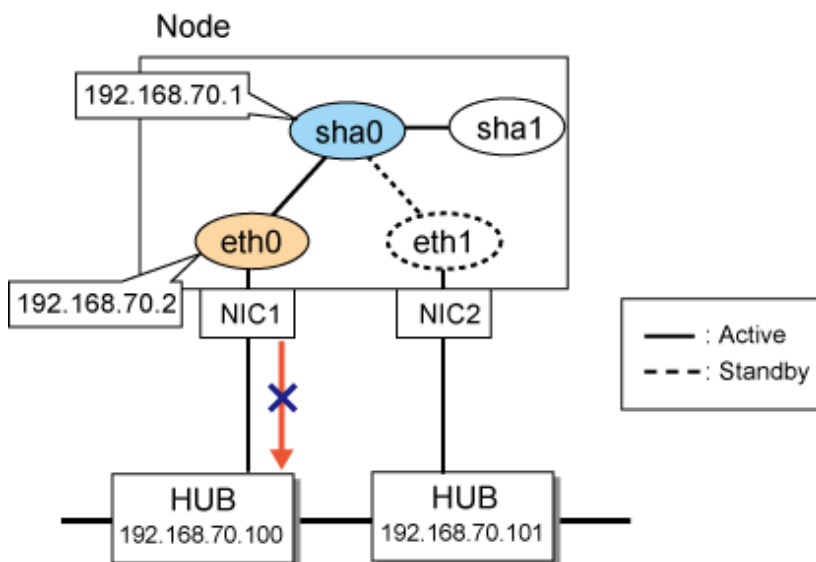
```
hanet: ERROR: 87000: polling status changed: Primary polling failed.  
(eth0,target=192.168.70.100)
```

```
# /opt/FJSSVhanet/usr/sbin/dsppoll
```

```
Polling Status      = ON  
interval(idle)      = 5( 60)  
times                = 5  
repair_time         = 5  
link detection       = NO  
FAILOVER Status     = YES
```

Status	Name	Mode	Primary Target/Secondary Target	HUB-HUB
ON	sha0	d	192.168.70.100(FAIL)/192.168.70.101(ON)	OFF

\*1) When using the second NIC as an active NIC, "Secondary polling" will be output instead of "Primary polling".



#### Corrective action:

Run the ping in specified monitored targets and monitoring the transmission path by NIC switch methods. When the communication failure of ping was detected, this message was output and NIC was switched. Please confirm the following items.

- Switch occurs during importing/constructing changes

Since settings of the GLS and errors of network structure caused a lot of switches during importing/ composing changes, please confirm the following items.

Confirmation item	
Cable	Connection confirmation
	Category
GLS settings	Settings of monitored targets
	Settings of monitoring parameters
	Netmask settings
HUB settings	Confirmation of STP settings
	VLAN-ID
Network status	Communication load
	System log
Settings of the own node	IP filter
	Settings of network address
	IP address

- When switch occurs in operation process

Since a lot of switches are caused by abnormal transmission path, confirm the following items.

Confirmation item	
Cable	Connection confirmation
	Category
HUB settings	Confirmation of communication mode
	Qos
Network status	Confirmation of maintenance working status
	Communication load
	HUB status
	System log
GLS settings	Settings of monitored targets

Detail of each confirmation item is as follows.

Confirmation item		Contents
Cable	Connection confirmation	1) Cable may be disconnected. Please confirm that the cable is connected with the node and HUB. 2) Cable may be damaged. Please confirm whether the LED light of the port that is connected with the cable in HUB is on. Please change the cable when the LED light is not on. 3) Please confirm that the cable has been connected correctly. 4) Changes to the installation location of server and settings of network port may result in changes to the internal connection wires in Blade server or PRIMEQUEST environment. Please Confirm whether the status of the connection wires is correct. 5) Generally, in the NIC switching mode, the NIC that is set to primary should be connected with the HUB which has the monitored IP address that is set to primary.
	Category	1) Confirm whether the category (straight cable, cross cable) used by cable is correct. In addition, if the communication mode is not set to auto negotiation, the function (Auto-MDIX) of automatic cable category identification will be invalid. For details, refer to the HUB manual.

Confirmation item		Contents
		2) Confirm whether the cable category (Category 5, Category 5e) that is used is matched with the transmission rate and cable length.
GLS settings	Settings for monitored targets	When the IP address of HUB that is the monitored target is different from the one defined as monitored target, failure of monitoring will occur and switch will be performed. Please confirm whether the two IP addresses mentioned above are in accordance by the hanetpoll command.
	Settings for monitoring parameters	The monitoring by ping is set to judge an abnormal transmission path when continuously failing five times every five seconds in default. When the parameter is set too short, incorrect switch (Incorrect switch still occur even if the transmission path is correct) may occur. When incorrect switch occurs frequently, please increase the monitoring time for transmission path anomaly.
	Netmask settings	When Netmask settings are incorrect, communication may fail. Please confirm Netmask is set by the ifconfig command. Confirm that the settings have completed by the hanetmask command.
HUB settings	Communication mode	Please confirm whether the communication mode set to the port of the interface matches that of HUB. When the communication mode of the HUB is different from that of the own node, the collision might result in the packet lost frequently. (For example: When setting the own node to auto negotiation and setting HUB to fixed full duplex) In addition, the following communication modes are required among the computers connecting with the Ethernet. - auto negotiation - auto negotiation - 100M full duplex - 100M full duplex - 100M half duplex - 100M full duplex - 10M full duplex - 10M full duplex - 10M half duplex - 10M half duplex
	STP settings	The communication will be disabled for about 30 seconds after the activation of the interface of GLS and the switch when STP (spanning tree protocol) becomes valid. During this period, the GLS suppresses the switch of NIC due to the failure of the HUB monitoring. Set the controlled time by the hanetpoll command as the parameter "Time of delay for Linking Up" (60 seconds in default). Incorrect switch of NIC may occur if this parameter value is small. Processing it in the following methods. 1) Change the parameter settings to prevent incorrect switch. 2) Invalidate STP of used HUB port in the network where the transmission of packet does not form loop.
	VLAN-ID	Errors may occur in VLAN-ID settings. Confirm whether the following VLAN-IDs are in accordance. 1) VLAN-ID of the port connected with the cable of primary NIC 2) VLAN-ID of the port connected with the cable of secondary NIC 3) VLAN-ID that is set as a monitored target by the management IP address of HUB
	QoS	When setting a low priority for ping in the QoS (Quality of Service) settings of HUB, the ping response from HUB might be delayed in network with a high load. In this case, switch of NIC may occur even if the transmission path is in correct. Please check the settings of QoS.
Network status	Maintenance work	Please confirm neither the reactivation of the monitored targets HUB nor the maintenance work of the exchange, etc, are done during the period of switch. In addition, when changing the monitored targets HUB, the HUB must be changed after the HUB monitor is stopped.
	Communication load	The delay and the packet lost of Ping may be caused by temporary high communication traffic of the network during the period of switch. Please confirm whether there are conflict and packet loss from the statistic information and logs of HUB. Please confirm the amount of received and sent packets etc. by the sar command in Linux environment. In addition, in the environment where the network

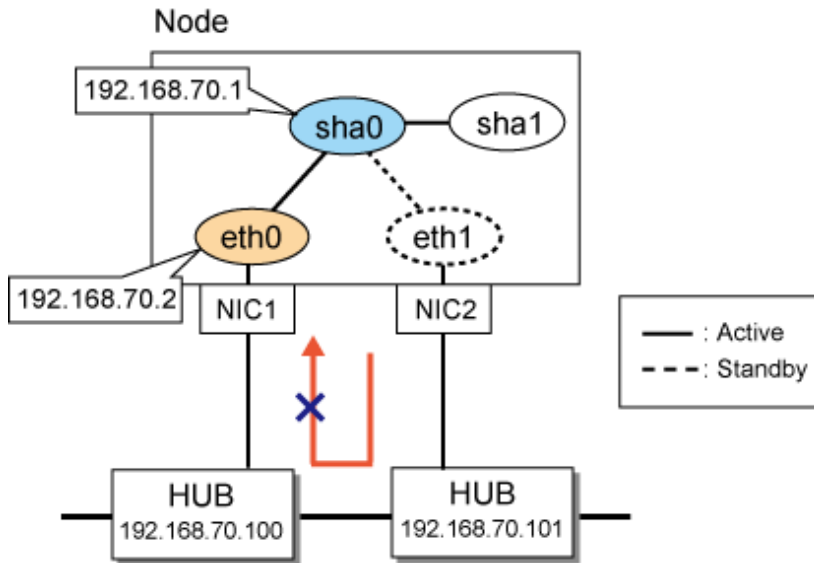
Confirmation item		Contents
		with different types of speed (1Gbps and 100Mbps, etc.) exists, even if the unoccupied bandwidth exists in a high-speed network, the packet may still be lost when transferring from the HUB to a low-speed network. Please confirm whether the traffic has been estimated correctly.
	HUB status	Errors may occur in HUB and the power supply may be cut off. Please confirm whether the link down message has been output to the system log. Packet might loop when errors occur in HUB, confirm whether a conflict has occurred by the netstat command. Moreover, when setting HUB monitoring function of a monitored target excluding adjacent HUBs, the cable connected with HUB and the monitored target may be disconnected.
	System log	1) The NIC that monitors HUB might have been linked down. Please confirm whether the link down message has been output to the system log during the period of switch. 2) Hardware (NIC or PCI bus and CPU or memory etc.) may have faults. The messages that indicate hardware faults might be output, please confirm the system log.
Settings for the own node	IPfilter	The IP packet to the interface used by the GLS might be filtered. Please confirm the setting of the firewall when you filter IP, and set that packets of ping can pass the firewall.
	Setting of network address	Please run the netstat -rn command to confirm that there is no virtual IP address of GLS same as transmission path of network. When the network is overlap, transmission of ping cannot be done by a correct path (HUB monitoring). Therefore, NIC switch cannot be performed when faults occur in the transmission path used by the GLS. Conversely, switch will occur when faults occur in the transmission path that has not been used by the GLS. Please check settings of IP address and netmask. In addition, confirm that there is no more than 3 NICs have been connected on the same subnet in the network structure (more than 2 types of structures of NIC combination that is bound with the virtual interface are in one subnet). Please check the construction in certain conditions.
	IP address	Please confirm that the IP address set in the own node is different from the ones set in other nodes. When the IP address is repeated, the response of ping from communication target is sent to the node address whose node is different from the transmission source node, and unable to communicate sometimes. In this case, the HUB monitor fails.

### F.3.2 Error messages(875) and corresponding actions for standby patrol

#### Symptom:

The following messages are output to the system log.

```
hanet: WARNING: 87500: standby interface failed. (sha1)
```



### Corrective action:

The standby patrol performs NIC switching by sending and receiving the monitoring frame via adjacent HUB from standby NIC (eth1) to active NIC (eth0). (When the primary NIC is using in communication at present) The message is output when cutting off the receiving and sending of the monitoring frame, the main output patterns are classified into the following four types.

#### Pattern 1:

Output the error messages that anomalies are detected by the standby patrol when the system is started, and the status of standby patrol output by the dsphanet command is in FAIL.

The following messages are output to the system log.

```
hanet: WARNING: 87500: standby interface failed. (sha1)
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active  d    OFF  eth0(ON),eth1(OFF)
sha1      Active  p    OFF  sha0(FAIL)
```

In pattern 1, the monitoring frame of the standby patrol may not reach to primary NIC (eth0) due to the HUB setting errors or cable connection errors.

#### Pattern 2:

Output messages that indicate normal working of the standby patrol when starting the system, and output the messages that indicate error occurrence in the standby patrol during operating. The status of the standby patrol output by the dsphanet command is in FAIL.

```
hanet: INFO: 89600: path to standby interface is established. (sha1)
:
hanet: WARNING: 87500: standby interface failed. (sha1)
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+-----+-----+-----+
sha0      Active  d    OFF  eth0(ON),eth1(OFF)
sha1      Active  p    OFF  sha0(FAIL)
```

In pattern 2, network faults may occur.

### Pattern 3:

Output messages that indicate the standby patrol anomalies during operation, and output messages indicating recovery after waiting for a moment, or the messages indicating anomaly and recovery are output in alternately.

```
hanet: INFO: 89600: path to standby interface is established. (sha1)
:
hanet: WARNING: 87500: standby interface failed. (sha1)
hanet: INFO: 88500: standby interface recovered. (sha1)
:
hanet: WARNING: 87500: standby interface failed. (sha1)
hanet: INFO: 88500: standby interface recovered. (sha1)
```

In pattern 3, the monitoring frame may lose temporarily due to error settings of HUB or GLS and increased network load.

### Pattern 4:

Output the messages indicating that anomalies are detected by the standby patrol every time when the system is started. Afterwards, and the message indicating recovery may be output immediately. Moreover, the status of standby patrol in operation is "ON".

```
hanet: WARNING: 87500: standby interface failed. (sha1)
hanet: INFO: 88500: standby interface recovered. (sha1)
```

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL   Device
+-----+-----+-----+-----+-----+
sha0      Active   d    OFF  eth0(ON),eth1(OFF)
sha1      Active   p    OFF  sha0(ON)
```

There is no problem in operation for pattern 4. When the STP (Spanning Tree protocol) is valid in HUB, the monitoring frame cannot be sent and received for about 30 seconds even if the interface has been linked up because of the transmission delay timer of STP. Therefore, Communication can be performed normally after ending the transmission delay timer when temporary errors are detected by the standby patrol. In addition, the output message can be suppressed by changing the settings.

Confirm the following items based on message output patterns.

Message output patterns	Confirmation items	
Pattern 1	HUB settings	Ethernet frame type VLAN ID
	Status of the own node and the network	HUB status System log
	Cable	Connection confirmation Category
Pattern 2	Status of the own node and the network	HUB status System log
	Cable	Connection confirmation Category
Pattern 3	GLS setting	MAC address
	HUB settings	Communication mode
	Status of the own node and the network	Maintenance work HUB status System log Communication load
Pattern 4	HUB settings	STP settings



Details of each confirmation item are as follows.

Confirmation item		Contents
Cable	Connection confirmation	<p>1) Please confirm the port of HUB connected with primary NIC and secondary NIC is correct. Please confirm the cascade connection between HUBs when connecting to a HUB that the primary NIC is different from the secondary NIC. Moreover, please confirm that the cable is not disconnected, which is indicated by the LED of NIC and HUB.</p> <p>2) The installation location of server and the settings of network port may cause changes of internal connection wires in the Blade server or PRIMEQUEST environment. Please confirm whether the connection wires are correct.</p>
	Category	<p>1) Confirm whether the category (straight cable, cross cable) used by cable is correct. In addition, if the communication mode is not set to auto negotiation, the function (Auto-MDIX) of automatic cable category identification will be invalid. For details, refer to the HUB manual.</p> <p>2) Confirm whether the cable category (Category 5, Category 5e) that is used is matched with the transmission rate and cable length.</p>
HUB settings	Ethernet frame type	The standby patrol monitoring by receiving and sending the monitoring frame. Communications can be performed by monitoring frame in most HUBs, but the HUB that cannot support monitoring frame in default settings also exists. In this case, please reset the HUB to enable arbitrary Ethernet frame to pass.
	Communication mode	<p>Please confirm whether the communication mode set to the port of the interface matches that of HUB. When the communication mode of the HUB is different from that of the own node, the collision might result in the packet lost frequently. (For example: When setting the own node to auto negotiation and setting HUB to fixed full duplex) In addition, the following communication modes are required among the computers connecting with the Ethernet.</p> <ul style="list-style-type: none"> <li>- auto negotiation - auto negotiation</li> <li>- 100M full duplex - 100M full duplex</li> <li>- 100M half duplex - 100M full duplex</li> <li>- 10M full duplex - 10M full duplex</li> <li>- 10M half duplex - 10M half duplex</li> </ul>
	STP settings	<p>The communication will be disabled for about 30 seconds after the activation of the interface of GLS and the switch when STP (spanning tree protocol) becomes valid. During this period, the GLS suppresses the switch of NIC due to the failure of the HUB monitoring. Set the controlled time by the hanetpoll command as the parameter "Time of delay for Linking Up" (60 seconds in default). Incorrect switch of NIC may occur if this parameter value is small. Processing it in the following methods.</p> <p>1) Change the parameter settings to prevent incorrect switch.</p> <p>2) Invalidate STP of used HUB port in the network where the transmission of packet does not form loop.</p>
	VLAN-ID	Please confirm that the VLAN ID of ports which connects the primary NIC is same as the one connects the secondary NIC when using the HUB that supports port VLAN. When the VLAN IDs are different, the monitoring frame cannot reach to the active NIC from the standby NIC.
Status of the own node and the network	Maintenance work	Please confirm neither the reactivation of the monitored targets HUB nor the maintenance work of the exchange, etc. are done during the period of detecting anomalies by the standby patrol. When changing the HUB, it is necessary to stop the standby patrol.
	HUB status	When the HUB is in trouble, the monitoring frame will be lost intermittently. Please confirm the abnormal messages are not output to the logs of HUB.
	System log	1) The NIC that monitors the standby patrol might have been linked down. Please confirm whether the link down messages have been output to the system log during

Confirmation item		Contents
		the period of detecting anomalies. 2) Hardware (NIC or PCI bus and CPU or memory etc.) may have faults. The messages that indicate hardware faults might be output, please confirm the system log.
	Communication load	The delay and the lost of the monitoring frame might occur when traffic on the network increases and the network is in state of a high load. Please confirm whether there are conflicts and packet loss from statistical information and logs of HUB. Please confirm the amount of received and sent packets during the period of switch by the sar command in Linux. In addition, in the environment where the network with a different speed (1Gbps and 100Mbps, etc.) exists, even if the unoccupied bandwidth exists in a high-speed network, packets may still be lost when they are transported from the HUB to a low-speed network. Please confirm whether the traffic has been estimated correctly.

### F.3.3 Switching takes place in NIC switching mode regardless of failure at the monitoring end

#### Symptom:

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.
(eth0,target=192.13.71.20)
hanet: ERROR: 87100: polling status changed: Secondary polling failed.
(eth1,target=192.13.71.21)
```

#### Corrective action:

In NIC switching mode, occasionally it takes time to establish a data link at Ethernet level following activation of an interface. Even though activated an interface, it is not possible to communicate immediately. Generally it becomes possible to communicate in dozens of seconds after activated, but some HUBs to connect take more than one minute, and occasionally HUB monitoring fails and switching occurs. In such a case, extend the time to wait for linking up (default value: 60 seconds) by a hanetpoll on command. Also when HUB to use is set to use STP (Spanning Tree Protocol), occasionally takes long time to become possible to communicate. Extend the time to wait for linking up if necessary. 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 your using.

$$\text{link up latency} > \text{STP transfer delay time} * 2 + \text{monitoring period} * \text{number of monitoring}$$


#### Note

To operate HUB monitoring over the system that runs firewall, configure the firewall so that ping can pass through the firewall. Otherwise, it fails to operate HUB monitoring.

### F.3.4 Takes time to execute an operation command or to activate a cluster service

#### Symptom:

Takes time to execute an operation command of a Redundant Line Control Function.  
Takes time to activate a service or to switch nodes at the cluster operation.

### Corrective action:

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/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/hosts, and that /etc/hosts is referred first at name-address conversion. Also, enable the hostname resolution function (set by hanetparam -h), which allows you to change the host name to the IP address using only the /etc/hosts file without depending on the /etc/nsswitch.conf file setting.

## F.3.5 Unable to communicate using virtual IP addresses after configuring a firewall

### Symptom:

Unable to communicate between GLS and the communication target using virtual IP addresses after configuring a firewall between the communication target and the local system to allow only virtual IP addresses to go through the firewall, by using the logical IP address takeover function in NIC switching mode.

### Corrective action:

When using the logical IP address takeover function in NIC switching mode, set the firewall to enable communications with the physical IP address (which is set by the -e option of the hanetconfig command), or use the physical IP takeover function rather than the logical IP address takeover function.

Virtual IP addresses of the logical IP address takeover function are created as the IP addresses assigned to the logical interfaces (ethX:Y). When you communicate using the logical interfaces and when the remote host is the transmitting side, the packet's destination will be virtual IP addresses and the packet's source will be the IP address of the remote host. When the local host (virtual IP address) is the transmitting side, the packet's destination will be the IP address of the remote host and the packet's source will be the physical IP address according to the routing table. Therefore, the firewall must be set so that the physical IP address can go through the firewall when you use the logical IP address takeover function.

Figure F.4 The remote host is the transmitting side.

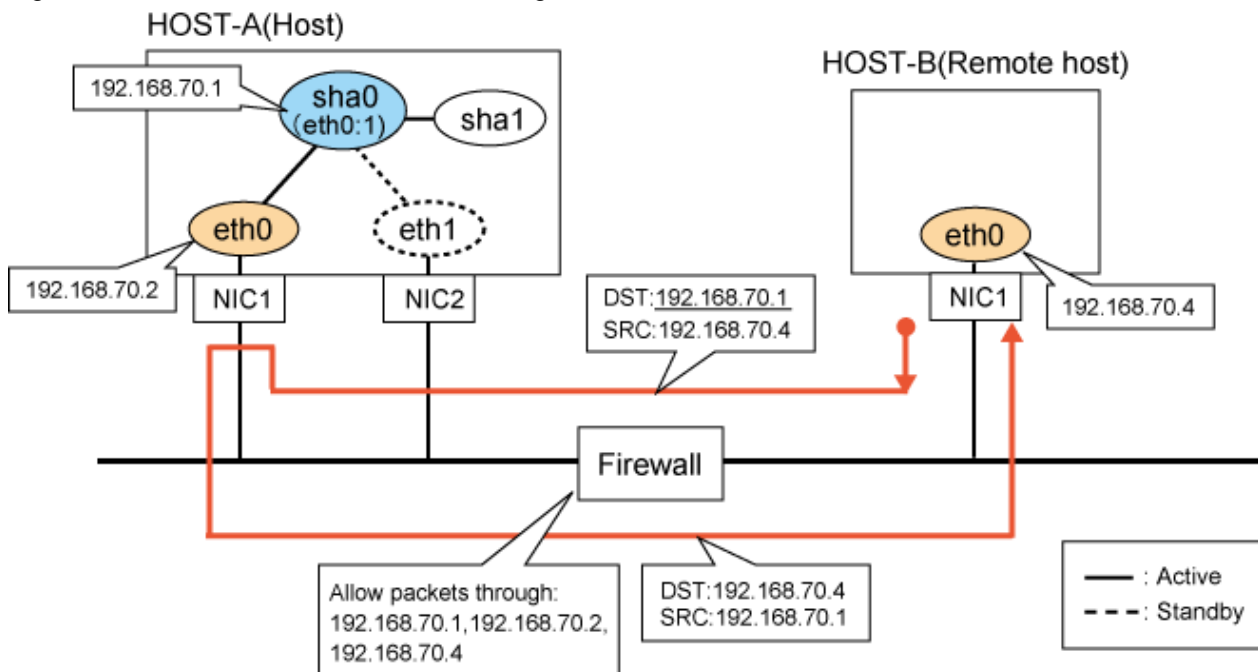
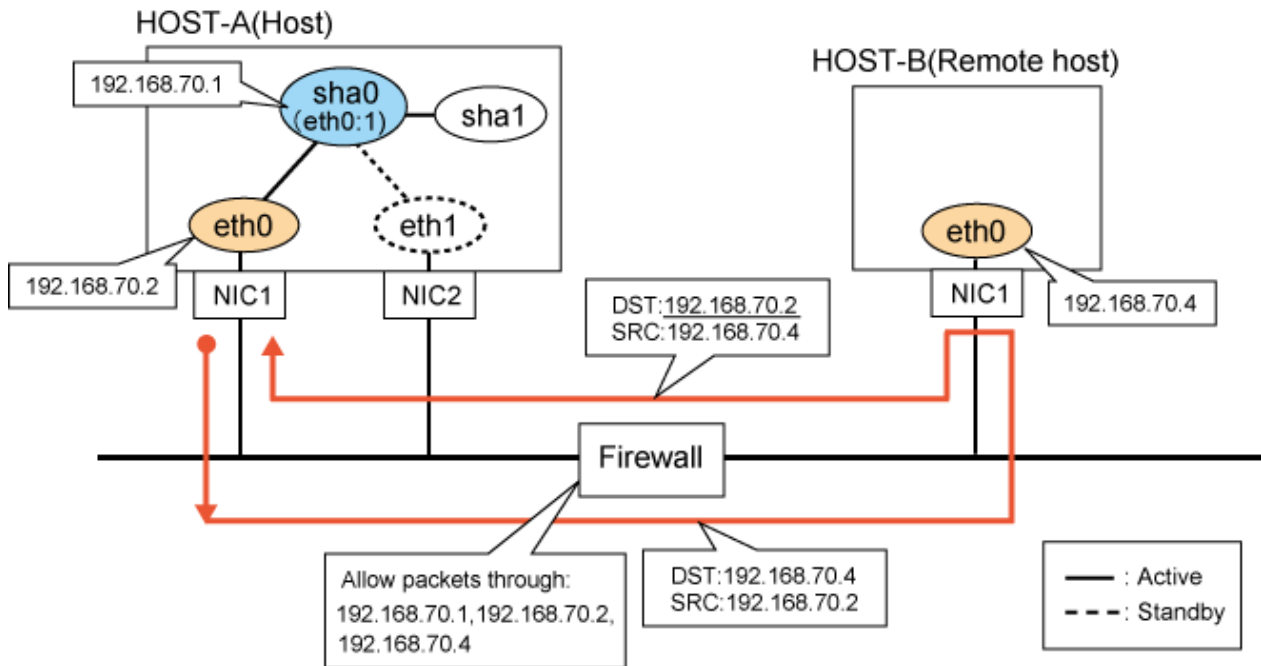


Figure F.5 The local host is the transmitting side.



### F.3.6 Virtual driver hang detected by Self-checking function

#### Symptom:

A virtual driver hang was detected by the Self-checking function.

#### Corrective action:

The Self-checking function starts a process for monitoring. If this process does not operate for 15 seconds or more due to burdens imposed on the process, the Self-checking function may detect a virtual driver hang mistakenly. If the status is correctly displayed with the dsphanet command after outputting a message that a virtual driver hang was detected, the driver is not hung up.

Extend the time to detect a virtual driver hang so that it may prevent the detection error. To extend the time for detecting a hang, perform the setting as follows:

1. Edit the setting file to set the time for detection.

```
/etc/opt/FJSVhanet/config/mond.conf
```

```
drv_resp 60    <- Set time for detecting a virtual driver hang in seconds
```

The setting file is not installed by default. Create a new one.

2. Restart the operating system.

```
# /sbin/shutdown -r now
```



#### Note

The setting file cannot be restored by backing up and restoring a configuration file. Set the file again depending on the environment.

## F.4 Failure occurs during operation (In the case of a Cluster system)

---

### F.4.1 Node switching is not executed in Fast switching mode

---

#### Symptom:

Failover between clusters (job switching between nodes) is not executed in Fast switching mode at cluster operation.

#### Corrective action:

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. If "Link detected: no" message pops up, check the status of the cable and HUB. Although, if the driver for NIC does not support ethtool command, you can not use this command. When the following message is often displayed, check the cables or HUBs.

```
# ethtool eth0
Settings for eth1:
    Supported ports: [ TP MII ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
    Advertised auto-negotiation: No
    Speed: 100Mb/s
    Duplex: Full
    Port: MII
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: off
    Supports Wake-on: g
    Wake-on: g
    Current message level: 0x00000007 (7)
    Link detected: yes
```

## F.5 Resuming connection lags after switching (Common to both Single and Cluster system)

---

### F.5.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode

---

#### Symptom:

When switching interface from operating 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.

#### Corrective action:

In the HUB where STP is running, establishing link by activating an interface does not necessarily 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.

## F.6 Incorrect operation by the user

---

### F.6.1 Accidentally deleted the virtual interface with ifconfig command

---

#### Symptom:

Unable recover the virtual interface (sha) deleted with ifconfig command by accident.

#### Corrective action:

There would be no guarantee on system behavior, if a virtual interface (sha) is disabled or deleted. In order to recover a virtual interface, follow the procedure below:

#### [Example 1]

Accidentally executing "ifconfig sha0 down" against a virtual interface sha0 for Fast switching mode.

```
If IPv4 address is being used:
# ifconfig sha0 IPv4 address netmask network mask broadcast broadcast
address arp up

If IPv6 address is being used:
# ifconfig sha0 up
# ifconfig sha0 add IPv6 address/prefi xlen
```



See

.....  
In the case of a cluster system, a virtual interface is restored automatically. In addition, please refer to "[2.7.1 Interface status monitoring feature](#)" automatically about the virtual interface which can be restored.  
.....

# Appendix G Check list

This appendix describes items to be checked before operating GLS. Using this checklist before operation can reduce the risk of incorrect settings.

## G.1 Checkpoint list

Table G.1 Common to all modes

NO	Checkpoint	Description	Check field
1	<a href="#">Network configuration</a>	Check that multiple, non-redundant NICs are not are not connected to the same network.	OK/NG
2	<a href="#">VLAN</a>	Check that the port VLAN and tagged VLAN are connected correctly to network devices.	OK/NG
3	<a href="#">Redundant network configuration</a>	Check whether unnecessary network groups have been created.	OK/NG
4	<a href="#">Firewall settings</a>	If there is a firewall, check whether the filtering has been set correctly.	OK/NG
5	<a href="#">IP address settings</a>	Check that IP addresses are not duplicated on each node. In a cluster configuration, check that the same takeover virtual IP addresses are set on each node.	OK/NG
6	<a href="#">Subnet mask settings</a>	Check that the subnet mask has been set using the "hanetmask" command for the IP address used by GLS.	OK/NG
7	<a href="#">Hotplug settings</a>	Check that the NICs used by GLS have been set to disable the operating system's hotplug function.	OK/NG
8	<a href="#">Hostname settings</a>	If GLS is set using the hostname rather than an IP address, enable the "hostname translation function".	OK/NG
9	<a href="#">Distribution procedure after settings change</a>	If you have changed the GLS settings, you need to distribute the reboot and other settings for operations. Check that the distribution procedure has been performed.	OK/NG
10	<a href="#">Procedure for network device maintenance</a>	If you stop the ping monitoring destination network device for maintenance, GLS may detect a network failure. Also, if a cluster configuration is in use, node failures may occur. When you perform network device maintenance, be sure to check with other persons in charge when you temporarily stop monitoring.	OK/NG
11	<a href="#">Network device rate settings</a>	Check that the rate settings for network devices or server's NICs have been set correctly. If you set auto negotiation and fixed full duplex, any half-duplex and full-duplex communications are mixed, resulting in an unstable communication state.	OK/NG
12	<a href="#">Application</a>	Check that the application to be used is the TCP/IP application using TCP and UDP.	OK/NG

Table G.2 Fast switching mode

NO	Checkpoint	Description	Check field
1	<a href="#">Network address</a>	Check that the network address has been set correctly. The virtual IP addresses of the local system and the target should be the same network addresses.	OK/NG
2	<a href="#">Node configuration</a>	In a cluster configuration, three or more nodes using Fast switching mode are required.	OK/NG

Table G.3 NIC switching mode

NO	Checkpoint	Description	Check field
1	<a href="#">Monitoring destination selection</a>	Check whether the monitoring destination in NIC switching mode is correct. Frequently rebooted servers are not suitable for monitoring destinations.	OK/NG

NO	Checkpoint	Description	Check field
2	<a href="#">Monitoring time adjustment</a>	If you want to shorten the monitoring time, check that the settings have been made with consideration to the state of applications and monitoring destinations.	OK/NG
3	<a href="#">Network cable</a>	Check that the cables of the primary monitoring destination and secondary monitoring destination are connected to the right switch as monitoring destinations in NIC switching mode.	OK/NG
4	<a href="#">Static route settings</a>	When you set the static route for the NIC switching mode, check that the settings have been made so that the static route is set for both of the interfaces bound by the virtual interface.	OK/NG

Table G.4 Virtual NIC mode

NO	Checkpoint	Description	Check field
1	<a href="#">Interface setting file</a>	Check that the IP addresses or subnet masks are defined in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) for the virtual interface.	OK/NG
2	<a href="#">Monitoring destination selection</a>	Check whether the monitoring destination in Virtual NIC mode is correct. Frequently rebooted servers are not suitable for monitoring destinations.	OK/NG
3	<a href="#">Monitoring time adjustment</a>	If you want to shorten the monitoring time, check that the settings have been made with consideration to the state of applications and monitoring destinations.	OK/NG
4	<a href="#">Network cable</a>	Check that the cables of the primary monitoring destination and secondary monitoring destination are connected to the right switch as monitoring destinations in Virtual NIC mode.	OK/NG

Table G.5 GS linkage mode

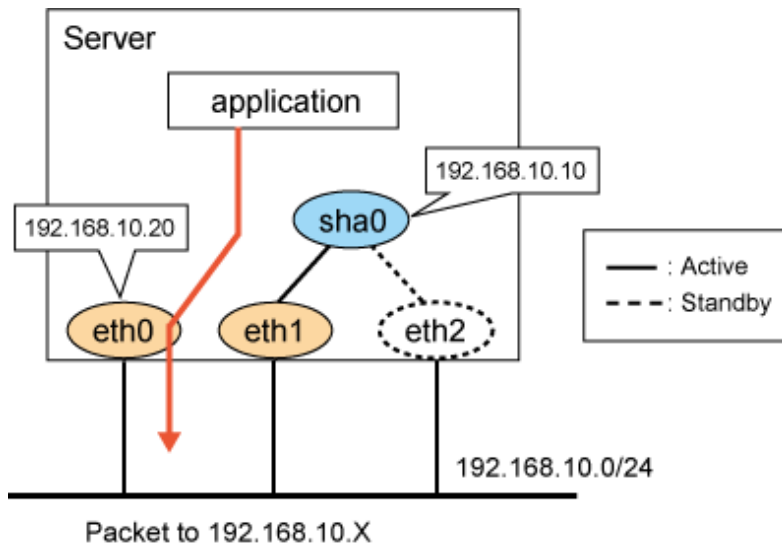
NO	Checkpoint	Description	Check field
1	<a href="#">Network address</a>	Check that the network address has been set correctly. The virtual IP addresses of the local system and the communication target should be different network addresses.	OK/NG
2	<a href="#">Communication target setting</a>	Check that the "hanetobserv" command has been set correctly.	OK/NG
3	<a href="#">Network device settings</a>	When you connect to GS through from GLS via router or LANC2, you need to set the gateway for the virtual IP address of GLS. Also, check that whether the settings have been made so that the device connected to the server used by GLS sends RIPv1.	OK/NG
4	<a href="#">Monitoring time adjustment</a>	If you are monitoring communications for virtual IP addresses with high level applications, adjust the monitoring time so that an error is not detected in less time than GLS needs to switch the network.	OK/NG
5	<a href="#">Maintenance procedure performed when the communication target stopped</a>	Check the maintenance procedure for shutting down the communication target completely when GLS is used in a cluster configuration. If you restart one cluster node, the other node determines that all networks have failed and a node failure occurs.	OK/NG
6	<a href="#">PTF of the communication target</a>	Check that the PTF needed to connect to GLS has been applied to the GS of the communication target.	OK/NG

## G.2 Setup common to modes

### G.2.1 Network configuration

Check that multiple, non-redundant NICs are not connected to the same network. The following configuration example shows that two activated NICs are connected to the same network. In this case, OS routing tables overlap, so communications may not be performed correctly. To avoid this, connect to a different network.





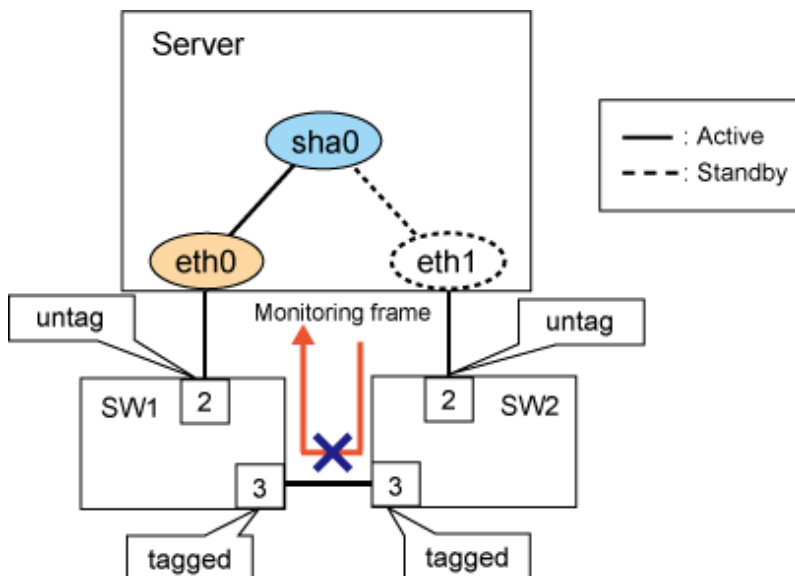
### Confirmation method

Use the "netstat -nr" command to check that the same network address is not set for a different device. In the following execution example, different devices have been set to the same network. Therefore, you need to change the network address of the either of the two.

```
# netstat -nr
Kernel IP routing table
Destination      Gateway         Genmask         Flags        MSS Window  irtt  Iface
192.168.10.0     0.0.0.0         255.255.255.0   U            0 0        0     eth0
192.168.10.0     0.0.0.0         255.255.255.0   U            0 0        0     eth1
```

## G.2.2 VLAN Setup

Check that the port VLAN and tagged VLAN have been connected correctly to network devices. In the following example, the tagged VLAN setting of the switch is incorrect. Therefore, monitoring frames are not communicated and an error is detected by the standby patrol (message number 875 appears).



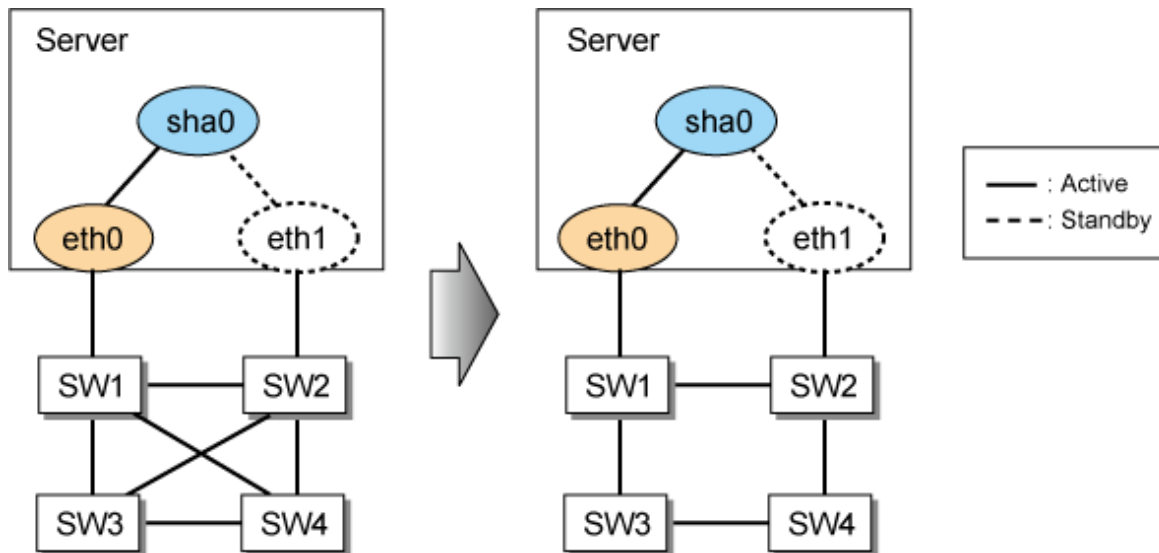
### Confirmation method

Check the VLAN settings of network devices

## G.2.3 Redundant network configuration

Check that unnecessary network groups are not created. If you create a network loop to create a highly reliable network, STP normally releases the loop and communications can be performed. However, the more complex the loop becomes, the harder the investigation is in the event of a network device failure. Also, in the event of a network device failure, STP does not work and the network loop will be created and the likelihood that the network goes down increase. Take care to design the network so that a network loop is not created. Additionally, consider using switches with storm control in case of a failure.

In the following configuration, you do not need to cross connect SW1 with SW4, and SW2 with SW3. Also, if you do not use STP, you do not need to cross connect SW1 with SW2, and SW2 with SW3.

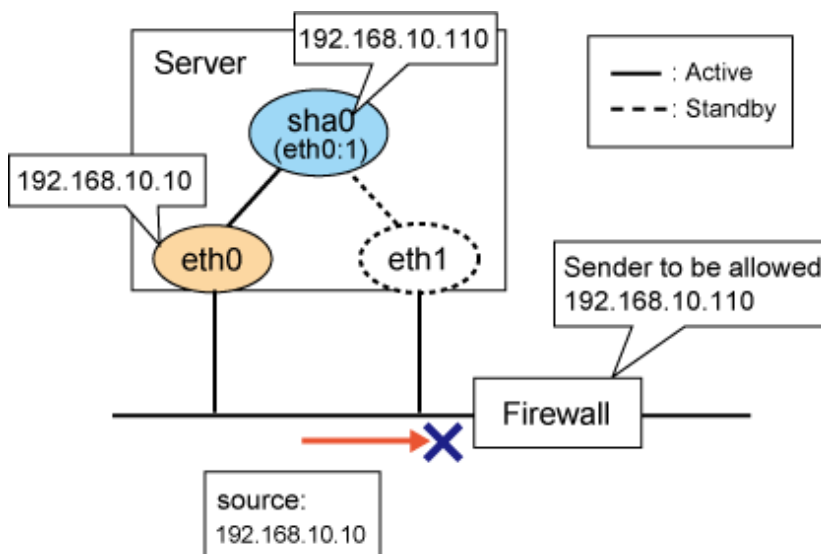


### Confirmation method

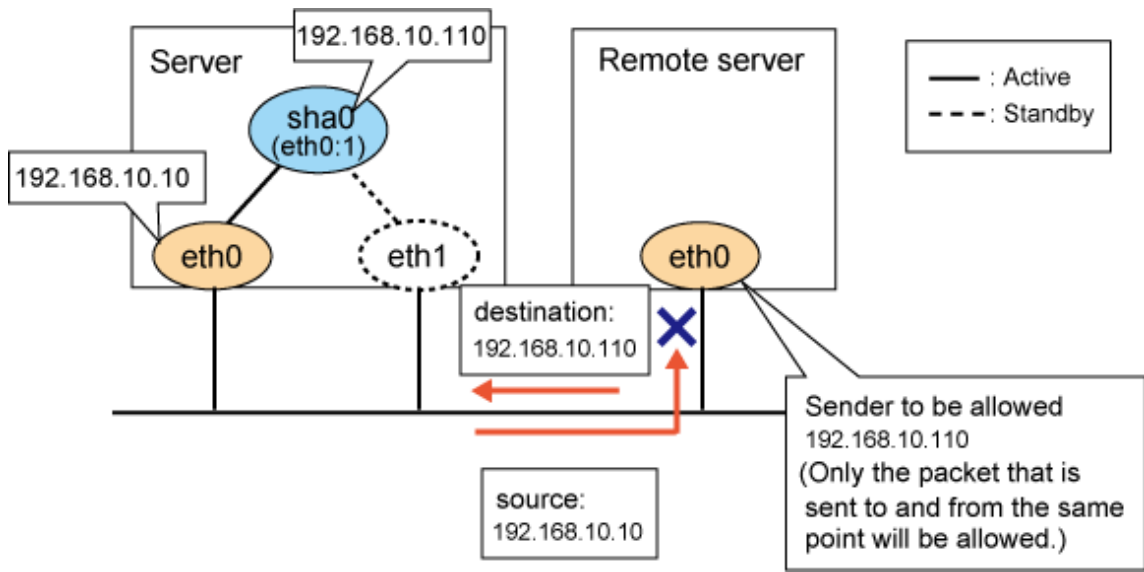
Check the connection of the network configuration diagram.

## G.2.4 Firewall settings

If there is a firewall, check that the filtering has been set correctly. If the server is the sender in the environment where multiple IP addresses are assigned to one NIC, the packet sender will be an IP address assigned to the physical interface. Therefore, if you use a virtual IP address to communicate through the firewall, set the filter so that the physical IP address can also go through the firewall. For details, see ["F.3.5 Unable to communicate using virtual IP addresses after configuring a firewall"](#).



Similarly, if you have created the settings so that the communication target does not allow a physical IP address using the filtering function, change the settings so that the physical IP address is allowed.



### Confirmation method

Check the filtering settings for the firewall and the communication target.

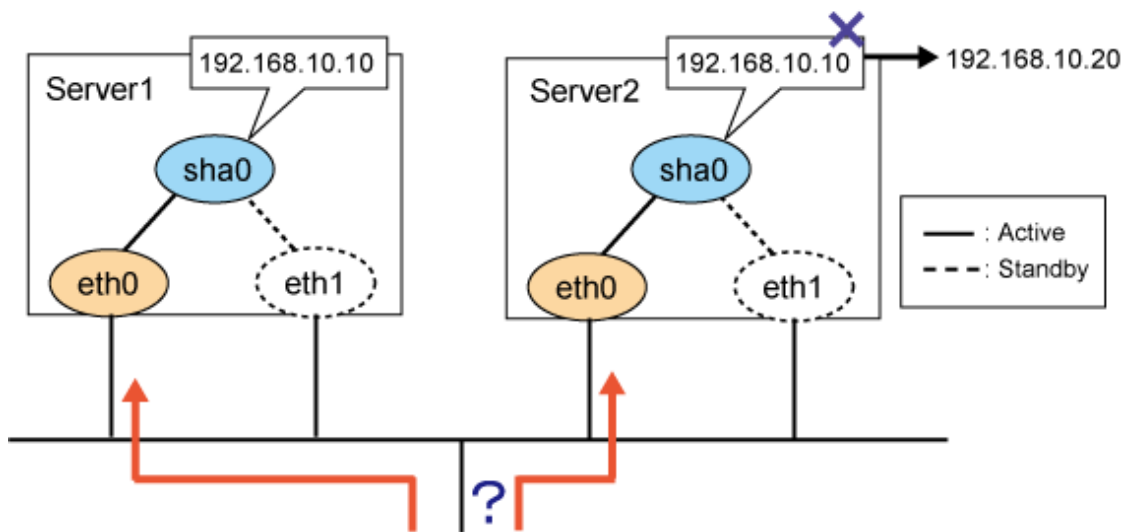


See  
 .....  
 "F.3.5 Unable to communicate using virtual IP addresses after configuring a firewall"  
 .....

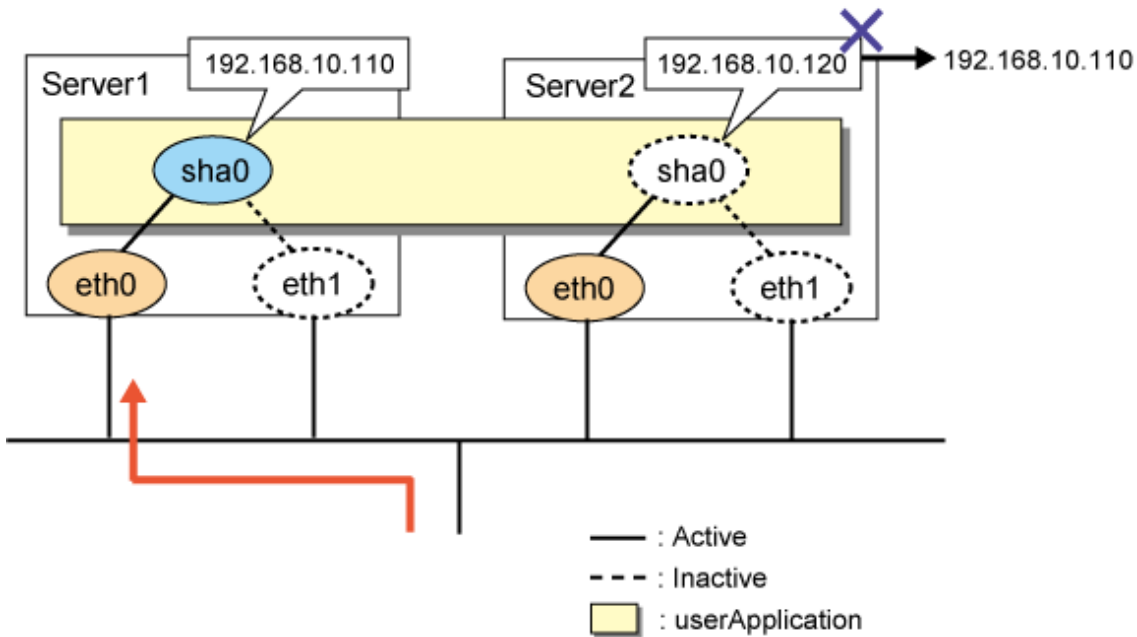
## G.2.5 IP address settings

Check whether IP addresses are duplicated on each node. In a cluster configuration, check that the same takeover virtual IP address is set for each node.

If an IP address is duplicated, ARP resolution cannot be performed correctly. Therefore, the communication target cannot send packets to the correct server.



Also, if the same takeover virtual IP address is not set in the cluster configuration settings, GLS resource process will fail. Check that the same takeover virtual IP address is set by hanethvrsc command.



### Confirmation method

Execute "hanethvrsc print" on each node that makes up the cluster to check that the takeover IP addresses are the same.

```
Server1
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4    takeover-ipv6    logical ip address list
+-----+-----+-----+-----+
sha0:65      192.168.10.110    -                -

Server2
# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4    takeover-ipv6    logical ip address list
+-----+-----+-----+-----+
sha0:65      192.168.10.110    -                -
```

## G.2.6 Subnet mask settings

Execute the "hanetmask" command for the IP address used by GLS to check that the subnet mask has been set.

### Confirmation method

Check that the subnet mask for the IP address that is displayed with the "hanetconfig print" command and "hanethvrsc print" command has been set correctly. Otherwise, the net mask that matches the class of each IP address will be set. For example, 255.0.0.0 is assigned to a Class A IP address.

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

Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.10.10  t      192.168.10.10        eth1,eth2
sha1      192.168.11.10  d      192.168.11.10        eth3,eth4
sha2      192.168.100.10 c      192.168.100.10       eth5,eth6

# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname      takeover-ipv4    takeover-ipv6    logical ip address list
+-----+-----+-----+-----+
sha0:65      192.168.10.110    -                -
```

```

sha0:65    192.168.10.110    -            -
sha1:65    192.168.11.10     -            -
sha2:65    192.168.100.10    -            192.168.12.1,192.168.14.1

# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
+-----+-----+
192.168.10.0    255.255.255.0
192.168.11.0    255.255.255.0
192.168.100.0   255.255.255.0
192.168.12.0    255.255.255.0
192.168.14.0    255.255.255.0

```



See

"7.5 hanetmask Command"

## G.2.7 Hotplug settings

Check that the NICs used by GLS have been set to disable the operating system's hotplug function. The hotplug function is a Linux function that automates the assignment of IP addresses when interfaces are created. When GLS is used, GLS itself manages IP addresses. Therefore, you need to disable this function. Also, if you do not make this setting, the activation and deactivation of interfaces by GLS may fail. For details, see "3.2.2.1 Setup common to modes". Note that, for RHEL5, you need to add settings in the /etc/udev/rules.d/60-net.rules file as well as in ifcfg-ethX.

### Confirmation method

- In RHEL5 and RHEL6, check that the HOTPLUG=no setting has been made for /etc/sysconfig/network-scripts/ifcfg-ethX.

```

# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=10.33.88.170
NETMASK=255.255.255.0
HWADDR=XX:XX:XX:XX:XX:XX
HOTPLUG=no

```

- In RHEL5, in addition to the setting of HOTPLUG=no, check that the hotplug function is set to be disabled for the device name "sha" in /etc/udev/rules.d/60-net.rules.

```

# cat /etc/udev/rules.d/60-net.rules
SUBSYSTEM=="net", ENV{INTERFACE}=="sha*", GOTO="skipgls"
ACTION=="add", SUBSYSTEM=="net", IMPORT{program}="/lib/udev/rename_device"
SUBSYSTEM=="net", RUN+="/etc/sysconfig/network-scripts/net.hotplug"
LABEL="skipgls"

```



See

"3.2.2.1 Setup common to modes"

## G.2.8 Hostname settings

If GLS is set using the hostname rather than an IP address, enable the "hostname translation function". If this function is enabled, even if you make the settings so that the hostname is changed using DNS on the system, you can change IP addresses by using a file (/etc/hosts) as GLS.

### Confirmation method

- Check the IP address settings of GLS. If the hostname has been set, check that the value for "Hostname resolution by file(h)" of the "hanetparam print" command is YES

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
[Fast switching]
  Line monitor interval(w)           :5
  Line monitor message output (m)    :0
  Cluster failover (l)               :5
  Cluster failover in unnormality (c):OFF
  Line status message output (s)     :OFF

[NIC switching]
  Standby patrol interval(p)         :15
  Standby patrol message output(o)   :3

[Virtual NIC]
  LinkDown detection time (q)        :0
  LinkUp detection time (r)          :1
  Link monitor starting delay (g)    :5

[Common Setting]
  Hostname resolution by file(h)      :YES
  Self-checking function(e)          :NO
```

## G.2.9 Distribution procedure after settings change

---

If you have changed the GLS settings, you need to distribute the reboot and other settings for operations. Check that the distribution procedure has been performed. For details, see "[3.4 Changing system setup](#)"

### Confirmation method

Check the procedure manual for settings changes.



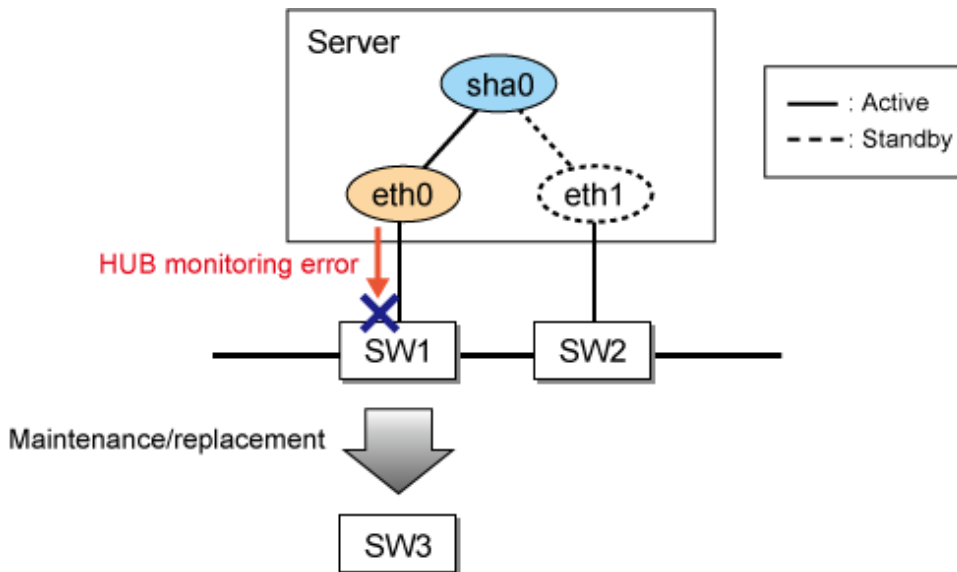
See

.....  
"3.4 Changing system setup"  
.....

## G.2.10 Procedure for network device maintenance

---

If you stop the ping monitoring destination network device for maintenance, GLS may detect a network failure. Also, if a cluster configuration is in use, node failures may occur. When you perform network device maintenance, be sure to notify other persons in charge that you are going temporarily stop monitoring.



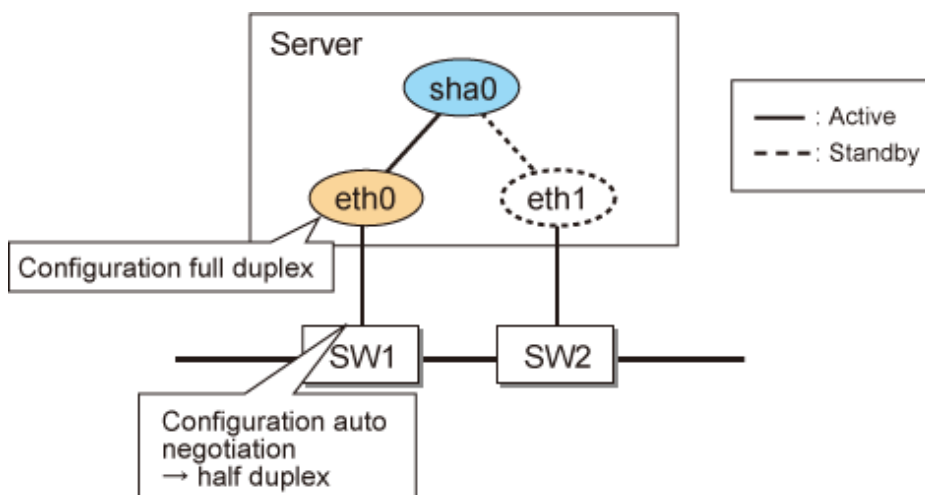
### Confirmation method

In a cluster configuration environment, if you want to stop all monitoring destinations for network device maintenance, check the maintenance procedure manual to see that the "hanetpoll off" command for temporarily stopping monitoring is set to be executed. Also, check that the "hanetpoll on" command is used to restart the monitoring after change.

```
Before the network device is changed
# /opt/FJSVhanet/usr/sbin/hanetpoll off
After the network device has been changed
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

## G.2.11 Network device rate settings

Check that the rate settings for network devices or server's NICs have been set correctly. If you set auto negotiation and fixed full duplex, any auto negotiation recognized as half-duplex will result in an unstable communication state.



### Confirmation method

Check the switch state. For a server, use the following command to check its state. Also, check the rate settings between switches not only between the server and switches.

```
# ethtool eth0
Settings for eth0:
    Supported ports: [ FIBRE ]
    Supported link modes:   1000baseT/Half 1000baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes:  1000baseT/Half 1000baseT/Full
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full

snip..

    Link detected: yes
```

## G.2.12 Application

---

Check that the application to be used is a TCP/IP application supporting TCP and UDP. Note that multicast applications cannot be used in Fast switching mode and NIC switching mode.

### Confirmation method

Check the communication method for the application to be used.



See

- "2.1.1.4 Available application"
- "2.1.1.5 Notes"
- "2.1.2.4 Available application"
- "2.1.2.5 Notes"
- "2.1.4.4 Available applications"
- "2.1.4.5 Notes"

## G.3 Fast switching mode

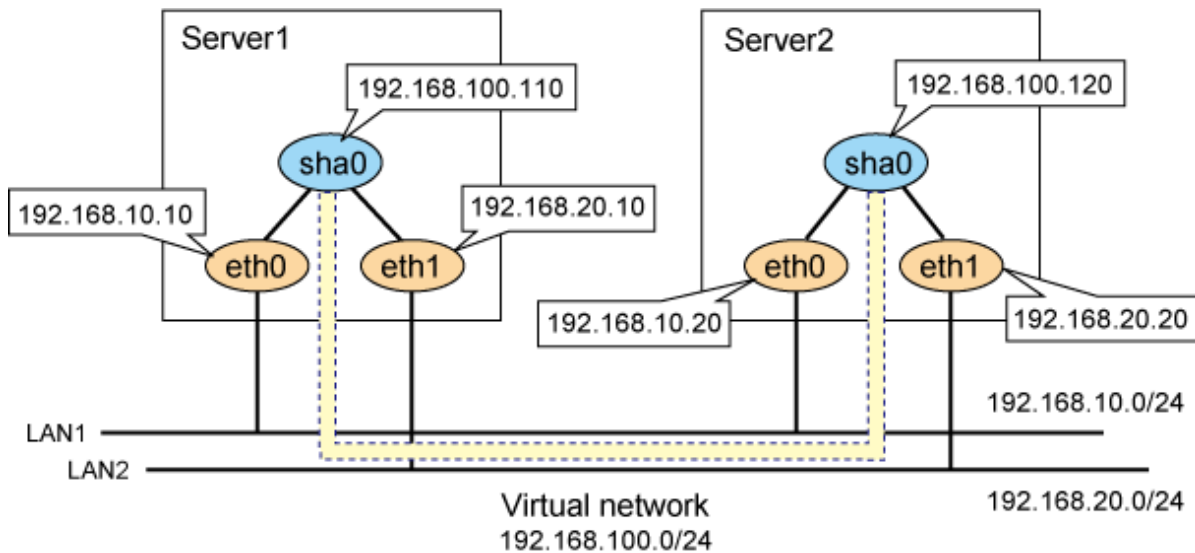
---

### G.3.1 Network address

---

Check that the network address has been set correctly. The virtual IP addresses of the local system and the communication target should be the same network addresses. Also, different network addresses should be used for each of the physical interfaces bound by virtual interfaces.





### Confirmation method

Use the "netstat -nr" command to check that the network address has been assigned correctly.

```
# netstat -nr
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	MSS Window	irrt	Iface
<u>192.168.10.0</u>	0.0.0.0	255.255.255.0	U	0 0	0	<u>eth0</u>
<u>192.168.20.0</u>	0.0.0.0	255.255.255.0	U	0 0	0	<u>eth1</u>
<u>192.168.100.0</u>	0.0.0.0	255.255.255.0	U	0 0	0	<u>sha0</u>

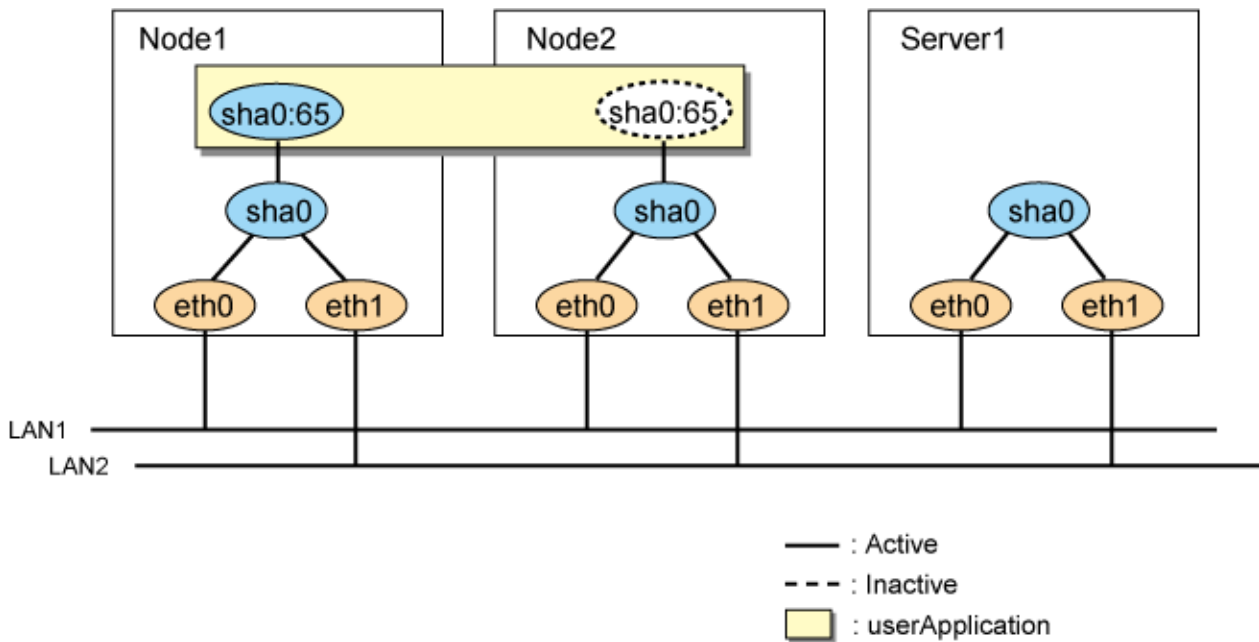


See

"2.1.1 Fast switching mode"

### G.3.2 Node configuration

In a cluster configuration, three or more nodes using Fast switching mode are required. In the following configuration, if there is no server1, node2 will determine that all of the monitoring targets have failed and bring the GLS resources to a failure state if node1 has stopped abnormally.



### Confirmation method

Check the network configuration diagram.



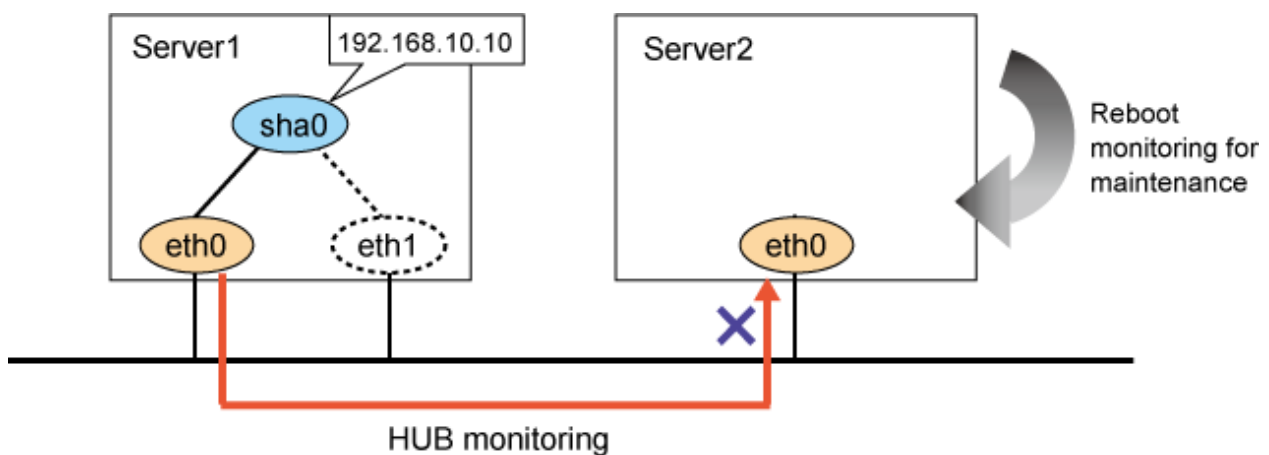
See

"5.1 Outline of Cluster System Support"

## G.4 NIC switching mode

### G.4.1 Monitoring destination selection

Check whether the monitoring destination in NIC switching mode is correct. Frequently rebooted servers are not suitable as monitoring destinations. Set the HUB or redundant router as a monitoring destination.



### Confirmation method

Use the "hanetpoll print" command to check the monitoring destination before checking the network configuration diagram.

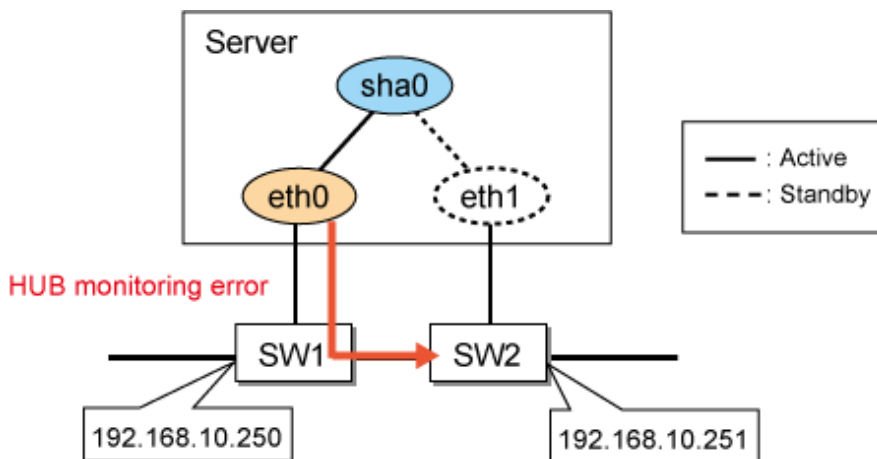
## G.4.2 Monitoring time adjustment

If you want to shorten the HUB monitoring time, change the settings with consideration to the state of the application to be used and the monitoring destination. For example, if you want to set the virtual IP address of a router as a monitoring destination, adjust the monitoring time so that GLS does not detect an error of a monitoring target during the time it takes for the virtual IP to be taken over to another router in the event of a router failure.

## G.4.3 Network cable

Check that the cables of the primary monitoring destination and secondary monitoring destination are connected to the right switch as monitoring destinations in NIC switching mode.

In the following example, the IP address of the monitoring destination HUB is set incorrectly, and therefore the correct monitoring cannot be performed. This may cause unintended NIC switching at the time of the network failure.



### Confirmation method

Use the "hanetpoll print" command to check the monitoring destination before checking the network configuration diagram. In the following example, check that the IP address 192.168.10.250 is assigned to the network device to which the primary interface eth0 of the Interface List is connected.

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

Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.10.110  d   192.168.10.10  eth0,eth1

# /opt/FJSVhanet/usr/sbin/hanetpoll print
snip..
Name      HUB Poll Hostname
+-----+-----+-----+
sha0      OFF    192.168.10.250,192.168.10.251
```

## G.4.4 Static route settings

When you set the static route for the NIC switching mode, check that the settings have been made so that the static route is set for both of the interfaces bound by the virtual interface.

If not, you will not be able to communicate with the network that has been set as a static route when a NIC is switched by GLS.

## Confirmation method

Check /etc/sysconfig/network-scripts/route-ethX to verify that the static route has been set for both of the physical interfaces bound by NIC switching mode. Check that the network address of GATEWAY to be set for route-ethX matches the address of the NIC bound by GLS.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
snip..
Name           Hostname           Mode Physical ipaddr   Interface List
+-----+-----+-----+-----+-----+
sha0           192.168.10.110     d    192.168.10.10   eth0,eth1

# cat /etc/sysconfig/network-scripts/route-eth0
GATEWAY0=192.168.10.254
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0

# cat /etc/sysconfig/network-scripts/route-eth1
GATEWAY0=192.168.10.254
NETMASK0=255.255.255.0
ADDRESS0=192.168.100.0
```



See

"3.2.2.1 Setup common to modes"

## G.5 Virtual NIC mode

---

### G.5.1 Interface setting file

---

Virtual interfaces in Virtual NIC mode are activated or deactivated in conjunction with the network service of the operating system in the same manner as normal physical NICs. Therefore, you need to define settings for IP addresses or subnet masks in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX).

#### Confirmation method

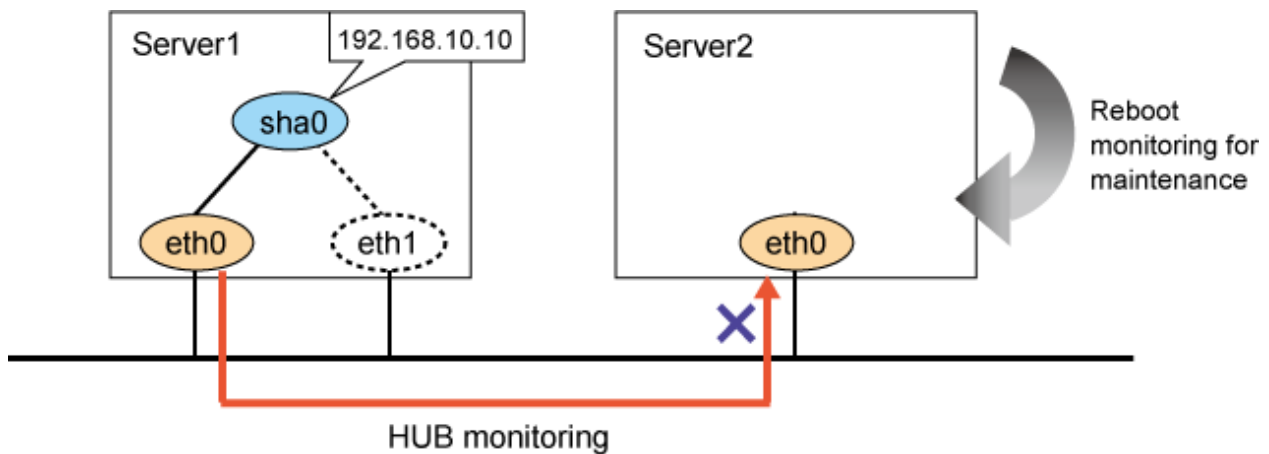
- Check that the IP addresses or subnet masks are defined in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) for the virtual interface.

```
# cat /etc/sysconfig/network-scripts/ifcfg-sha0
DEVICE=sha0
IPADDR=192.168.1.1
NETMASK=255.255.255.0
BOOTPROTO=static
ONBOOT=yes
DEVICETYPE=sha
HOTPLUG=no
```

### G.5.2 Monitoring destination selection

---

Check whether the monitoring destination in Virtual NIC mode is correct. Frequently rebooted servers are not suitable as monitoring destinations.



### Confirmation method

Use the "hanetpathmon target" command to check the monitoring destination before checking the network configuration diagram.

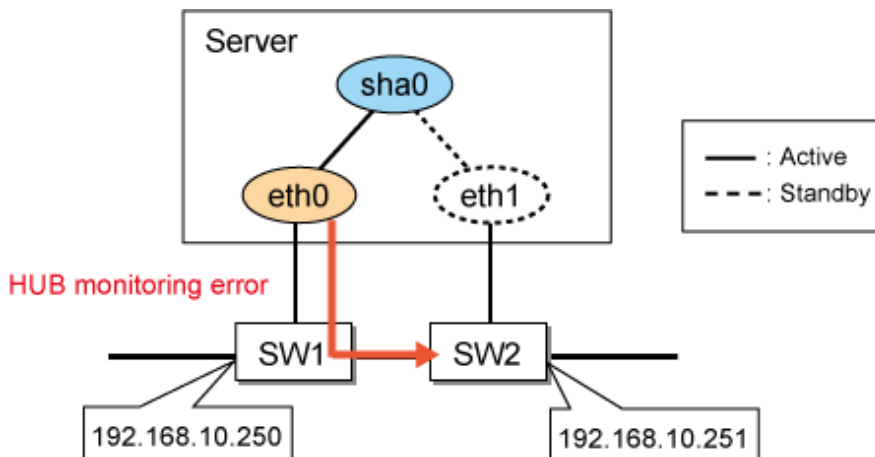
## G.5.3 Monitoring time adjustment

If you want to shorten the network monitoring time, change the settings with consideration to the state of the application to be used and the monitoring destination. For example, if you want to set the virtual IP address of a router as a monitoring destination, adjust the monitoring time so that GLS does not detect an error of a monitoring target during the time it takes for the virtual IP to be taken over to another router in the event of a router failure.

## G.5.4 Network cable

Check that the cables of the primary monitoring destination and secondary monitoring destination are connected to the right switch as monitoring destinations in Virtual NIC mode.

In the following example, the IP address of the monitoring destination HUB is set incorrectly, and therefore the correct monitoring cannot be performed. This may cause unintended NIC switching at the time of the network failure.



### Confirmation method

- Use the "hanetpathmon target" command to check the monitoring destination before checking the network configuration diagram. In the following example, check that the IP address 192.168.10.250 is assigned to the network device to which the primary interface eth0 of the Interface List is connected.

```
# hanetconfig print
[IPv4,Patrol / Virtual NIC]

Name      Hostname      Mode Physical ipaddr  Interface List
```

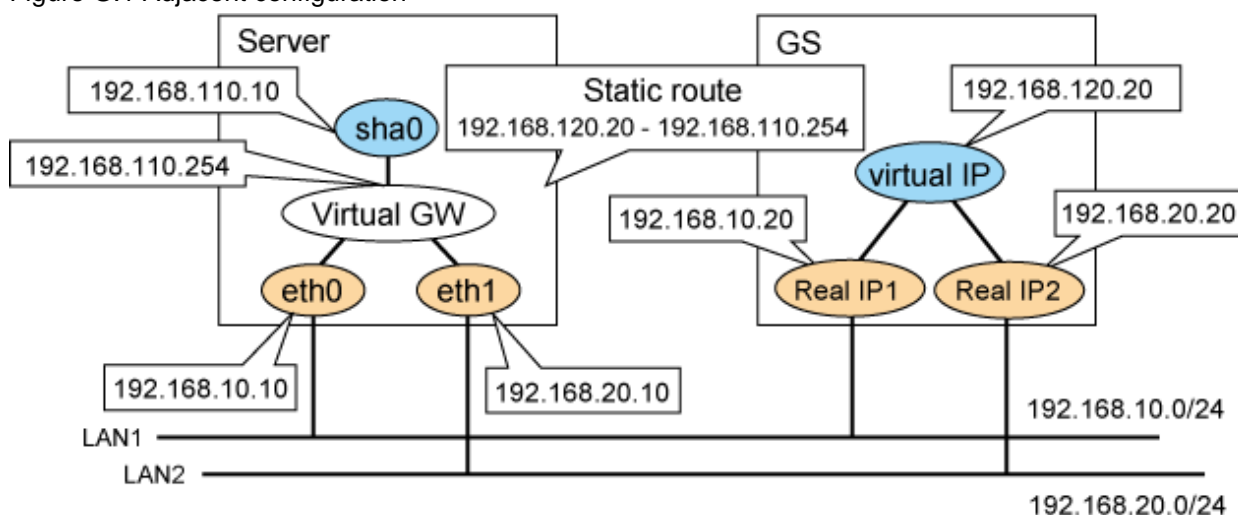
sha0	v	eth0,eth1
[IPv6]		
Name	Hostname/prefix	Mode Interface List
# hanetpathmon target		
[Target List]		
Name	VID	Target
sha0	-	192.168.10.250,192.168.10.251

## G.6 GS linkage mode

### G.6.1 Network address

Check that the network address has been set correctly. The virtual IP addresses of the local system and the communication target should be different network addresses.

Figure G.1 Adjacent configuration



### Confirmation method

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print
snip..
Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.110.10  c          eth0,eth1

# /opt/FJSVhanet/usr/sbin/hanetobserv print
snip..
Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+-----+
GS        192.168.120.20  192.168.10.20,192.168.20.20

# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
+-----+-----+
192.168.110.0   255.255.255.0

# /opt/FJSVhanet/usr/sbin/hanetgw print
```

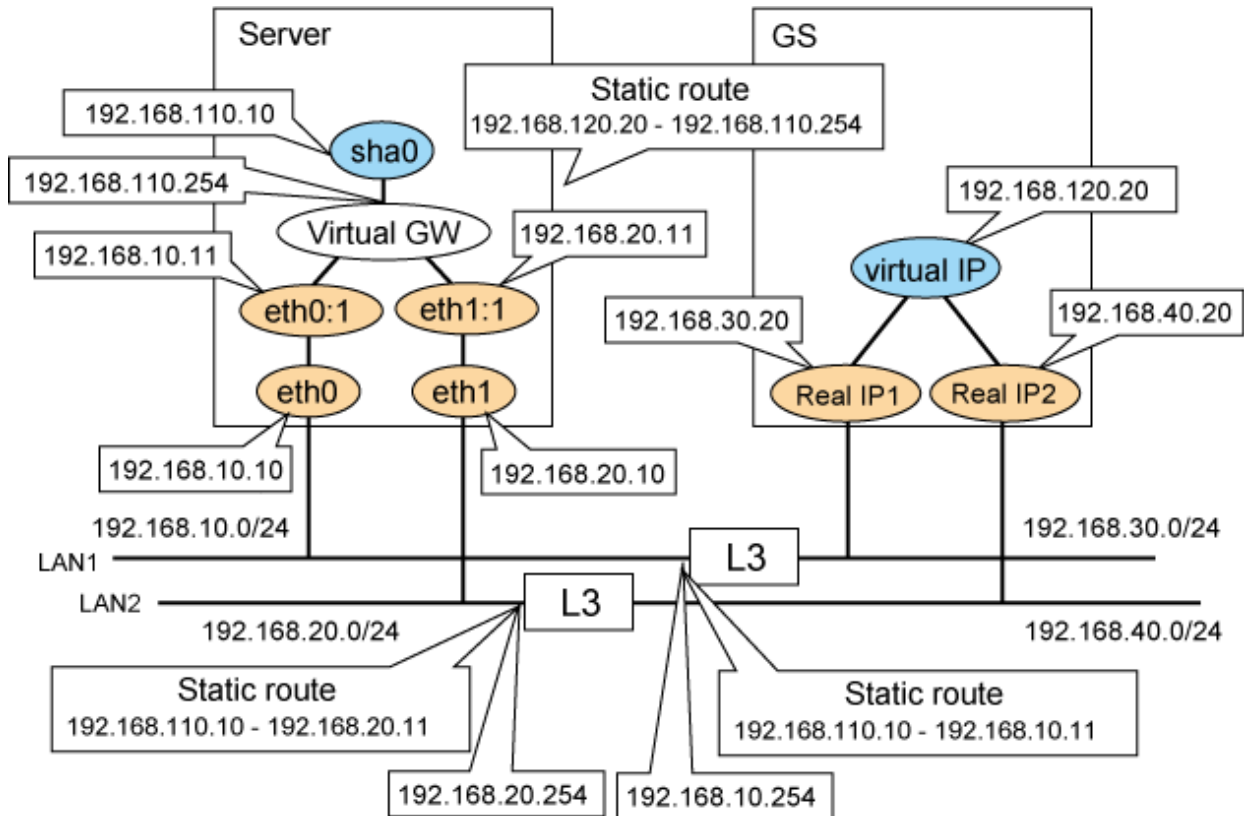
```

ifname  GW Address
+-----+-----+
sha0    192.168.110.254

# cat /etc/sysconfig/network-scripts/route-sha0
GATEWAY0=192.168.110.254
NETMASK0=255.255.255.255
ADDRESS0=192.168.120.20

```

Figure G.2 Remote configuration



### Confirmation method

```

# /opt/FJSVhanet/usr/sbin/hanetconfig print
snip..
Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.110.10  c               eth0,eth1

# /opt/FJSVhanet/usr/sbin/hanetobserv print
snip..
Destination Host Virtual Address  (Router Address+)NIC Address
+-----+-----+-----+-----+-----+
GS          192.168.120.20  192.168.30.20,192.168.40.20

# /opt/FJSVhanet/usr/sbin/hanethvrsc print
ifname    takeover-ipv4  takeover-ipv6    logical ip address list
+-----+-----+-----+-----+-----+
sha0:65   192.168.110.10  -                192.168.10.11,192.168.20.11

# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
+-----+-----+
192.168.110.0   255.255.255.0

```

```

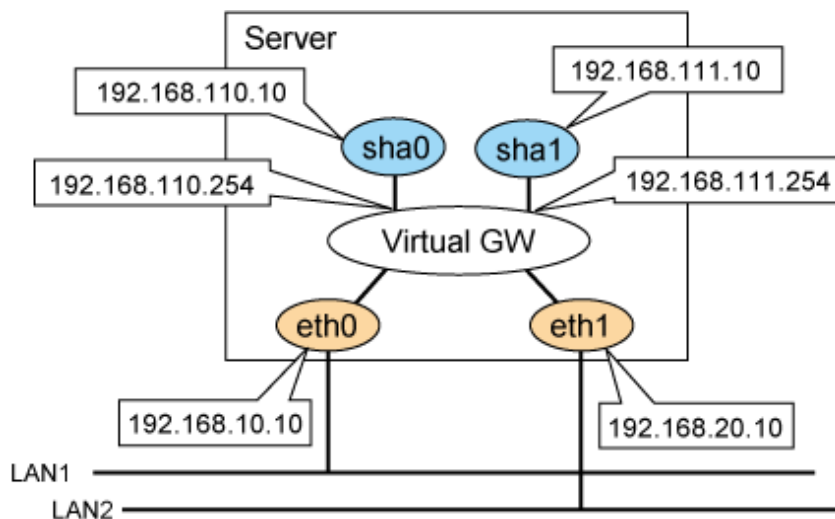
192.168.10.0    255.255.255.0
192.168.20.0    255.255.255.0

# /opt/FJSVhanet/usr/sbin/hanetgw print
ifname  GW Address
+-----+-----+
sha0    192.168.110.254

# cat /etc/sysconfig/network-scripts/route-sha0
GATEWAY0=192.168.110.254
NETMASK0=255.255.255.255
ADDRESS0=192.168.120.20
# cat /etc/sysconfig/network-scripts/route-eth0
GATEWAY0=192.168.10.254
NETMASK0=255.255.255.0
ADDRESS0=192.168.30.20
# cat /etc/sysconfig/network-scripts/route-eth1
GATEWAY0=192.168.20.254
NETMASK0=255.255.255.0
ADDRESS0=192.168.40.20

```

Note that if you want to use multiple virtual interfaces, you need to set different network addresses between virtual IP addresses.



## Confirmation method

```

# /opt/FJSVhanet/usr/sbin/hanetconfig print
snip..
Name      Hostname      Mode Physical ipaddr  Interface List
+-----+-----+-----+-----+-----+
sha0      192.168.110.10  c               eth0,eth1
sha1      192.168.111.10  c               eth0,eth1

# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
+-----+-----+
192.168.110.0    255.255.255.0
192.168.111.0    255.255.255.0

# /opt/FJSVhanet/usr/sbin/hanetgw print
ifname  GW Address
+-----+-----+
sha0    192.168.110.254
sha1    192.168.111.254

```





See

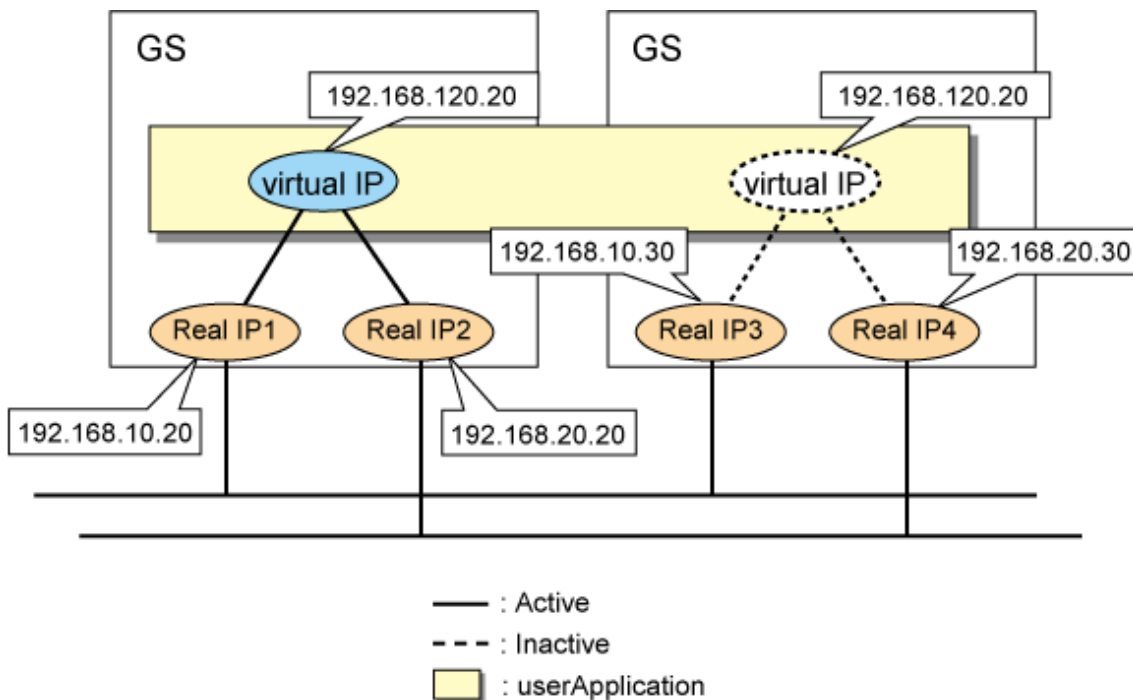
"2.2.2.3 Using GS linkage mode"

## G.6.2 Communication target setting

Check whether the "hanetobserv" command has been set correctly.

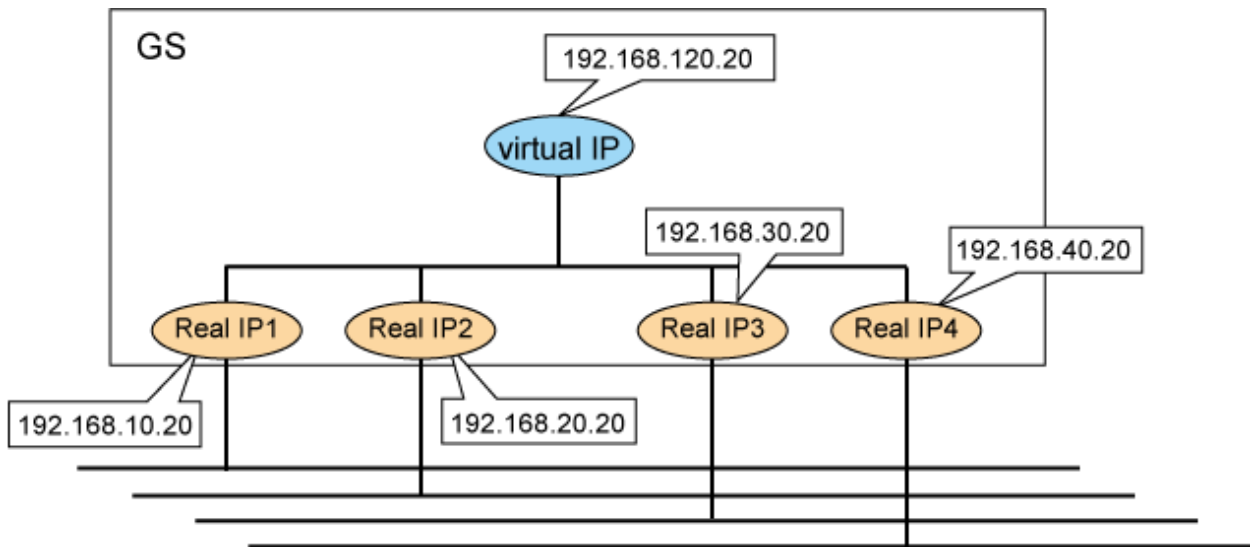
If GS's IP address moves between nodes as follows, execute the "hanetobserv create" command for each GS node.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.20,192.168.20.20
# /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      (Router Address+)NIC Address
+-----+-----+-----+-----+
GS          192.168.120.20      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.

```
# /opt/FJSVhanet/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
# /opt/FJSVhanet/usr/sbin/hanetobserv print
Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+-----+
GS          192.168.120.20      192.168.10.20,192.168.20.20,
                                     192.168.30.20,192.168.40.20
```

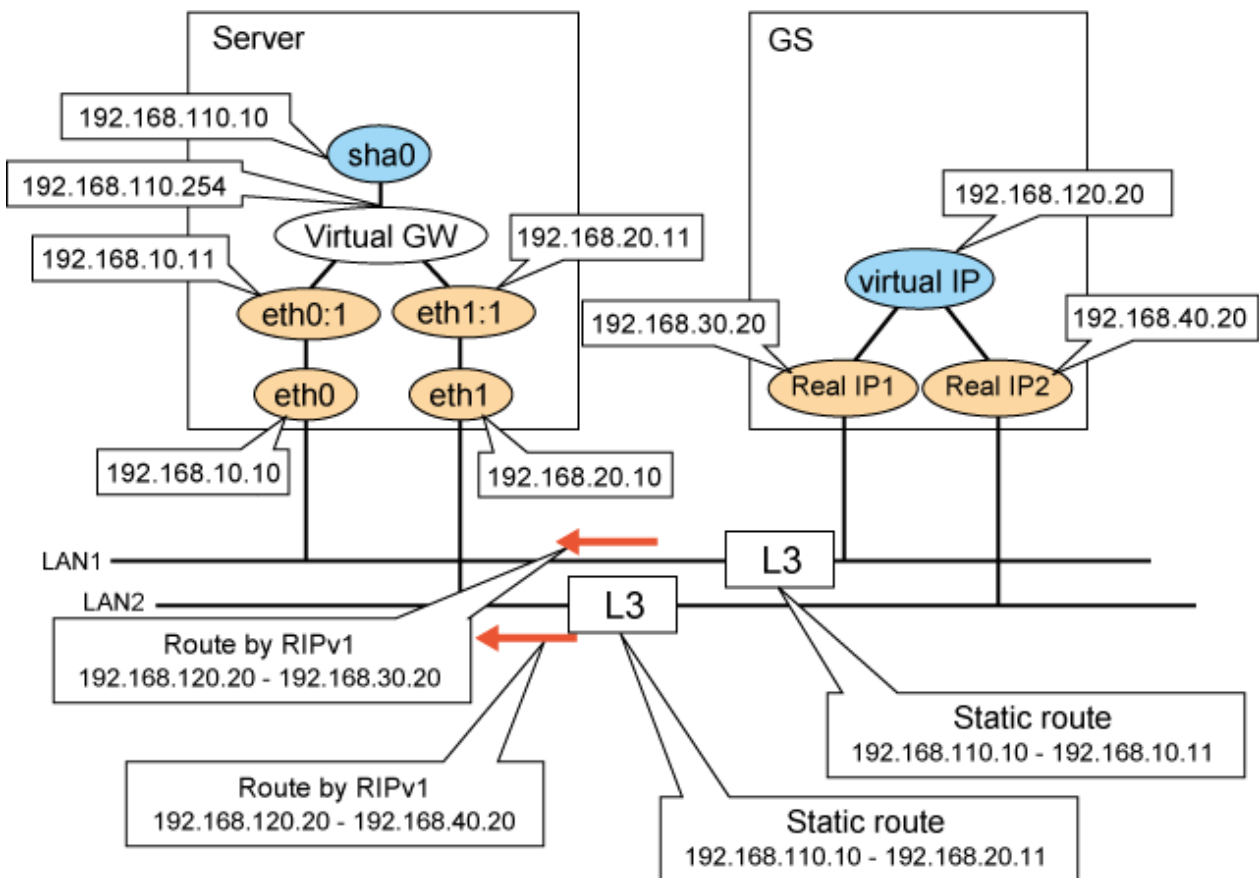


See

"3.10.1.1 Setting the monitoring destination information"

### G.6.3 Network device settings

When you connect to GS from GLS via router or LANC2, you need to set the gateway route for GLS's virtual IP address for the router or LANC2. Also, you need to set the router to broadcast the route for GS's virtual IP with RIPv1 to the server that uses GLS.



## Confirmation method

- Check the settings of the static route for the router and RIP broadcasts.
- Since RIP is processed within GLS, it is not necessary to run the daemon (quagga(ripd)) which obtains RIP in the server.

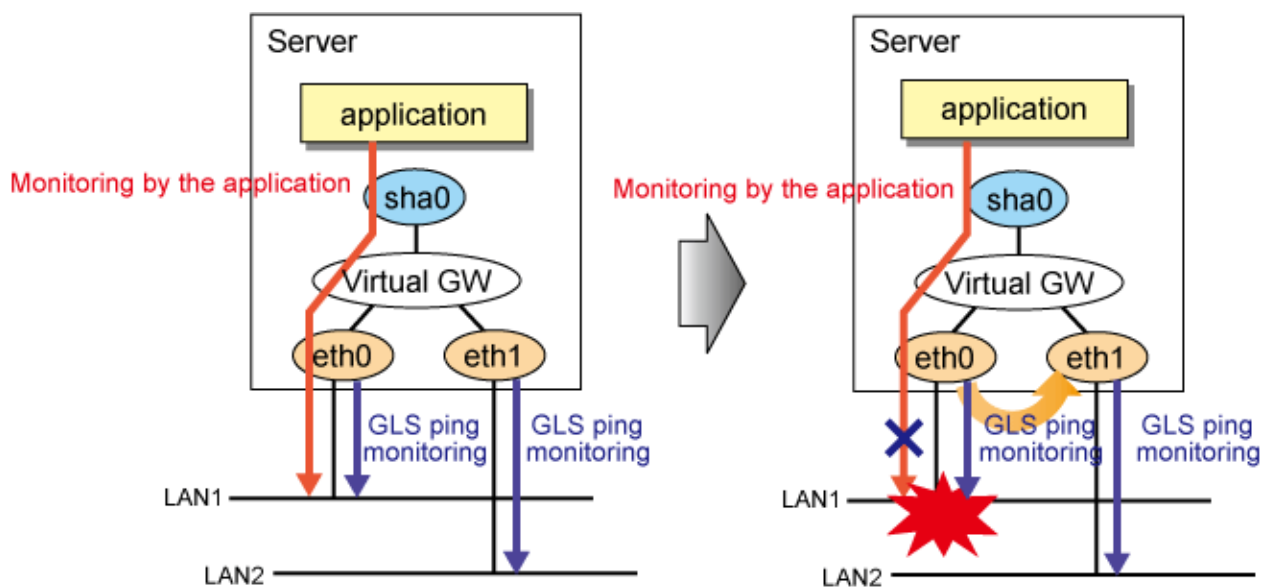


See

- "2.1.4.5 Notes"
- "2.10.5 Duplicated operation via GS linkage mode"

## G.6.4 Monitoring time adjustment

If you are monitoring communications for virtual IP addresses with high level applications, adjust the monitoring time taken by GLS or the application so that an error is not detected by the application in less time than GLS needs to switch the network.



## Confirmation method

Use the "hanetobserv" command to check the time it takes for an error to be detected (interval x times)

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = YES
```

## G.6.5 Maintenance procedure performed when the communication target stopped

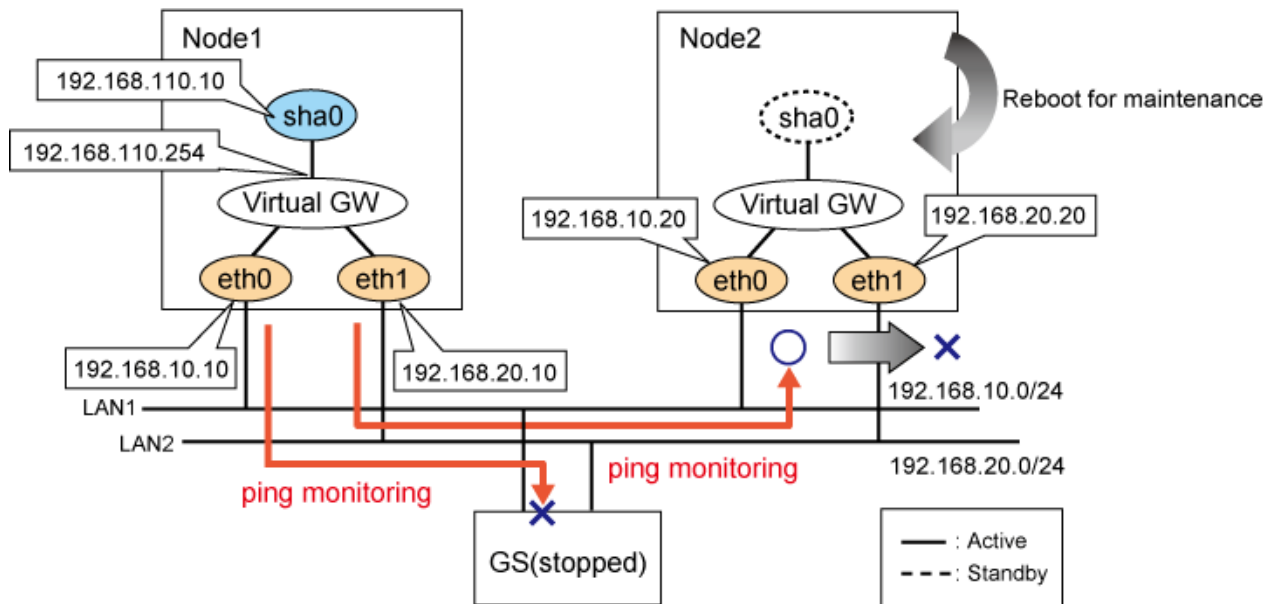
Actions to be taken will differ depending on whether the IP addresses of neighboring switches are set or not in the destination cluster node monitoring information.

When IP addresses of neighboring switches have been set

No particular procedure is required.

When IP addresses of neighboring switches have not been set

When GLS is used in a cluster configuration, if you shut down the communication target completely and reboot another cluster node, the other node determines that all networks have failed and a node failure occurs.



Perform maintenance procedure when the communication target stopped (rebooting, etc.) using one of the following procedures.

- Maintenance procedure1

1. Stop the cluster of both nodes (node1 and node2)
2. Perform maintenance (rebooting, etc.) on the node to be serviced.
3. Boot the cluster on both nodes (node1 and node2)

- Maintenance procedure2

1. Check that all GLS resource states are Offline or Standby on the standby node to be serviced. If there is a GLS resource on the maintenance side, check that the GLS resource has failed over to the other node (node2).
2. Adjust the GLS settings so that any network errors will not be detected by the active node.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv param -f no
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
fail over mode(f) = NO
```

3. Stop the standby node's cluster.
4. Perform maintenance on the standby node.
5. After completing the maintenance, check that a ping can be sent to the physical IP address of the node on which you have performed maintenance. Check the settings so that a network error can be detected.

```
# ping 192.168.10.20
# ping 192.168.20.20
# /opt/FJSVhanet/usr/sbin/hanetobserv param -f yes
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
```

```
repair_time(b)      =    5 sec  
fail over mode(f)  = YES
```

#### Confirmation method

Check the maintenance procedure performed when the communication target stopped.



See

"2.8.1.4 Cluster fail-over of GS linkage mode"

### G.6.6 PTF of the communication target

---

See the GLS handbook to check whether the PTF required for connecting GLS has been applied to the GS of the communication target.

#### Confirmation method

Check the GLS handbook.



See

"2.1.4.5 Notes"

# Appendix H Changes from previous versions

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

## H.1 Changes from Redundant Line Control function 4.0A20 to version 4.1A20

Table H.1 List of changes from Redundant Line Control function 4.0A20 to 4.1A20 is a list of changes made from the previous version.

Table H.1 List of changes from Redundant Line Control function 4.0A20 to 4.1A20

Category	Item	Version
New command	None	-
Incompatible commands	hanetconfig command	Redundant Line Control function 4.1A20
	hanetpoll command	Redundant Line Control function 4.1A20
	strhanet command	Redundant Line Control function 4.1A20
	stphanet command	Redundant Line Control function 4.1A20
Incompatible functions	Resource state monitoring function for standby node	Redundant Line Control function 4.1A20
	Interface state monitoring feature	Redundant Line Control function 4.1A20

### H.1.1 New commands

There are no new commands for Redundant Line Control function 4.1A20.

### H.1.2 Incompatible commands

The following are the incompatible commands of Redundant Line Control function from the previous version.

#### (1) hanetconfig command

##### [Contents]

If a host name you specify via "-i" or "-e" option of the hanetconfig command includes invalid characters (except for alpha-numeric characters, period, and hyphen) mentioned in RFC952 and RFC1123, it is treated as an error. For details on this issue, refer to "[7.1 hanetconfig 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 4.0A20 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.

## (2) hanetpoll command

### [Contents]

If a host name you specify via "-p" option of the hanetpoll command includes invalid characters (except for alpha-numeric characters, period, and hyphen) mentioned in RFC952 and RFC1123, it is treated as an error. For details on this issue, refer to "[7.7 hanetpoll 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 4.0A20 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.

## (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.

## (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.

## H.1.3 Incompatible functions

---

The following are the incompatible commands of Redundant Line Control function from the previous version.

### (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 "Standby Transition" attribute and to monitor the status of GLS resource in the standby node. If neglecting this configuration, it will not monitor the status of standby node of GLS resource. For reference, see ["5.3.1 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]

When attempting to restore the configuration file for 4.0A20 to the cluster system of version 4.1A20 or later using the backup function of a cluster system, the value "StandbyTransistion" 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 Admin View to apply the "StandbyTransition" attribute in the configuration file.

### (2) Interface status monitoring feature

[Contents]

If a user abruptly use ifconfig 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 ["2.7.1 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 apply changes to physical interfaces, restart interface status monitoring function of the bundled physical interface using `resethanet -s` command after applying changes to the configuration settings. For details on `resethanet` command, refer to ["7.20 resethanet Command"](#).



## H.2 Changes from Redundant Line Control function 4.1A20 to version 4.1A30

---

Table H.2 List of changes from Redundant Line Control function 4.1A20 to 4.1A30 is a list of changes made from the previous version.

Table H.2 List of changes from Redundant Line Control function 4.1A20 to 4.1A30

Category	Item	Version
New command	None	-
Incompatible commands	hanetpoll Command	Redundant Line Control function 4.1A30
	resethanet Command	Redundant Line Control function 4.1A30
Incompatible function	Verifying the Network address	Redundant Line Control function 4.1A30

### H.2.1 New commands

---

There are no new commands for Redundant Line Control function 4.1A30.

### H.2.2 Incompatible commands

---

#### (1) hanetpoll command

[Contents]

In the "-p" option of the hanetpoll command, the IP address of IPv6 link-local address can be specified as a monitoring target.

[Changes]

- Before modification

It will become an error if the IP address of IPv6 link-local address is specified to be a monitoring target.

- After modification

It does not become an error even if it specifies the IP address of IPv6 link-local address to be a monitoring target.

[Notes]

In the case of the network environment where an IPv6 address is not defined automatically, if the IP address of IPv6 link-local address is specified to be a monitoring target, it can monitor.

#### (2) resethanet command

[Contents]

When an environmental definition is deleted by using the "resethanet -i" command, subnet mask information defined by the "hanetmask" command is deleted together.

[Changes]

- Before modification

Subnet mask information defined by "hanetmask" command is not deleted.

- After modification

Subnet mask information defined by "hanetmask" command is deleted.

### H.2.3 Incompatible functions

---

## (1) 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 are 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 subnet mask by hanetmask command. A warning message may be output when subnet 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	No warning message

- 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)

### [Notes]

- If warning message (No.358) displays while running the following commands, check the IP address or net mask value configured on the physical and virtual interfaces. It is possible that IP address or net mask value is invalid. Note that, command process continues execution regardless of the warning messages.
  - /opt/FJSVhanet/usr/sbin/hanetconfig create
  - /opt/FJSVhanet/usr/sbin/hanetconfig modify
  - /opt/FJSVhanet/usr/sbin/hanetconfig copy
  - /opt/FJSVhanet/usr/sbin/strhanet
  - /opt/FJSVhanet/usr/sbin/hanetnic add
  - /opt/FJSVhanet/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 the system log instead of a standard error (stderr).

## H.3 Changes from Redundant Line Control function 4.1A30 to version 4.1A40

---

There is no difference of the function.

## H.4 Changes from Redundant Line Control function 4.1A40 to version 4.2A00

---

[Table H.3 List of changes from Redundant Line Control function 4.1A40 to 4.2A00](#) is a list of changes made from the previous version.

Table H.3 List of changes from Redundant Line Control function 4.1A40 to 4.2A00

Category	Item	Version
New command	None	-
Incompatible command	None	-
Incompatible function	Supports tagged VLAN (IEEE 802.1Q) in Redundant Line Control function.	Redundant Line Control function 4.2A00

### H.4.1 New commands

---

There are no new commands for Redundant Line Control function 4.2A00.

### H.4.2 Incompatible commands

---

No commands in the Redundant Line Control function 4.2A00 are incompatible from the previous versions.

### H.4.3 Incompatible functions

---

#### (1) Support for tagged VLAN interfaces

[Contents]

If tagged VLAN interfaces (e.g. eth0.2 and eth1.5) are generated through the Ethernet driver with IEEE 802.1Q tagged VLAN, they can be made redundant and used with the redundant line control function.

[Changes]

- Before modification

The tagged VLAN interfaces cannot be made redundant and used with the redundant line control function.

- After modification

The tagged VLAN interfaces can be made redundant and used with the redundant line control function.

## H.5 Changes from Redundant Line Control function 4.2A00 to version 4.2A30

---

[Table H.4 List of changes from Redundant Line Control function 4.2A00 to 4.2A30](#) is a list of changes made from the previous version.

Table H.4 List of changes from Redundant Line Control function 4.2A00 to 4.2A30

Category	Item	Version
New commands	hanetgw Command	Redundant Line Control function 4.2A30
	hanetobserv Command	Redundant Line Control function 4.2A30
	dspobserv Command	Redundant Line Control function 4.2A30

Category	Item	Version
Incompatible command	None	-
Incompatible functions	GS linkage mode	Redundant Line Control function 4.2A30
	Link monitoring	Redundant Line Control function 4.2A30
	Operation for Virtual Machine Function	Redundant Line Control function 4.2A30
	Hostname resolution	Redundant Line Control function 4.2A30

## H.5.1 New commands

---

Redundant Line Control function 4.2A30 provides the following commands.

- hanetgw Command
- hanetobserv Command
- dspobserv Command

For details on each command, see "[Chapter 7 Command references](#)".

## H.5.2 Incompatible commands

---

No commands in the Redundant Line Control function 4.2A30 are incompatible from the previous versions.

## H.5.3 Incompatible functions

---

### (1) GS linkage mode

[Contents]

GS linkage mode provides highly reliable communications between GS (Global Server) and GLS.

[Changes]

- Before modification

Highly reliable communication between GS and GLS is not available.

- After modification

Highly reliable communication between GS and GLS is available.

### (2) Link monitoring

[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. 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).

- 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).

### (3) Operation for Virtual Machine Function

#### [Contents]

The PRIMEQUEST 1000 Series Virtual Machine Function and the Linux Virtual Machine Function support GLS operation.

#### [Changes]

- Before modification

GLS is not available on the Virtual Machine Function.

- After modification

GLS is available on the Virtual Machine Function.

### (4) Hostname resolution

#### [Contents]

The function is added that enables you to change the host name from the /etc/hosts file without depending on the OS settings if the host name is used for the GLS settings. This function is enabled by the -h option of the hanetparam command.

#### [Changes]

- Before modification

If the operating system is set to use DNS servers or similar to change the host name, the GLS's command may take long time to complete.

- After modification

Even if the operating system is set to use DNS servers or similar, the command will complete immediately.

## H.6 Changes from Redundant Line Control function 4.2A30 to version 4.3A00

Table H.5 List of changes from Redundant Line Control function 4.2A30 to 4.3A00 is a list of changes made from the previous version.

Table H.5 List of changes from Redundant Line Control function 4.2A30 to 4.3A00

Category	Item	Version
New command	None	-
Incompatible command	hanetpoll Command	Redundant Line Control function 4.3A00
Incompatible functions	Parameter settings for each virtual interface	Redundant Line Control function 4.3A00
	Self-checking function	Redundant Line Control function 4.3A00
	Configuration in which the tagged VLAN and normal LAN are mixed	Redundant Line Control function 4.3A00
	Cluster operation on the virtual machine function	Redundant Line Control function 4.3A00
	VLAN operation on the virtual machine function	Redundant Line Control function 4.3A00

### H.6.1 New commands

There are no new commands for Redundant Line Control function 4.3A00.

## H.6.2 Incompatible commands

---

### (1) hanetpoll command

#### [Contents]

A new suboption (devparam) for setting parameter functions for each virtual interface has been added. For details, see "[7.7 hanetpoll Command](#)".

#### [Changes]

- Before modification

The "devparam" suboption cannot be specified in the "hanetpoll" command.

- After modification

The "devparam" suboption can be specified in the "hanetpoll" command.

## H.6.3 Incompatible functions

---

### (1) Parameter setting function for each virtual interface

#### [Contents]

The NIC switching mode allows you to set monitoring parameters for each virtual interface. With this, you can create the settings so that the cluster is not switched even if an error occurs on the administrative LAN in an environment where there is an administrative LAN and public LAN. Set each parameter by hanetpoll command.

#### [Changes]

- Before modification

Monitoring parameters for each virtual interface cannot be set in NIC switching mode.

- After modification

Monitoring parameters for each virtual interface can be set in NIC switching mode.

### (2) Self-checking function

#### [Contents]

This function allows you to monitor the operational state of GLS (state of the control daemon and virtual driver) and have a message output to the system log in the event of an error. To enable this function, reboot the system after modifying the settings using the "hanetparam" command.

#### [Changes]

- Before modification

The operational state of GLS cannot be monitored.

- After modification

The operational state of GLS can be monitored.

### (3) Configuration in which the tagged VLAN and normal LAN are mixed

#### [Contents]

The tagged VLAN interface and normal interface (no tag) can be bound. (Synchronous switching mode only)

#### [Changes]

- Before modification

The tagged VLAN and normal LAN cannot be bound.

- After modification

The tagged VLAN and normal LAN can be bound. (Synchronous switching mode only)

#### (4) Cluster operation on the virtual machine function

[Contents]

GLS operations associated with the cluster on the PRIMEQUEST 1000 Series Virtual Machine Function are supported.

[Changes]

- Before modification

GLS and PCL cannot be linked and operated on the guest OS of the virtual machine function.

- After modification

GLS and PCL can be linked and operated on the guest OS of the virtual machine function.

#### (5) VLAN operation on the virtual machine function

[Contents]

The VLAN that is supported on the virtual machine function can be made highly reliable.

[Changes]

- Before modification

The VLAN on the virtual machine function cannot be made highly reliable.

- After modification

The VLAN on the virtual machine function can be made highly reliable.

## H.7 Functional Improvements in Redundant Line Control function 4.3A00

Table H.6 List of Functional Improvements in Redundant Line Control 4.3A00 is a list of functional improvements.

For the latest information on compatibility, refer to the update information file included in the patch.

Table H.6 List of Functional Improvements in Redundant Line Control 4.3A00

Category	Item	Patch Condition
New command	None	-
Incompatible commands	dspobserv Command	T002518QP-01 or later, and T002830QP-01 or later
	hanetobserv Command	T002830QP-02 or later
Incompatible function	Retry function for recovery monitoring in GS linkage mode	T002830QP-02 or later

### H.7.1 New commands

There are no new commands for functional improvements in Redundant Line Control function 4.3A00.

### H.7.2 Incompatible commands

#### (1) dspobserv command

[Contents]

In GS linkage mode, a new suboption (-d) is added to display the place of a node which is a communication target of GLS.

An asterisk (\*) is displayed at the end of a physical IP address of a node which is recognized as a communication target.

```
# /opt/FJSVhanet/usr/sbin/dspobserv -d
observ status      = ON
interval           = 5 sec
times              = 5 times
idle               = 60 sec
repair_time        = 5 sec
fail over mode     = YES
```

Node	VIP	NIC	Status
host1	192.168.100.10	192.168.10.10*	ACTIVE
		192.168.20.10*	ACTIVE
		192.168.10.20	ACTIVE
		192.168.20.20	ACTIVE

#### [Changes]

- Before modification

The "-d" suboption cannot be specified with the "dspobserv" command.

- After modification

The "-d" suboption can be specified with the "dspobserv" command.

## (2) hanetobserv command

#### [Contents]

In GS linkage mode, a new suboption (-r) is added to set the retry count of recovery monitoring. In addition, if the retry count is set to the value of one or more, the setting value "repair\_retry = (r) times" is displayed when the "hanetobserv print" command or the "dspobserv" command is executed.

The following is the format to execute the "hanetobsrev" command.

```
/opt/FJSVhanet/usr/sbin/hanetobserv param [-s sec] [-c times] [-p sec] [-b sec] [-r times] [-f {yes | no}]
```

#### -r times

Specify the retry count to return to the regular monitoring if recovery monitoring has been consecutively successful after detecting an error in recovery monitoring by remote host monitoring. A value from 0 to 300 can be specified. The default value is 0 (time).

The following is a setting example.

- 1) Display the current setting.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)       = 5 sec
times(c)          = 5 times
idle(p)           = 60 sec
repair_time(b)    = 5 sec
fail over mode(f) = YES
```

Destination Host	Virtual Address	(Router Address+)NIC Address
host1	192.168.100.10	192.168.10.10,192.168.20.10 192.168.10.20,192.168.20.20

- 2) Change the retry count of the recovery monitoring function.



```
# /opt/FJSVhanet/usr/sbin/hanetobserv param -r 3
```

3) Displays the changed setting. The item of "repair\_retry(r)" is displayed.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv print
interval(s)      = 5 sec
times(c)         = 5 times
idle(p)          = 60 sec
repair_time(b)   = 5 sec
repair_retry(r)  = 3 times
fail over mode(f) = YES

Destination Host Virtual Address      (Router Address+)NIC Address
+-----+-----+-----+
+
host1          192.168.100.10          192.168.10.10,192.168.20.10
                                           192.168.10.20,192.168.20.20

# /opt/FJSVhanet/usr/sbin/dspobserv
observ status    = OFF
interval        = 5 sec
times           = 5 times
idle            = 60 sec
repair_time      = 5 sec
repair_retry     = 3 times
fail over mode  = YES

Node            VIP            NIC            Status
+-----+-----+-----+-----+
host1          192.168.100.10          192.168.10.10    ----
                                           192.168.20.10    ----
                                           192.168.10.20    ----
                                           192.168.20.20    ----
```

4) Specify "0" to change the setting back to the default.

```
# /opt/FJSVhanet/usr/sbin/hanetobserv param -r 0
```

#### [Changes]

- Before modification

The "-r" suboption cannot be specified with the "hanetobserv" command.

- After modification

The "-r" suboption can be specified with the "hanetobserv" command.

## H.7.3 Incompatible functions

### (1) Retry function for recovery monitoring in GS linkage mode

Previously, in the GS linkage mode, recovery monitoring by ping commands determined a target to have recovered when a single ping was successfully returned.

The new version allows for setting the retry count of ping monitoring so that the function determines that the transfer path is recovered when ping is successful for several times.

For information on retry count, see "(2) hanetobserv command".

#### Recovery detection time:

Recovery detection time = recovery monitoring interval (in seconds) +  
recovery monitoring interval (in seconds) x retry count (times)

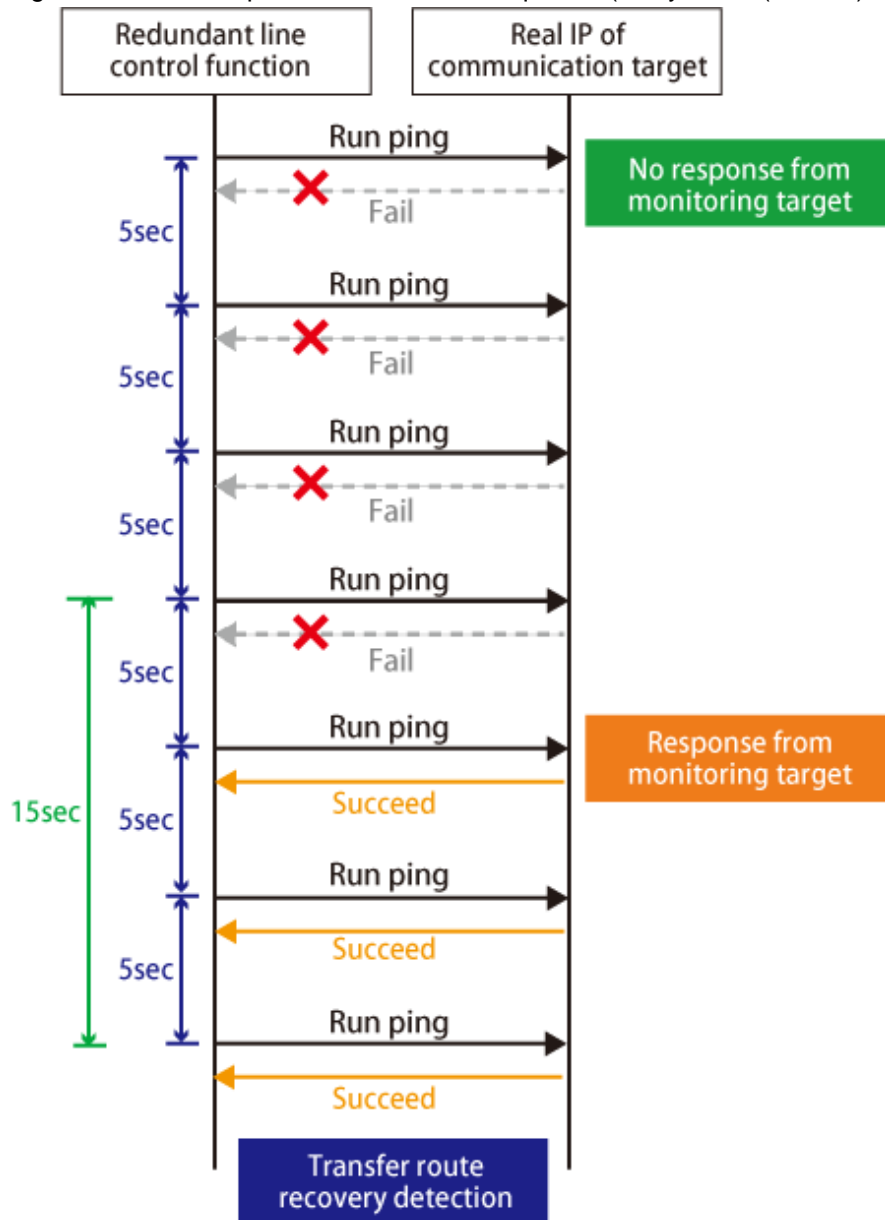
The default value would look like the following.

5 sec = 5 sec

When the retry count is 2 times, the value would look like the following.

15 sec = 5 sec + 5 sec x 2 time

Figure H.1 Transfer path error detection sequence (Retry count (2 times))



[Changes]

- Before modification

When ping is successful one time by the recovery monitoring function in GS linkage mode, the function determines that the transfer path is recovered.

- After modification

When ping is successful for several times by the recovery monitoring function in GS linkage mode, the function determines that the transfer path is recovered.

## H.8 Changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10

Table H.7 List of changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10 is a list of changes.

Table H.7 List of changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10

Category	Item	Version
New commands	hanetpathmon Command	Redundant Line Control function 4.3A10 or later
	dsppathmon Command	Redundant Line Control function 4.3A10 or later
Incompatible commands	hanetconfig Command	Redundant Line Control function 4.3A10 or later
	hanetnic Command	Redundant Line Control function 4.3A10 or later
	dsphanet Command	Redundant Line Control function 4.3A10 or later
	hanethvrsc Command	Redundant Line Control function 4.3A10 or later
	hanetparam Command	Redundant Line Control function 4.3A10 or later
	hanetobserv Command	Redundant Line Control function 4.3A10 or later
Incompatible functions	NIC switching mode	Redundant Line Control function 4.3A10 or later
	GS load sharing	Redundant Line Control function 4.3A10 or later
	Option for UDP application	Redundant Line Control function 4.3A10 or later
	Conditions to output the message in Fast switching mode	Redundant Line Control function 4.3A10 or later
	Order to start and stop of GLS service	Redundant Line Control function 4.3A10 or later
	Conditions to output the message for a NIC bundled in the GLS virtual interface	Redundant Line Control function 4.3A10 or later

### H.8.1 New commands

#### (1) hanetpathmon command

[Contents]

A command to set network monitoring in Virtual NIC mode is added. For details, see "[7.12 hanetpathmon Command](#)".

[Changes]

- Before modification

There are no commands to set network monitoring in Virtual NIC mode.

- After modification

A command to set network monitoring in Virtual NIC mode is added.

#### (2) dsppathmon command

[Contents]

A command to display the status of network monitoring in Virtual NIC mode is added. For details, see "[7.13 dsppathmon Command](#)".

[Changes]

- Before modification

There are no commands to display the status of network monitoring in Virtual NIC mode.

- After modification

A command to display the status of network monitoring in Virtual NIC mode is added.

## H.8.2 Incompatible commands

---

### (1) hanetconfig command

[Contents]

The new version allows for settings of the virtual interfaces in Virtual NIC mode. For details, see "[7.1 hanetconfig Command](#)".

[Changes]

- Before modification

You cannot set virtual interfaces in Virtual NIC mode by the "hanetconfig" command.

- After modification

You can set virtual interfaces in Virtual NIC mode by the "hanetconfig" command.

### (2) hanetnic command

[Contents]

The new version allows for dynamically adding, deleting, and switching the physical interface bundled by the virtual interface in Virtual NIC mode. For details, see "[7.9 hanetnic Command](#)".

[Changes]

- Before modification

You cannot change the configuration of virtual interfaces in Virtual NIC mode by the "hanetnic" command.

- After modification

You can change the configuration of virtual interfaces in Virtual NIC mode by the "hanetnic" command.

### (3) dsphanet command

[Contents]

The new version allows for displaying the statuses of virtual interfaces in Virtual NIC mode. For details, see "[7.4 dsphanet Command](#)".

[Changes]

- Before modification

You cannot display the statuses of virtual interfaces in Virtual NIC mode by the "dsphanet" command.

- After modification

You can display the statuses of virtual interfaces in Virtual NIC mode by the "dsphanet" command.

### (4) hanethvrsc command

[Contents]

Virtual interfaces in Virtual NIC mode can be registered in the cluster resource management. Moreover, modifications are applied to check for any failures of HUB monitoring settings in NIC switching mode. For details, see "[7.17 hanethvrsc Command](#)".

[Changes 1]

- Before modification

You cannot specify Virtual NIC mode by the "hanethvrsc" command.

- After modification

You can specify Virtual NIC mode by the "hanethvrsc" command.

#### [Changes 2]

- Before modification

Error messages are not output when registering virtual interfaces of NIC switching, for which HUB monitoring is not set, to the cluster.

- After modification

Error messages are output when registering virtual interfaces of NIC switching, for which HUB monitoring is not set, to the cluster.

## (5) hanetparam command

#### [Contents]

Parameters for Virtual NIC mode can be set. In addition, the screen displayed by the "hanetparam print" command is changed. For details, see "[7.6 hanetparam Command](#)".

#### [Changes 1]

- Before modification

You cannot change parameters for Virtual NIC mode by the "hanetparam" command.

- After modification

You can change parameters for Virtual NIC mode by the "hanetparam" command.

#### [Changes 2]

- Before modification

Parameter entries are displayed in random order by the "hanetparam print" command.

```
# /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
Cluster failover in unnormality (c):OFF
Line status message output (s)     :OFF
Hostname resolution by file(h)     :NO
```

- After modification

Parameter entries are displayed for each switching mode by the "hanetparam print" command.

```
# /opt/FJSVhanet/usr/sbin/hanetparam print
[Fast switching]
Line monitor interval(w)          :5
Line monitor message output (m)    :0
Cluster failover (l)               :5
Cluster failover in unnormality (c):OFF
Line status message output (s)     :OFF

[NIC switching]
Standby patrol interval(p)         :15
Standby patrol message output(o)   :3

[Virtual NIC]
LinkDown detection time (q)        :0
LinkUp detection time (r)          :1
Link monitor starting delay (g)    :5
```

[Common Setting]	
Hostname resolution by file(h)	:NO
Self-checking function(e)	:NO

## (6) hanetobserv command

### [Contents]

Changes are made for the upper limit of the number of virtual IP addresses which can be set for the communication target monitoring function. For details, see "[7.15 hanetobserv Command](#)".

### [Changes]

- Before modification  
Up to 64 virtual IP addresses can be set for the communication target monitoring function.
- After modification  
Up to 128 virtual IP addresses can be set for the communication target monitoring function.

## H.8.3 Incompatible functions

---

### (1) Virtual NIC mode

#### [Contents]

Virtual NIC mode is added.

#### [Changes]

- Before modification  
Virtual NIC mode is not provided.
- After modification  
Virtual NIC mode is added.

### (2) Configuration of GS load sharing

#### [Contents]

In GS linkage mode, in addition to conventional GS of hot-standby configurations or single system configurations, protocols used on GS in load sharing configurations are supported.

#### [Changes]

- Before modification  
No communication is possible with GS in a load sharing configuration, even when using GS linkage mode.
- After modification  
Communication is possible with GS in a load sharing configuration when using GS linkage mode.

#### [Notes]

GS load sharing configurations are supported by default. Therefore, you do not need to change GLS parameters. In addition, load sharing configurations are valid even when the following parameters are set:

/etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
# Each entry is of the form:
#
# <param> <value>
```

```
#
observ_msg      0
observ_polling_timeout  180
max_node_num    4
load_sharing    1
```

### (3) Options for UDP application

#### [Contents]

Settings of arpflag parameters are not required in environments in which frequently transmitting UDP applications (\*1) use NIC switching mode.

Note \*1: For example, applications that implement heartbeat processing between nodes

#### [Changes]

- Before modification

For using frequently transmitting UDP applications, "arpflag 1" must be specified.

- After modification

For using frequently transmitting UDP applications, "arpflag 1" is not required to be specified.

#### [Notes]

Frequently transmitting UDP applications are supported by default. In addition, they are valid even when the following parameters are set:

/etc/opt/FJSVhanet/config/ctld.param

```
#
# HA-Net Configuration File
#
#      Each entry is of the form:
#
#      <param> <value>
#
observ_msg      0
observ_polling_timeout  180
max_node_num    4
arpflag        1
```

### (4) Conditions to output the message in Fast switching mode

#### [Contents]

The condition to output the console message (message number: 990) for Fast switching mode has been changed.

#### Console output message:

```
hanet: 99080: line status changed: all lines disabled: (devicename: interface1=Down,
interface2=Down, ...)
```

#### [Changes]

- Before modification

This message is output if no communication target is recognized.

- After modification

This message is output if at least one communication target is recognized and then the target becomes unrecognizable.

[Notes]

- The console output message (message number: 990) is displayed if the "Line status message output (s)" is set to "ON" by using the "hanetparam" command with the "-s" option (The default value is OFF).
- This change of the condition to output the message is applied for startup of the system or execution of the "strhanet" command. In cases other than above (for example, communication or switching), no changes are applied for conditions to output the message.

## (5) Order to start and stop of GLS service

[Contents]

Order to start and stop of GLS service (hanet) is changed on startup of the operating system.

[Changes]

- Before modification  
Start with S32hanet. Stop with K68hanet.
- After modification  
Start with S11hanet. Stop with K89hanet.

[Notes]

The virtual IP address of GLS which is not registered in a cluster is activated on startup of GLS service (hanet). The virtual IP address is deactivated on stop of GLS service. In addition, the virtual IP of the Virtual NIC mode is activated with the S10network.

## (6) Conditions to output the message for a NIC bundled in the GLS virtual interface

[Contents]

In Fast switching mode, NIC switching mode, or GS linkage mode, when the virtual interface of GLS is activated and a physical interface cannot be UP, the following message is output to the system log:

```
hanet: ERROR: 853XX: physical interface up failed. nicname=ethY name=shaZ
```

[Changes]

- Before modification  
The error message (message number: 853) is not output to the system log.
- After modification  
The error message (message number: 853) is output to the system log.

[Notes]

For the virtual NIC mode, the following message is output to the system log:

```
hanet: WARNING: 91180: link down detected: the physical interface link is down. (shaX: ethY)
```

## H.9 Changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20

Table H.8 List of changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20 is a list of changes.

Table H.8 List of changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20

Category	Item	Version
New command	None	-
Incompatible command	hanetconfig Command	Redundant Line Control function 4.3A20 or later
Incompatible functions	Checking the physical interface configuration file	Redundant Line Control function 4.3A20 or later



Category	Item	Version
	Conditions to output the message for the GLS virtual interface	Redundant Line Control function 4.3A20 or later

## H.9.1 New commands

---

There are no new commands for Redundant Line Control function 4.3A20.

## H.9.2 Incompatible commands

---

The following are the incompatible commands of Redundant Line Control function from the previous version.

### (1) hanetconfig command

#### [Contents]

A new function for checking the contents of the physical interface configuration file (/etc/sysconfig/network-scripts/ifcfg-device name) has been added. This function is used when creating the configuration information of the virtual interface by using the "create" subcommand of the "hanetconfig" command.

#### [Changes]

##### - Before modification

The contents of the physical interface configuration file cannot be checked with the hanetconfig command.

##### - After modification

The contents of the physical interface configuration file can be checked with the hanetconfig command. If a setting error is detected, the warning message (message number: 927) is output.

#### [Notes]

##### - The contents of the following are checked:

- "HOTPLUG"
- "GATEWAY" (only for the NIC switching mode)
- "DEVICETYPE" and "TYPE" (only for the virtual NIC mode)

##### - Even if a setting error is detected, the virtual interface configuration information is created.

If you do not modify the setting error, the warning message (message number: 927) is output to the system log when starting the operating system or executing the resethanet -s command.

## H.9.3 Incompatible functions

---

### (1) Checking the physical Interface configuration file

#### [Contents]

A new function for checking the existence and contents of the physical interface configuration file (/etc/sysconfig/network-scripts/ifcfg-device name) has been added.

#### [Changes]

##### - Before modification

The existence and contents of the physical interface configuration file are not checked when starting the system.

##### - After modification

The existence and contents of the physical interface configuration file are checked when starting the system.

##### - When the physical interface configuration file does not exist.

The warning message (message number: 928) is output to the system log.

- When there is an error in the contents of the physical interface configuration file.

The warning message (message number: 927) is output to the system log.

[Notes]

The contents of the following are checked:

- "HOTPLUG"
- "GATEWAY" (only for the NIC switching mode)
- "DEVICETYPE" and "TYPE" (only for the virtual NIC mode)

## (2) Conditions to output the message for the GLS virtual interface

[Contents]

When activating the GLS virtual interface is failed in starting OS, the following message is output to the system log.

```
hanet: ERROR: 81400: cannot up interface. (shaX)
```

[Changes]

- Before modification

The error message (message number: 814) is not output to the system

- After modification

The error message (message number: 814) is output to the system

## H.10 Changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30

Table H.9 List of changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30 is a list of changes.

Table H.9 List of changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30

Category	Item		Version
New command	None		-
Incompatible command	hanetnic Command		Redundant Line Control function 4.3A30 or later
Incompatible functions	Virtual NIC mode	MAC address setting function	Redundant Line Control function 4.3A30 or later
		Supporting communication by a takeover IP in the configuration where the virtual bridge is connected	Redundant Line Control function 4.3A30 or later
		Strengthening the link monitoring	Redundant Line Control function 4.3A30 or later

### H.10.1 New commands

There are no new commands for Redundant Line Control function 4.3A30.

### H.10.2 Incompatible commands

The following are the incompatible commands of Redundant Line Control function from the previous version.

## (1) hanetnic command

### [Contents]

The procedure to recover from the following statuses:

- A cluster is configured with the NIC switching mode,
- NO is set to "FAILOVER Status" in the monitoring setting, and
- Both system failure is detected with the ping monitoring

### [Changes]

- Before modification

You need to fail back the path after restarting the monitoring with the hanetpoll on command.

- After modification

Restarting the monitoring is not required.

## H.10.3 Incompatible functions

---

### (1) The MAC address setting function for Virtual NIC mode

#### [Contents]

The setting function of MAC address is added for Virtual NIC mode.

#### [Changes]

- Before modification

The MAC address cannot be set to the virtual interface.

- After modification

By setting SHAMACADDR to the setting file of the virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX), any MAC address can be set to the virtual interface. For details, see "[3.3.3 Virtual NIC mode](#)."

If the setting of SHAMACADDR is invalid, the warning message (No: 930) is output.

If SHAMACADDR is not set on a guest OS in VMware, the warning message (No: 929) is output.

#### [Notes]

When using Virtual NIC mode on a guest OS in VMware, the MAC address needs to be set by this function.

### (2) Supporting communication by a takeover IP in the configuration where the virtual bridge is connected in Virtual NIC mode

#### [Contents]

Communication by a takeover IP address is supported in the configuration where the virtual bridge is connected to the virtual interface in Virtual NIC mode.

#### [Changes]

- Before modification

Communication is failed by a takeover IP address in the configuration where the virtual bridge is connected.

- After modification

Communication is possible by a takeover IP address in the configuration where the virtual bridge is connected.

#### [Notes]

If the virtual bridge is connected, the takeover IP address is set to the virtual bridge.

### (3) Strengthening the link monitoring of Virtual NIC mode

#### [Contents]

Added the condition that the link monitoring detects an error.

**[Changes]**

- Before modification

An error is detected due to a link down of the physical interface.

- After modification

An error is detected by a link down of the physical interface or deactivation.

# 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.

---

## Dynamic switching function

A function to switch to a standby interface while an active interface is active.

---

## 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.

---

## GLS

Stands for Global Link Services.

---

## GS

Stands for Global Server.

---

## GS linkage mode

A method that provides high-reliability by multiplexing transfer routes between GS (Global Server) and GLS, and switching to a normal route during transfer route failure.

---

## 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] [HUB-to-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](#)

---

## KVM

This structure employs the Linux kernel itself as a hypervisor, with total virtualization providing a virtualized OS environment.

---

## KVM guest

Guest OS running in a KVM environment.

---

## KVM host

Guest OS running in a KVM environment.

---

## 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

---

## Link status monitoring function

This function monitors the Ethernet link statuses of all duplicated LAN cards. When a link down occurred with a LAN card on the active side, a failover to a LAN card on the standby side is performed.

---

## Load sharing configuration

A load sharing configuration connects multiple GSs for distributing processing and thereby balancing load, intended to improve processing efficiency and reliability.

---

## 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

---

## Network monitoring function

This function uses two methods (HUB monitoring and standby patrol) to monitor statuses of networks to which virtual interfaces are connected.

---

## NIC

Stands for Network Interface Card. Also called a LAN card.

---

## NIC sharing

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.

---

## 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.

---

## Sharing transfer route monitoring

This refers to the case where multiple virtual interfaces specifies the same polling target. All of the virtual interfaces specified with the same polling target will simultaneously switch over when a failure occurs on the transfer route.

[Related article] [NIC switching mode](#)

---

## SIS

Stands for Scalable Internet Services.

---

## 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 (IEEE 802.1Q)

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 interface generated from a VLAN module that supports Tagged VLAN functionality (IEEE 802.1Q).



---

## 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.

---

## TNOTIFY command

This is the command for OS IV VTAM-G TISP.

If the host (GS) is in the hot-standby configuration, this command is used to notify in which host (GS) the virtual IP address (\*) exists.

For details, refer to "OSIV VTAM-G TISP HANDBOOK (V10)".

\*: The virtual IP address as the communication target of GLS

---

## User command execution function

This refers execution of a command manually operated by the user.

[Related article] NIC switching mode, GS linkage mode

---

## Virtual bridge

One of elements constituting a virtual network. It consists of bridge modules on the host OS (Linux).

---

## 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

Communication method generating virtual interfaces for making multiple physical NICs (LAN cards) connected on the same network logically look like a single one. This mode controls switching of transfer paths by exclusively using redundant NICs. Without any limitations on communication targets, this mode also enables to communicate with hosts on other networks via routers.

---

## 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".

# Index

<b>[A]</b>	
Active interface.....	742
Active Standby.....	168,171
Automatic fail-back function.....	41,742
<b>[C]</b>	
Cascade.....	192,195,205
Cluster failover function (failover function).....	742
Cluster system	
....	164,165,379,382,385,389,404,408,412,417,436,440,444,450,479,483,487,491,494,498,502,518,521,525,529,549,553,558,562
Configuration of GS load sharing.....	735
Configuring Tagged VLAN interface.....	32
<b>[D]</b>	
dsphanet Command.....	285
dspobserv Command.....	324
dspobserv command.....	728,733
dspathmon Command.....	315
dspathmon command.....	732
dspoll Command.....	304
Duplicated operation via Virtual NIC mode.....	63
Dynamic switching function.....	742
<b>[E]</b>	
Example of configuring Virtual NIC mode.....	567
<b>[F]</b>	
Fast switching mode	
....	1,7,10,28,62,67,85,89,94,114,117,160,370,393,422,583,742
Fault monitoring function.....	11,15,21,25
<b>[G]</b>	
GS linkage mode	
....	2,8,22,30,56,58,64,71,87,93,111,115,148,154,156,184,725,727,742
GS Load Sharing.....	591
<b>[H]</b>	
hanetbackup Command.....	330
hanetconfig Command.....	271,719,738
hanetconfig command.....	733
hanetgw Command.....	316
hanethvrsc Command.....	325
hanethvrsc command.....	733
hanetmask Command.....	287
hanetnic Command.....	305
hanetnic command.....	740
hanetobserv Command.....	318
hanetobserv command.....	729,735
hanetparam Command.....	290
hanetparam command.....	734
hanetpathmon Command.....	309
hanetpathmon command.....	732
hanetpoll Command.....	295,720,722
hanetrestore Command.....	330
Hostname resolution.....	726,728
Hot-standby.....	137
HUB-to-HUB monitoring function.....	742
HUB monitoring.....	122
HUB monitoring function.....	37,122,742
<b>[I]</b>	
Interface status monitoring feature.....	46,721
<b>[K]</b>	
KVM.....	742
KVM guest.....	742
KVM host.....	743
<b>[L]</b>	
LAN card.....	743
Line monitoring.....	743
link monitoring.....	725,727
Link status monitoring function.....	44,743
Load sharing configuration.....	139,743
Logical interface.....	743
Logical IP address.....	743
Logical IP address takeover function.....	743
Logical virtual interface.....	372,396,426,743
<b>[M]</b>	
Monitoring frame.....	743
Monitoring the remote host.....	135
Mutual standby.....	187,188,190,191
<b>[N]</b>	
Network monitoring function.....	44,743
NIC sharing.....	459,487,508,525,536,558,744
NIC switching mode	
....	1,7,14,29,52,63,68,86,90,96,114,118,124,147,149,160,209,456,505,532,744
<b>[O]</b>	
Operation on the Virtual Machine Function (for RHEL6).....	656
Operation on VMware.....	675
<b>[P]</b>	
Physical interface.....	32,744
Physical IP address.....	744
Physical IP address takeover function.....	744
Physical IP address takeover function I.....	744
Physical IP address takeover function II.....	744
Primary interface.....	744
<b>[R]</b>	
Real interface.....	744
Redundant Line Control Function.....	158,215,333,744
resethanet Command.....	331,722
Resource state monitoring function for standby node.....	721
RMS Wizard.....	745
<b>[S]</b>	
Secondary interface.....	745

Sharing physical interface.....	28,116
Sharing transfer route monitoring.....	745
Single configuration.....	136
Standby interface.....	745
Standby patrol function.....	41,129,745
Standby patrol function (automatic fail-back if a failure occurs) .....	745
Standby patrol function (immediate automatic failback).....	745
stphanet Command.....	283
stphanet command.....	720
stpptl Command.....	308
strhanet Command.....	281,720
strptl Command.....	308
Switching function.....	12,17,22

## [T]

Tagged VLAN.....	724,745
Tagged VLAN interface.....	33,745
Takeover physical IP address.....	463,491,494
Takeover virtual interface.....	165,166,746
TNOTIFY command.....	746

## [U]

userApplication.....	165
User command execution function.....	51,147,746

## [V]

Verifying the Network address.....	723
Virtual bridge.....	746
Virtual interface.....	746
Virtual IP address (virtual IP).....	746
Virtual Machine Function.....	726,727
Virtual Machine Function (For RHEL5).....	607
Virtual NIC mode .....	2,8,19,69,87,90,102,115,121,160,210,212,213,680,735,746

## [W]

Web-Based Admin View.....	746
---------------------------	-----