

# Fujitsu Software

## PRIMECLUSTER Global Link Services

# Configuration and Administration Guide 4.7

## Redundant Line Control Function

Linux

J2UL-2826-03ENZ0(00)  
April 2024

# Preface

---

## Purpose

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

## Who should use this document

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

## Abstract

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

### [Chapter 1 Overview](#)

This chapter explains the overview of the Redundant Line Control Function.

### [Chapter 2 Feature description](#)

This chapter explains the functions and features of the Redundant Line Control Function.

### [Chapter 3 Environment configuration](#)

This chapter explains how to configure the environment of the Redundant Line Control Function.

### [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 Function on a cluster system.

### [Chapter 6 Maintenance](#)

This chapter explains the required investigation material to troubleshoot the problems of the Redundant Line Control Function.

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

This chapter explains how to use the commands provided by the Redundant Line Control Function.

### [Appendix A Messages and corrective actions](#)

This appendix explains the messages output by the Redundant Line Control Function.

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

This appendix explains how to configure the system environment of the Redundant Line Control Function.

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

This appendix explains how to operate the Redundant Line Control Function on the virtual machine function.

### [Appendix D Operation on RHOSP](#)

This appendix explains how to operate the Redundant Line Control Function on RHOSP.

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

This appendix explains how to operate the Redundant Line Control Function on VMware.

### [Appendix F Operation on Hyper-V](#)

This appendix explains how to operate the Redundant Line Control Function on Hyper-V.

### [Appendix G Cloning environment](#)

This appendix explains how to configure the system by cloning the Redundant Line Control Function.

### [Appendix H Troubleshooting](#)

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

[Appendix I Check list](#)

This appendix explains items to be checked before operating the Redundant Line Control Function.

[Appendix J Resident Process in GLS and Monitoring Target](#)

This appendix explains the resident process of the Redundant Line Control Function and the monitoring target.

[Appendix K Changes from previous versions](#)

This appendix explains the new functions and the specification change of the Redundant Line Control Function.

[Glossary](#)

This section explains terms related to the Redundant Line Control Function.

### Related Documentation

Refer to the following manuals as necessary.

- PRIMECLUSTER Concepts Guide
- PRIMECLUSTER Installation and Administration Guide
- PRIMECLUSTER Installation and Administration Guide Cloud Services
- FJQSS (Information Collection Tool) User's Guide
- PRIMEQUEST 3000 Series Administration Manual
- OS IV VTAM-G TISP Handbook

### 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 6	RHEL6	RHEL
Red Hat Enterprise Linux 7	RHEL7	
Red Hat Enterprise Linux 8	RHEL8	
Red Hat Enterprise Linux 9	RHEL9	
Linux Virtual Machine Function	Virtual Machine Function	
FUJITSU Server PRIMEQUEST	PRIMEQUEST	
FUJITSU Server PRIMERGY	PRIMERGY	
Red Hat OpenStack Platform	RHOSP	

## 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(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.
- Red Hat and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- Microsoft and Hyper-V are trademarks of the Microsoft group of companies.
- Ethernet is a trademark of Fuji Xerox Corporation.
- VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.
- Other product names are product names, trademarks, or registered trademarks of these companies.

## Date of publication and edition

Feb 2023, First edition July 2023, Second edition April 2024, Third 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> |
|--|

Copyright Fujitsu Limited 2024.

# 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.....	6
1.2 Redundant line control effects.....	7
1.3 System Configuration.....	7
Chapter 2 Feature description.....	11
2.1 Overview of Functions.....	11
2.1.1 Fast switching mode.....	11
2.1.1.1 Fault monitoring function.....	12
2.1.1.2 Switching function.....	13
2.1.1.3 Connectable remote host.....	14
2.1.1.4 Available application.....	14
2.1.1.5 Notes.....	15
2.1.2 NIC switching mode.....	15
2.1.2.1 Fault monitoring function.....	16
2.1.2.2 Switching function.....	19
2.1.2.3 Connectable remote host.....	21
2.1.2.4 Available application.....	21
2.1.2.5 Notes.....	21
2.1.3 Virtual NIC mode.....	21
2.1.3.1 Fault monitoring function.....	23
2.1.3.2 Switching function.....	23
2.1.3.3 Connectable remote host.....	24
2.1.3.4 Available application.....	24
2.1.4 GS linkage mode.....	24
2.1.4.1 Fault monitoring function.....	27
2.1.4.2 Switching function.....	28
2.1.4.3 Connectable remote host.....	28
2.1.4.4 Available applications.....	28
2.1.4.5 Notes.....	29
2.2 Interface structure.....	29
2.2.1 Configuring multiple virtual interfaces.....	29
2.2.2 Sharing physical interface.....	30
2.2.2.1 Using Fast switching mode.....	30
2.2.2.2 Using NIC switching mode.....	31
2.2.2.3 Using GS linkage mode.....	32
2.2.3 Configuring multiple logical virtual interfaces.....	32
2.2.4 Configuring single physical interface.....	34
2.2.5 Configuring Tagged VLAN interfaces.....	34
2.2.5.1 Redundant Line Control function using Tagged VLAN interface.....	35
2.3 Monitoring function of Fast switching mode.....	38
2.3.1 Communication target monitoring.....	38
2.4 Monitoring function of NIC switching mode.....	39
2.4.1 HUB monitoring function.....	39
2.4.1.1 Not using HUB-to-HUB monitoring feature.....	41
2.4.1.2 Using HUB-to-HUB monitoring feature.....	41
2.4.1.3 Multiple HUB monitoring on a single interface.....	43
2.4.2 Standby patrol function.....	43
2.4.3 Automatic fail-back function.....	44
2.5 Monitoring function of Virtual NIC mode.....	46
2.5.1 Link status monitoring function.....	46
2.5.2 Network monitoring function.....	46
2.6 Monitoring function of GS linkage mode.....	47

2.6.1 Communication target monitoring.....	48
2.7 Other monitoring functions.....	48
2.7.1 Interface status monitoring feature.....	49
2.7.2 Self-checking function.....	49
2.8 Linkage functions.....	50
2.8.1 Cluster fail-over when entire transfer routes fails.....	50
2.8.1.1 Cluster fail-over of Fast switching mode.....	51
2.8.1.2 Cluster fail-over of NIC switching mode.....	52
2.8.1.3 Cluster fail-over of Virtual NIC mode.....	53
2.8.1.4 Cluster fail-over of GS linkage mode.....	54
2.8.2 User command execution function.....	54
2.8.2.1 NIC switching mode.....	55
2.8.2.2 Virtual NIC mode.....	59
2.8.2.3 GS linkage mode.....	61
2.8.2.4 All of Fast switching mode, Virtual NIC mode, and GS linkage mode.....	62
2.8.2.5 Self-checking function.....	63
2.8.3 Suppression of stopping userApplication when entire transfer routes fails.....	63
2.9 Maintenance function.....	63
2.9.1 Dynamically adding/deleting/switching physical interface.....	64
2.9.2 Hot maintenance of NIC (PCI card).....	66
2.10 Notes.....	67
2.10.1 General.....	67
2.10.2 Duplicated operation by Fast switching mode.....	68
2.10.3 Duplicated operation via NIC switching mode.....	68
2.10.4 Duplicated operation via Virtual NIC mode.....	69
2.10.5 Duplicated operation via GS linkage mode.....	70
<b>Chapter 3 Environment configuration.....</b>	<b>72</b>
3.1 Setup.....	72
3.1.1 Selecting mode.....	72
3.1.2 Selecting appropriate contents.....	73
3.1.2.1 Fast switching mode.....	73
3.1.2.2 NIC switching mode.....	74
3.1.2.3 Virtual NIC mode.....	76
3.1.2.4 GS linkage mode.....	77
3.1.2.5 Configuration of individual mode.....	79
3.1.2.6 Upper limit of configuration.....	83
3.2 System Setup.....	83
3.2.1 Setup kernel parameters.....	84
3.2.2 Network configuration.....	84
3.2.2.1 Setup common to modes.....	84
3.2.2.2 System setup in Fast switching mode.....	93
3.2.2.3 System setup in NIC switching mode.....	94
3.2.2.4 System setup in Virtual NIC mode.....	94
3.2.2.5 System setup in GS linkage mode.....	95
3.3 Additional system setup.....	95
3.3.1 Fast switching mode.....	96
3.3.2 NIC switching mode.....	96
3.3.3 Virtual NIC mode.....	96
3.3.4 GS linkage mode.....	102
3.3.5 Setting parameter for individual mode.....	102
3.4 Changing system setup.....	102
3.4.1 Fast switching mode.....	102
3.4.2 NIC switching mode.....	105
3.4.3 Virtual NIC mode.....	111
3.4.4 GS linkage mode.....	122
3.4.5 Note on changing configuration information.....	125

3.5 Deleting configuration information.....	125
3.5.1 Fast switching mode.....	125
3.5.2 NIC switching mode.....	125
3.5.3 Virtual NIC mode.....	125
3.5.4 GS linkage mode.....	126
3.5.5 Note on deleting configuration information.....	126
3.6 Configuring interfaces.....	126
3.6.1 Configuring multiple virtual interfaces.....	126
3.6.2 Sharing physical interface.....	127
3.6.3 Multiple logical virtual interface definition.....	127
3.6.4 Single physical interface definition.....	128
3.6.5 Transfer route multiplexing with Tagged VLAN interface.....	128
3.6.5.1 Operating tagged VLAN interface on Fast switching mode.....	128
3.6.5.2 Operating tagged VLAN interface on NIC switching mode.....	129
3.6.5.3 Operating tagged VLAN interface on Virtual NIC mode.....	132
3.7 Setting monitoring function of Fast switching mode.....	132
3.7.1 Communication target monitoring function.....	132
3.7.1.1 Setting the monitoring destination information.....	132
3.7.1.2 Setting the monitoring interval.....	132
3.7.1.3 Setting the message output when a monitoring error occurs.....	133
3.8 Setting monitoring function of NIC switching mode.....	133
3.8.1 HUB monitoring.....	133
3.8.1.1 Creating monitoring information.....	133
3.8.1.2 Enabling HUB monitoring function.....	133
3.8.1.3 Transfer route error detection time for NIC switching mode.....	135
3.8.2 Standby patrol function.....	140
3.8.2.1 Setting what to be monitored.....	140
3.8.2.2 Setting monitoring interval.....	141
3.8.2.3 Setting error monitoring interval.....	141
3.8.3 Setting parameters for each virtual interface.....	141
3.9 Setting monitoring function of Virtual NIC mode.....	143
3.9.1 Link status monitoring function.....	143
3.9.2 Network monitoring function.....	143
3.9.2.1 Disabling the network monitoring function.....	143
3.9.2.2 Setting the monitoring destination information.....	143
3.9.2.3 Enabling the network monitoring function.....	143
3.9.2.4 Transfer route error detection time for network monitoring function.....	143
3.9.2.5 Transfer route recovery detection time for network monitoring function.....	145
3.10 Setting monitoring function of GS linkage mode.....	147
3.10.1 Monitoring the remote host.....	147
3.10.1.1 Setting the monitoring destination information.....	147
3.10.1.2 Transfer route error detection time in GS linkage mode.....	154
3.10.1.3 Transfer route recovery detection time in GS linkage mode.....	156
3.11 Setting other monitoring function.....	157
3.11.1 Interface status monitoring feature.....	157
3.11.2 Self-checking feature.....	157
3.11.2.1 How to set up the self-checking function.....	157
3.11.2.2 Error detection of the self-checking function.....	158
3.12 Setting Linkage function.....	160
3.12.1 Cluster switching behavior for failure of all the transfer paths.....	160
3.12.2 Setting user command execution function.....	160
3.12.2.1 Settings for NIC switching mode.....	162
3.12.2.2 Settings of Virtual NIC mode.....	168
3.12.2.3 Settings for GS linkage mode.....	169
3.12.2.4 Settings for all of Fast switching mode, Virtual NIC mode, and GS linkage mode.....	171
3.12.2.5 Settings for Self-checking function.....	173
3.12.3 Setting suppression of stopping userApplication when entire transfer routes fails.....	174

3.13 Setting Maintenance function.....	177
3.13.1 Setting dynamic addition/deletion/switching function of physical interfaces.....	177
3.13.1.1 Dynamic addition of physical interfaces.....	177
3.13.1.2 Dynamic deletion of physical interfaces.....	177
3.13.1.3 Dynamic switching of physical interfaces.....	177
3.13.2 Hot maintenance of NIC (PCI card).....	177
<b>Chapter 4 Operation.....</b>	<b>178</b>
4.1 Starting and Stopping Redundant Line Control Function.....	178
4.1.1 Starting Redundant Line Control Function.....	178
4.1.2 Stopping Redundant Line Control Function.....	178
4.2 Activating and Inactivating Virtual Interfaces.....	178
4.2.1 Activating virtual interfaces.....	179
4.2.2 Inactivating virtual interfaces.....	179
4.3 Displaying Operation Status.....	179
4.4 Displaying Monitoring Status.....	179
4.5 Recovery Procedure from Line Failure.....	179
4.5.1 Recovery procedure from line failure in Fast switching mode and GS linkage mode .....	180
4.5.2 Recovery procedure from line failure in NIC switching mode.....	180
4.5.3 Recovery procedure from line failure in Virtual NIC mode.....	180
4.6 Backing up and Restoring Configuration Files.....	180
4.6.1 Backing up Configuration Files.....	180
4.6.2 Restoring Configuration Files.....	180
<b>Chapter 5 GLS operation on cluster systems.....</b>	<b>182</b>
5.1 Outline of Cluster System Support.....	182
5.2 Configuration for Cluster system.....	183
5.2.1 Adding configuration.....	184
5.2.2 Modifying configuration for Cluster system.....	185
5.2.3 Deleting configuration.....	185
5.3 Configuration for user application.....	187
5.3.1 Monitoring resource status of standby node.....	187
5.3.1.1 Preface.....	187
5.3.1.2 Configuration.....	187
5.3.1.3 Recovering from a resource failure in Standby node.....	187
5.4 Operation on cluster systems.....	188
5.4.1 Active Standby (Fast switching mode).....	188
5.4.1.1 Starting.....	188
5.4.1.2 Switching.....	188
5.4.1.3 Fail-back.....	190
5.4.1.4 Stopping.....	191
5.4.2 Active Standby (NIC switching mode).....	191
5.4.2.1 Starting.....	191
5.4.2.2 Switching.....	195
5.4.2.3 Fail-back.....	199
5.4.2.4 Stopping.....	200
5.4.3 Active Standby (Virtual NIC mode).....	202
5.4.3.1 Starting.....	202
5.4.3.2 Switching.....	203
5.4.3.3 Fail-back.....	204
5.4.3.4 Stopping.....	205
5.4.4 Active Standby (GS linkage mode).....	205
5.4.4.1 Starting.....	205
5.4.4.2 Switching.....	206
5.4.4.3 Fail-back.....	208
5.4.4.4 Stopping.....	208
5.4.5 Mutual standby (Fast switching mode).....	208
5.4.5.1 Starting.....	208



5.4.5.2 Switching.....	209
5.4.5.3 Fail-back.....	209
5.4.5.4 Stopping.....	209
5.4.6 Mutual standby (NIC switching mode).....	209
5.4.6.1 Starting.....	209
5.4.6.2 Switching.....	209
5.4.6.3 Fail-back.....	211
5.4.6.4 Stopping.....	211
5.4.7 Mutual standby (Virtual NIC mode).....	211
5.4.7.1 Starting.....	211
5.4.7.2 Switching.....	211
5.4.7.3 Fail-back.....	212
5.4.7.4 Stopping.....	212
5.4.8 Mutual standby (GS linkage mode).....	212
5.4.8.1 Starting.....	212
5.4.8.2 Switching.....	212
5.4.8.3 Fail-back.....	213
5.4.8.4 Stopping.....	213
5.4.9 Cascade (Fast switching mode).....	213
5.4.9.1 Starting.....	213
5.4.9.2 Switching.....	214
5.4.9.3 Fail-back.....	215
5.4.9.4 Stopping.....	216
5.4.10 Cascade (NIC switching mode).....	216
5.4.10.1 Starting.....	216
5.4.10.2 Switching.....	219
5.4.10.3 Fail-back.....	223
5.4.10.4 Stopping.....	223
5.4.11 Cascade (Virtual NIC mode).....	226
5.4.11.1 Starting.....	226
5.4.11.2 Switching.....	227
5.4.11.3 Fail-back.....	228
5.4.11.4 Stopping.....	229
5.5 Tagged VLAN interface multiplexing on cluster system.....	229
5.5.1 Active standby (Fast switching mode).....	229
5.5.2 Active standby (NIC switching mode).....	230
5.5.3 Active Standby (Virtual NIC mode).....	231
5.5.4 Mutual Standby (Fast switching mode).....	231
5.5.5 Mutual Standby (NIC switching mode).....	232
5.5.6 Mutual Standby (Virtual NIC mode).....	233
5.5.7 Cascade (Fast switching mode).....	233
5.5.8 Cascade (NIC switching mode).....	234
5.5.9 Cascade (Virtual NIC mode).....	234
<b>Chapter 6 Maintenance.....</b>	<b>236</b>
6.1 Redundant Line Control Function Troubleshooting Data to be Collected.....	236
6.1.1 Command to collect materials.....	236
6.1.2 Collecting Information by FJQSS (Information Collection Tool).....	242
6.1.3 Collecting packet traces.....	242
6.2 HUB maintenance.....	243
6.2.1 Swapping or Restarting HUB procedure (Fast switching mode / GS linkage mode).....	244
6.2.2 Swapping or Restarting HUB procedure (NIC switching mode / IP address remains unchanged).....	244
6.2.3 Swapping HUB procedure (NIC switching mode / IP address is changed).....	245
6.2.4 Swapping or Restarting HUB procedure (Virtual NIC mode / IP address remains unchanged).....	246
6.2.5 Swapping HUB procedure (Virtual NIC mode / IP address is changed).....	247
6.3 NIC maintenance.....	248
6.3.1 Shutdown maintenance for a NIC.....	249

6.3.2 Hot maintenance of NIC.....	251
6.3.2.1 Addition procedure.....	252
6.3.2.2 Removal procedure.....	253
6.3.2.3 Swapping procedure.....	254
<b>Chapter 7 Command references.....</b>	<b>260</b>
7.1 hanetconfig Command.....	260
7.2 strhanet Command.....	270
7.3 sphanet Command.....	272
7.4 dsphanet Command.....	274
7.5 hanetmask Command.....	276
7.6 hanetparam Command.....	279
7.7 hanetpoll Command.....	284
7.8 dsppoll Command.....	293
7.9 hanetnic Command.....	294
7.10 strptl Command.....	297
7.11 stppl Command.....	298
7.12 hanetpathmon Command.....	299
7.13 dsppathmon Command.....	304
7.14 hanetgw Command.....	305
7.15 hanetobserv Command.....	307
7.16 dspobserv Command.....	313
7.17 hanethvrsc Command.....	315
7.18 hanetbackup Command.....	319
7.19 hanetrestore Command.....	320
7.20 resethanet Command.....	321
<b>Appendix A Messages and corrective actions.....</b>	<b>323</b>
A.1 Messages Displayed by Redundant Line Control Function.....	323
A.1.1 Information message (number 0) .....	324
A.1.2 Error output message (numbers 100 to 700) .....	324
A.1.3 Console output messages (numbers 800 to 900).....	347
A.2 Messages Displayed in the Cluster System Logs.....	359
<b>Appendix B Examples of configuring system environments.....</b>	<b>362</b>
B.1 Example of configuring Fast switching mode (IPv4) .....	362
B.1.1 Example of the Single system.....	362
B.1.2 Example of the Single system in Logical virtual interface.....	365
B.1.3 Configuring virtual interfaces with tagged VLAN.....	368
B.1.4 Example of the Cluster system (1:1 Standby).....	373
B.1.5 Example of the Cluster system (Mutual Standby) .....	377
B.1.6 Example of the Cluster system (N:1 Standby) .....	381
B.1.7 Example of the Cluster system (Cascade) .....	386
B.2 Example of configuring NIC switching mode (IPv4).....	391
B.2.1 Example of the Single system without NIC sharing.....	391
B.2.2 Example of the Single system with NIC sharing.....	395
B.2.3 Example of the Single system in Takeover physical IP address (pattern II).....	398
B.2.4 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Synchronous switching).....	402
B.2.5 Configuring virtual interfaces with tagged VLAN (Logical IP takeover, Asynchronous switching).....	410
B.2.6 Configuring virtual interfaces with tagged VLAN (Physical IP takeover, Asynchronous switching).....	417
B.2.7 Example of the Single system without IP address setting of monitoring target.....	425
B.2.8 Example of the Cluster system (1:1 Standby).....	428
B.2.9 Example of the Cluster system (Mutual standby) without NIC sharing.....	431
B.2.10 Example of the Cluster system (Mutual standby) with NIC sharing.....	437
B.2.11 Example of the Cluster system in Takeover physical IP address (pattern I).....	441
B.2.12 Example of the Cluster system in Takeover physical IP address (pattern II).....	445
B.2.13 Example of the Cluster system (Cascade).....	448
B.2.14 Example of the Cluster system (NIC non-redundant).....	453

B.3 Example of configuring Virtual NIC mode (IPv4).....	457
B.3.1 Example of the Single system.....	457
B.3.2 Configuring virtual interfaces with tagged VLAN.....	459
B.3.3 Example of the Cluster system (1:1 Standby).....	464
B.3.4 Example of the Cluster system (Mutual Standby).....	466
B.3.5 Example of the Cluster system (Cascade).....	469
B.3.6 Example of the Cluster system (No IP takeover).....	473
B.4 Example of configuring Virtual NIC mode (IPv6).....	476
B.4.1 Example of the Single system.....	476
B.4.2 Example of the Cluster system (1:1 Standby).....	478
B.5 Example of configuring Virtual NIC mode (IPv4/IPv6).....	481
B.5.1 Example of the Single system.....	481
B.5.2 Example of the Cluster system (1:1 Standby).....	484
B.6 Example of configuring GS linkage mode.....	487
B.6.1 Example of the Single system.....	487
B.6.2 Example of the Single system on remote network.....	489
B.6.3 Example of the Single system (GS Hot-standby).....	492
B.6.4 Example of the Single system (GS Load Sharing).....	495
B.6.5 Example of the Cluster system (1:1 Standby).....	497
B.6.6 Example of the Cluster system on remote network(1:1 Standby).....	502
B.6.7 Example of the Cluster system (Mutual Standby).....	508
Appendix C Operation on the Virtual Machine Function.....	514
C.1 Virtual Machine Function Overview.....	514
C.2 Configuration of the Virtual Machine Function.....	514
C.3 Virtual Network Design in Virtual Machine Function.....	515
C.3.1 Concept of network configuration in the virtual machine function.....	515
C.3.2 Support set for each redundant line switching mode.....	515
C.3.3 Flow for selecting the virtual network configuration in each redundant line switching mode.....	516
C.3.4 Details on each configuration.....	516
C.4 Operation of Redundant Line Switching Mode on the Virtual Machine Function.....	518
C.4.1 Configuration for creating a highly reliable network of KVM guests on the KVM host (Configuration 1).....	518
C.4.2 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2).....	519
C.4.3 Configuration for creating a highly reliable network on each KVM guest of a cluster system (Configuration 3).....	520
C.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function.....	520
C.5.1 Setting up the virtual network on the host OS.....	521
C.5.2 Assigning the IP address, setting the transfer route and others (for host OS).....	521
C.5.3 Setting up GLS (for host OS).....	521
C.5.4 Sample configurations for the virtual bridge.....	521
C.5.5 Setting up GLS on guest domains (guest OSes).....	524
C.6 Examples of Configuration Setup.....	524
C.6.1 Setup example for creating a highly reliable network of guest domains on KVM hosts (Untagged VLAN).....	524
C.6.2 Setup example for creating a highly reliable network of guest domains on KVM hosts (Tagged VLAN).....	527
C.6.3 Setup example for creating a highly reliable network of guest domains on KVM hosts in a cluster system.....	529
Appendix D Operation on RHOSP.....	532
Appendix E Operation on VMware.....	533
E.1 VMware Overview.....	533
E.2 Configuration of VMware.....	533
E.3 Virtual Network Design in VMware.....	533
E.3.1 Concept of network configuration in VMware.....	533
E.3.2 Support set for each redundant line switching mode.....	534
E.4 Operation of Redundant Line Switching Mode on VMware.....	534
E.4.1 Configuration for creating a highly reliable network on guest OSes in a single system.....	534
E.4.2 Configuration for creating a highly reliable network on guest OSes in a cluster system.....	536
E.5 Setting up Redundant Line Switching Mode on VMware.....	536
E.6 Examples of Configuration Setup.....	536

E.6.1 Setup example for creating a highly reliable network of guest OSes.....	536
E.6.2 Setup example for creating a highly reliable network of guest OSes in a cluster system.....	537
E.6.3 Setup example in a cluster system (NIC non-redundant).....	537
Appendix F Operation on Hyper-V.....	541
F.1 Hyper-V Overview.....	541
F.2 Configuration of Hyper-V.....	541
F.3 Virtual Network Design in Hyper-V.....	541
F.3.1 Concept of network configuration in Hyper-V.....	541
F.3.2 Support set for each redundant line switching mode.....	542
F.4 Operation of Redundant Line Switching Mode on Hyper-V.....	542
F.4.1 Configuration for creating a highly reliable network on guest OSes in a single system.....	542
F.4.2 Configuration for creating a highly reliable network on guest OSes in a cluster system.....	544
F.5 Setting up Redundant Line Switching Mode on Hyper-V.....	544
F.6 Examples of Configuration Setup.....	544
F.6.1 Setup example for creating a highly reliable network of guest OSes.....	544
F.6.2 Setup example for creating a highly reliable network of guest OSes in a cluster system.....	545
F.6.3 Setup example in a cluster system (NIC non-redundant).....	545
Appendix G Cloning environment.....	547
G.1 Designing network of the copy destination system.....	547
G.1.1 Designing the network of Fast switching mode.....	548
G.1.2 Designing the network of NIC switching mode.....	548
G.1.3 Designing the network of Virtual NIC mode.....	549
G.1.4 Designing the network of GS linkage mode.....	550
G.2 Copying the system image.....	551
G.3 Changing the setting of the copy destination system.....	551
G.3.1 Preparations.....	551
G.3.2 Changing the IP address of the physical interface.....	552
G.3.3 Changing the IP address of the virtual interface.....	553
G.3.4 Changing the IP address of the monitoring destination and the remote host.....	556
G.3.5 Changing the static route information.....	557
G.3.6 Changing the setting of cluster application (in cluster operation).....	557
G.3.7 Enabling the changed setting.....	558
Appendix H Troubleshooting.....	559
H.1 Communication as expected cannot be performed (Common to IPv4 and IPv6).....	559
H.1.1 The route information set by a route command is deleted.....	559
H.1.2 Automatic address configuration lags behind for IPv6.....	559
H.1.3 Communication is not switched in the event of HUB monitoring error in Virtual NIC mode.....	559
H.2 Virtual interface or the various functions of Redundant Line Control Function cannot be used.....	561
H.2.1 An interface of NIC switching mode is not activated.....	561
H.2.2 The immediate automatic fail-back is not executed when the standby patrol is recovered in NIC switching mode.....	562
H.2.3 Error detection message displays for standby patrol in NIC switching mode.....	562
H.3 Failure occurs during operation (Common to both Single and Cluster system).....	563
H.3.1 Error messages(870) and corresponding actions for HUB monitoring.....	563
H.3.2 Error messages(875) and corresponding actions for standby patrol.....	566
H.3.3 Switching takes place in NIC switching mode regardless of failure at the monitoring end.....	570
H.3.4 Takes time to execute an operation command or to activate a cluster service.....	570
H.3.5 Unable to communicate using virtual IP addresses after configuring a firewall.....	571
H.3.6 Virtual driver hang detected by Self-checking function.....	572
H.4 Failure occurs during operation (In the case of a Cluster system).....	573
H.4.1 Node switching is not executed in Fast switching mode.....	573
H.5 Resuming connection lags after switching (Common to both Single and Cluster system).....	574
H.5.1 Recovery of transmission falls behind after switching to standby interface in NIC switching mode.....	574
H.6 Incorrect operation by the user.....	574
H.6.1 Accidentally deleted the virtual interface.....	574
H.6.2 Cluster applications are switched or stopped during maintenance work of network devices.....	575

Appendix I Check list.....	576
I.1 Checkpoint list.....	576
I.2 Setup common to modes.....	578
I.2.1 Network configuration.....	578
I.2.2 VLAN Setup.....	578
I.2.3 Redundant network configuration.....	579
I.2.4 Firewall settings.....	580
I.2.5 IP address settings.....	580
I.2.6 Subnet mask settings.....	582
I.2.7 Hostname settings.....	582
I.2.8 Distribution procedure after settings change.....	583
I.2.9 Procedure for network device maintenance.....	583
I.2.10 Network device rate settings.....	584
I.2.11 Application.....	584
I.3 Fast switching mode.....	585
I.3.1 Network address.....	585
I.3.2 Node configuration.....	585
I.4 NIC switching mode.....	586
I.4.1 Monitoring destination selection.....	586
I.4.2 Monitoring time adjustment.....	587
I.4.3 Network cable.....	587
I.4.4 Static route settings.....	587
I.5 Virtual NIC mode.....	588
I.5.1 Interface setting file.....	588
I.5.2 Monitoring destination selection.....	589
I.5.3 Monitoring time adjustment.....	589
I.5.4 Network cable.....	589
I.6 GS linkage mode.....	590
I.6.1 Network address.....	590
I.6.2 Communication target setting.....	593
I.6.3 Network device settings.....	594
I.6.4 Monitoring time adjustment.....	595
I.6.5 Maintenance procedure performed when the communication target stopped.....	596
I.6.6 PTF of the communication target.....	598
Appendix J Resident Process in GLS and Monitoring Target.....	599
Appendix K Changes from previous versions.....	600
K.1 Changes from Redundant Line Control function 4.0A20 to version 4.1A20.....	600
K.1.1 New command.....	600
K.1.2 Incompatible commands.....	600
K.1.3 Incompatible functions.....	602
K.2 Changes from Redundant Line Control function 4.1A20 to version 4.1A30.....	603
K.2.1 New command.....	603
K.2.2 Incompatible commands.....	603
K.2.3 Incompatible function.....	603
K.3 Changes from Redundant Line Control function 4.1A30 to version 4.1A40.....	605
K.4 Changes from Redundant Line Control function 4.1A40 to version 4.2A00.....	605
K.4.1 New command.....	605
K.4.2 Incompatible command.....	605
K.4.3 Incompatible function.....	605
K.5 Changes from Redundant Line Control function 4.2A00 to version 4.2A30.....	606
K.5.1 New commands.....	606
K.5.2 Incompatible command.....	606
K.5.3 Incompatible functions.....	606
K.6 Changes from Redundant Line Control function 4.2A30 to version 4.3A00.....	607
K.6.1 New command.....	608
K.6.2 Incompatible command.....	608

K.6.3 Incompatible functions.....	608
K.7 Functional Improvements in Redundant Line Control function 4.3A00.....	609
K.7.1 New command.....	610
K.7.2 Incompatible commands.....	610
K.7.3 Incompatible function.....	611
K.8 Changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10.....	613
K.8.1 New commands.....	614
K.8.2 Incompatible commands.....	615
K.8.3 Incompatible functions.....	617
K.9 Changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20.....	619
K.9.1 New command.....	620
K.9.2 Incompatible command.....	620
K.9.3 Incompatible functions.....	620
K.10 Changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30.....	621
K.10.1 New command.....	621
K.10.2 Incompatible command.....	621
K.10.3 Incompatible functions.....	622
K.11 Changes from Functional Improvements in Redundant Line Control function 4.3A30 to 4.3A40.....	623
K.11.1 New command.....	623
K.11.2 Incompatible commands.....	623
K.11.3 Incompatible function.....	624
K.12 Changes from Functional Improvements in Redundant Line Control function 4.3A40 to 4.4A00.....	624
K.12.1 New command.....	624
K.12.2 Incompatible commands.....	625
K.12.3 Incompatible functions.....	626
K.13 Changes from Functional Improvements in Redundant Line Control function 4.4A00 to 4.5A00.....	629
K.13.1 New command.....	629
K.13.2 Incompatible commands.....	629
K.13.3 Incompatible functions.....	633
K.14 Changes from Functional Improvements in Redundant Line Control function 4.5A00 to 4.5A10.....	635
K.14.1 New command.....	635
K.14.2 Incompatible commands.....	635
K.14.3 Incompatible function.....	635
K.15 Changes from Functional Improvements in Redundant Line Control function 4.5A10 to 4.6A00.....	636
K.15.1 New command.....	636
K.15.2 Incompatible command.....	636
K.15.3 Incompatible function.....	636
K.15.4 Specification changes for RHEL8.....	636
K.16 Changes from Functional Improvements in Redundant Line Control function 4.6A00 to 4.6A10.....	638
K.17 Changes from Functional Improvements in Redundant Line Control function 4.6A10 to 4.6A20.....	638
K.18 Changes from Functional Improvements in Redundant Line Control function 4.6A20 to 4.7A00.....	638
K.18.1 Incompatible function.....	638
K.18.2 Specification changes for RHEL9.....	639
Glossary.....	640
Index.....	645

# Chapter 1 Overview

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

## 1.1 What is redundant line control?

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

The redundant line control function provides the following four network control methods:

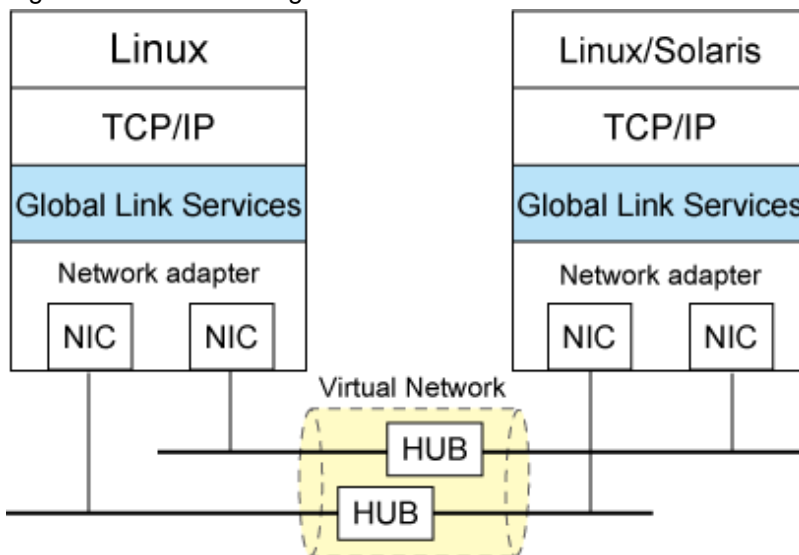
### Fast switching mode

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 transfer path that is not multiplexed. For details, refer to "[2.2.4 Configuring single physical interface](#)".

Figure 1.1 Fast switching mode



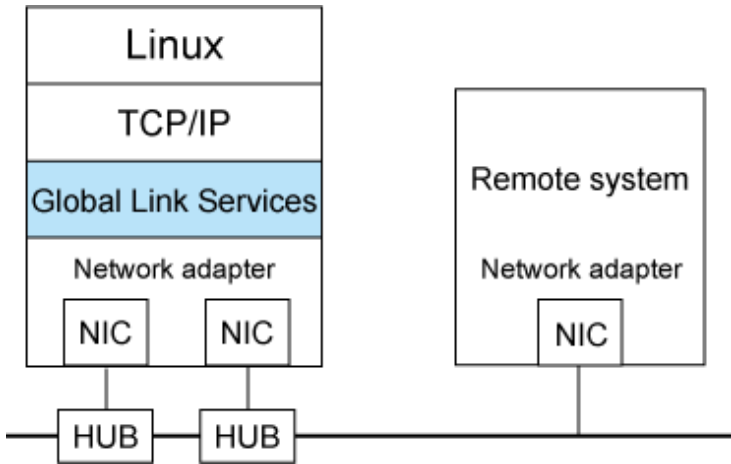
### NIC switching mode

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 NIC that is not multiplexed. For details, refer to "[2.2.4 Configuring single physical interface](#)".

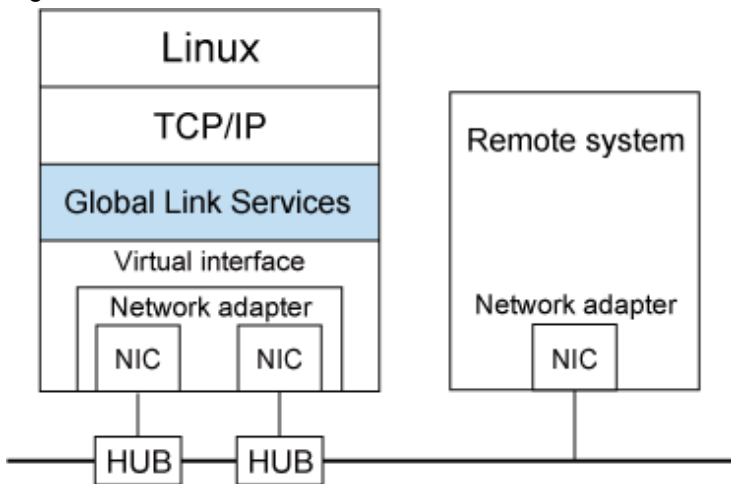
Figure 1.2 NIC switching mode



**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 NIC that is not multiplexed. For details, refer to "2.2.4 Configuring single physical interface".

Figure 1.3 Virtual NIC mode



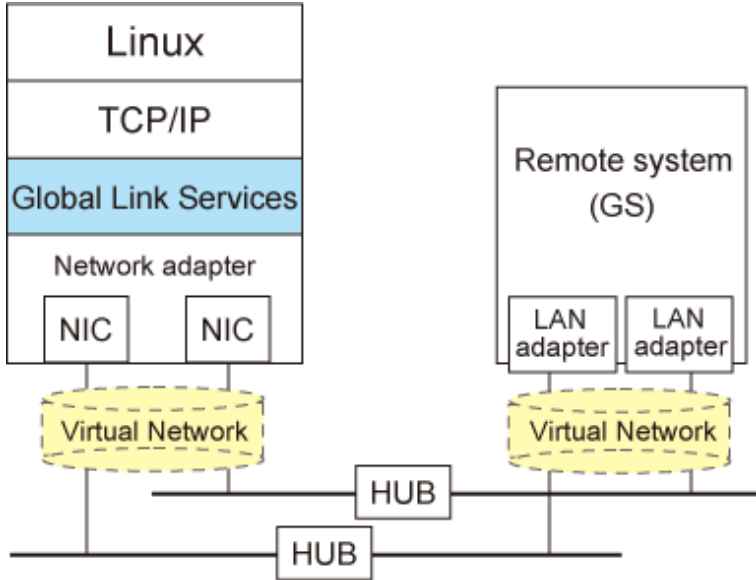
**GS linkage mode**

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 NIC that is not multiplexed. 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)

Function		Redundant line switching mode	
		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. If the transmission route is not multiplexed, used the route as it is active.
Fault monitoring	Detectable failures	NIC, cable, switch/HUB, remote host (system down etc.)	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.
	Failure detection time	5 to 10 seconds (Default)	Monitoring can be done by combining the following 2 monitoring functions. <ul style="list-style-type: none"> <li>- Monitors switch/HUB using the ping command: If there is no response for a certain period of time, a transmission route failure will be detected.</li> <li>- Monitors link status of NIC: If the NIC is link down, a transmission route failure will be detected.</li> </ul>
			- When an error is detected by ping: 22 to 27 seconds (Default)

Function			Redundant line switching mode	
			Fast switching mode	NIC switching mode
				<ul style="list-style-type: none"> <li>- When a NIC link down is detected: Using ping monitoring at the same time: 2 to 7 seconds (Default) Using ping monitoring not at the same time: 1 to 6 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.	
	Recovery detection time	1 to 5 seconds (Default)	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	IPv4 address	

GLS: Global Link Services

Table 1.2 Function comparison (2)

Function		Redundant line switching mode		
		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	<ul style="list-style-type: none"> <li>- When a NIC link down is detected (Link status monitoring): About 1 second</li> <li>- Network monitoring: 14 to 17 seconds (Default)</li> </ul>	25 to 30 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.	If a failed transmission route is recovered, it will automatically join communication.

Function		Redundant line switching mode	
		Virtual NIC mode	GS linkage mode
		Manual rejoining is also allowed with the operational command.	Manual rejoining is not supported.
Conditions	Remote hosts	Arbitrary host	GS (Global Server), PRIMEQUEST, PRIMERGY
	IP addresses	IPv4 address, IPv6 address	IPv4 address

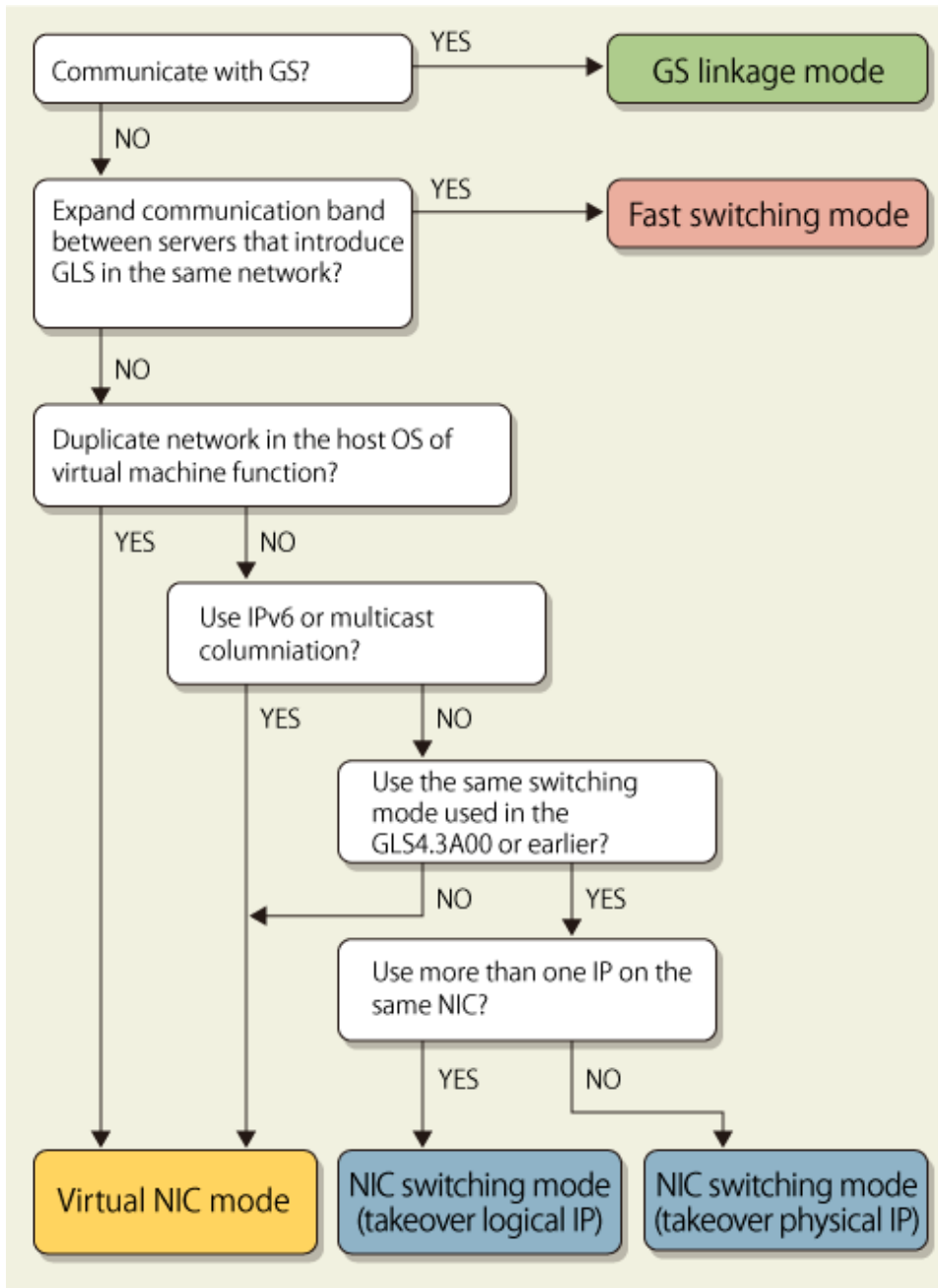
## 1.1.2 Criteria for selecting redundant line control methods

---

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



GLS: Global Link Services

## 1.2 Redundant line control effects

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

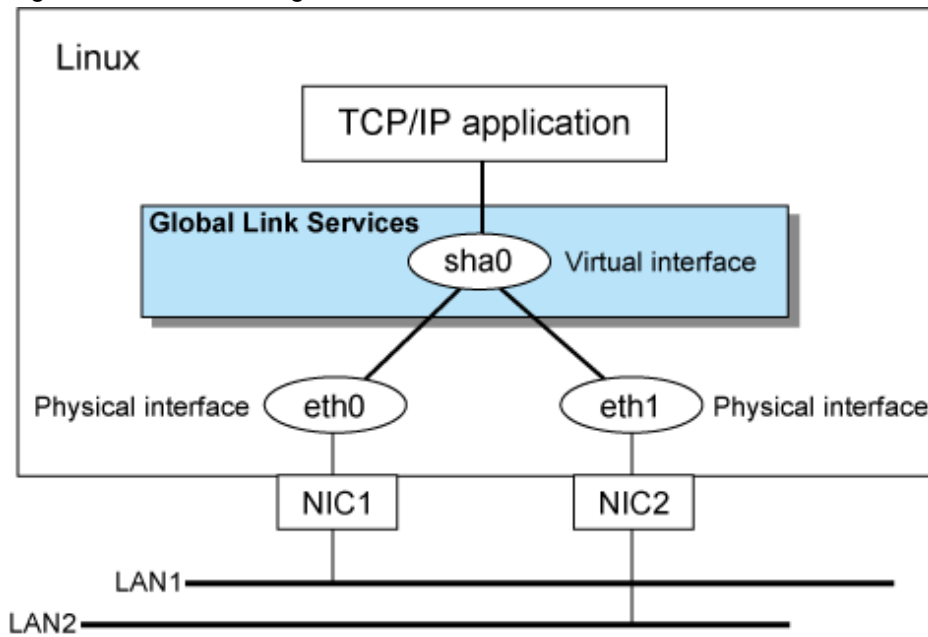
## 1.3 System Configuration

### Note

This version does not support IPv6 addresses for the Fast switching mode and NIC switching mode.

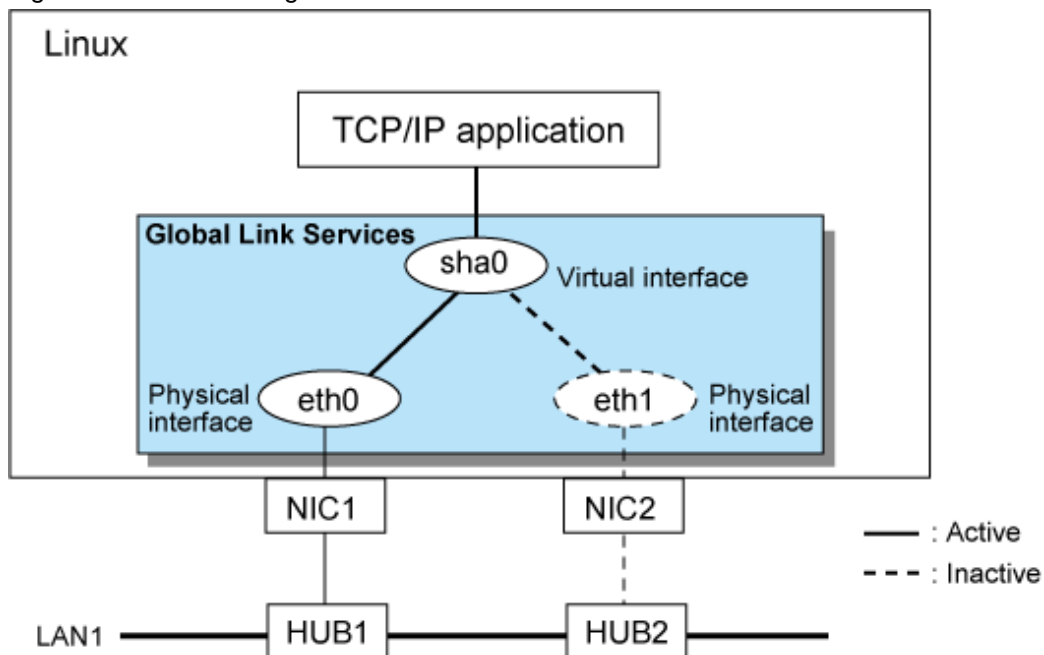
### Fast switching mode

Figure 1.6 Fast switching mode



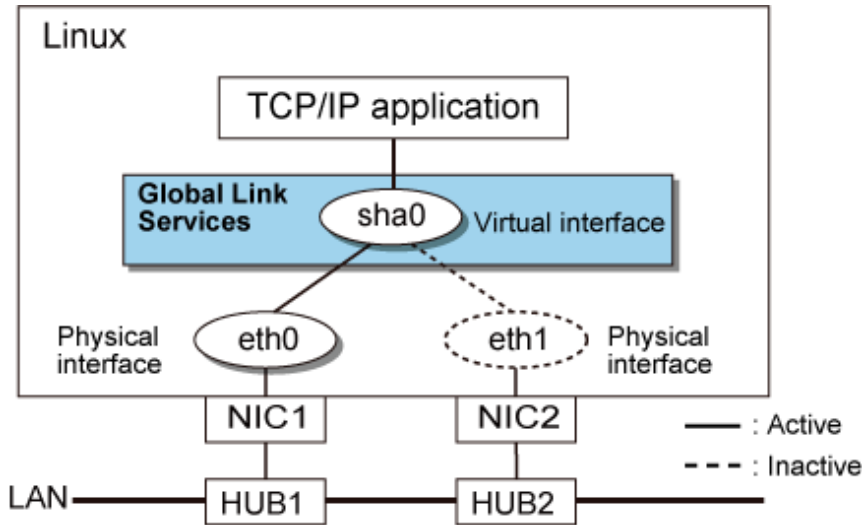
### NIC switching mode

Figure 1.7 NIC switching mode



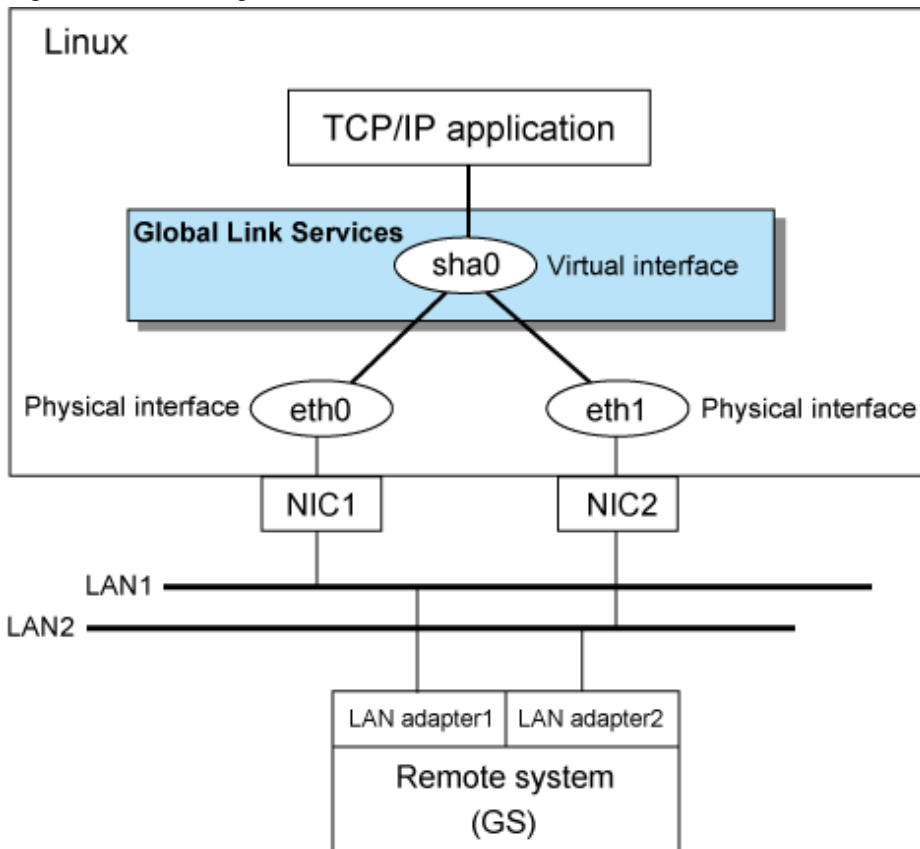
### Virtual NIC mode

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 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 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.
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



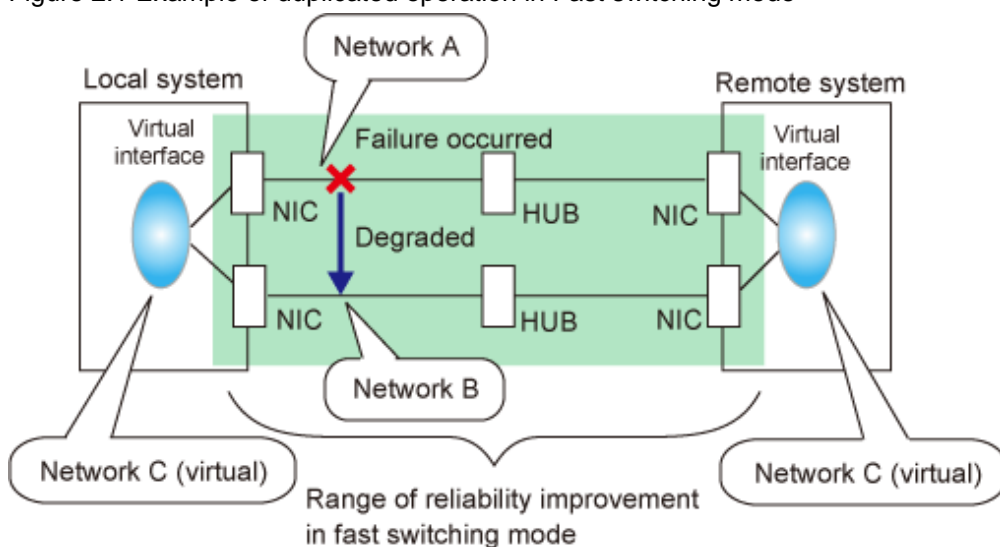
Note

This version does not support IPv6 addresses for the 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.

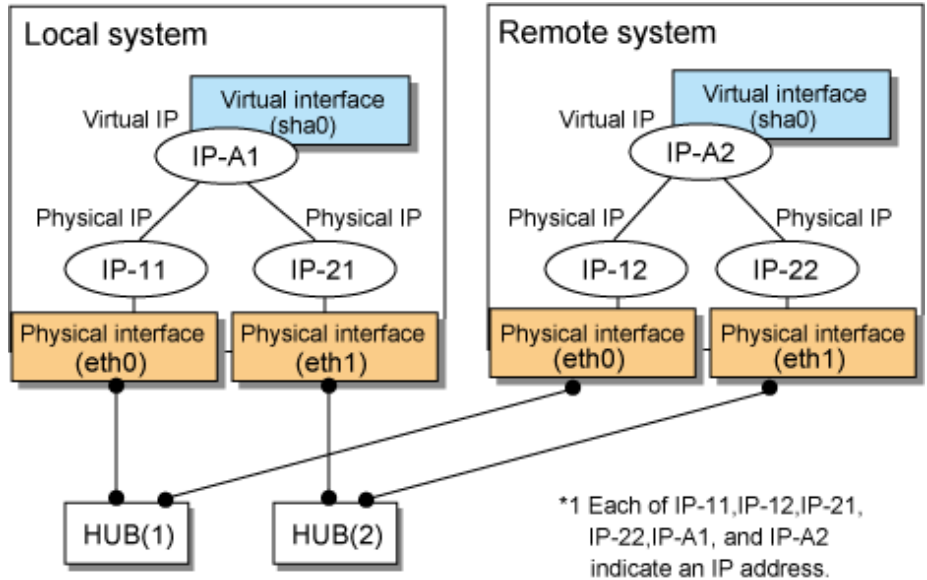
#### Recommended application areas

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

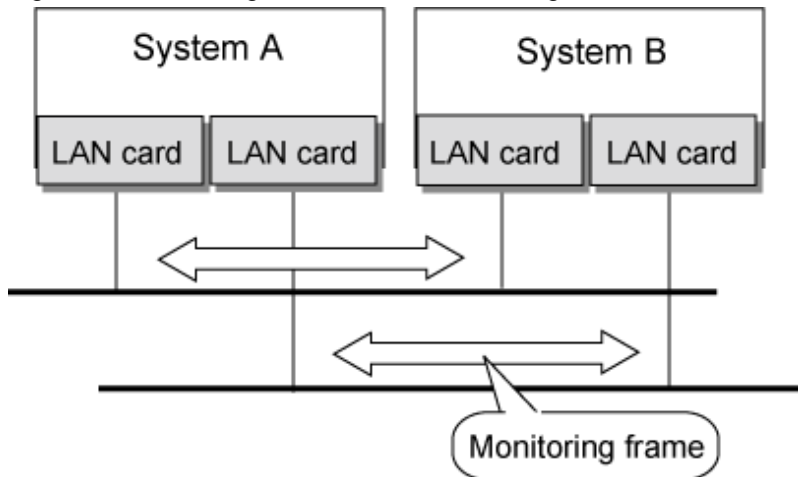
Indicates a source IP address to be allocated to the virtual interface for communication with the remote hosts. Available IP addresses are IPv4 and IPv6 address.

### 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.

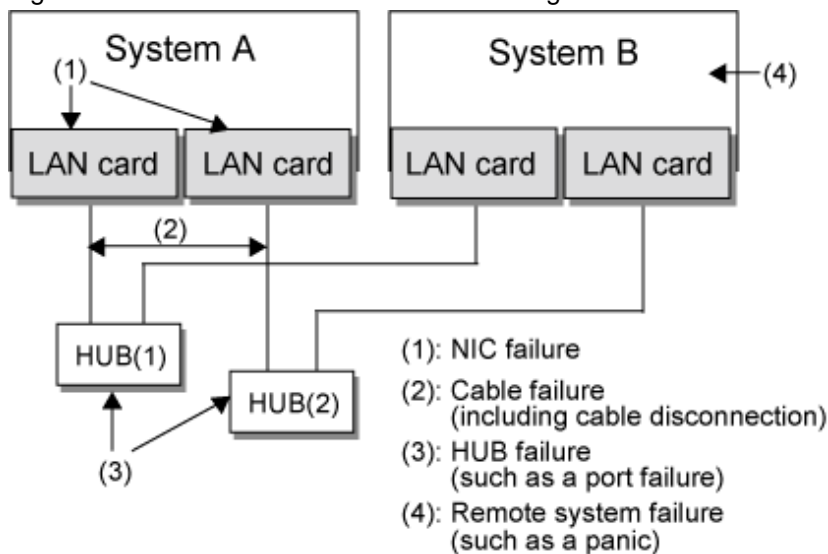
#### Switching time

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

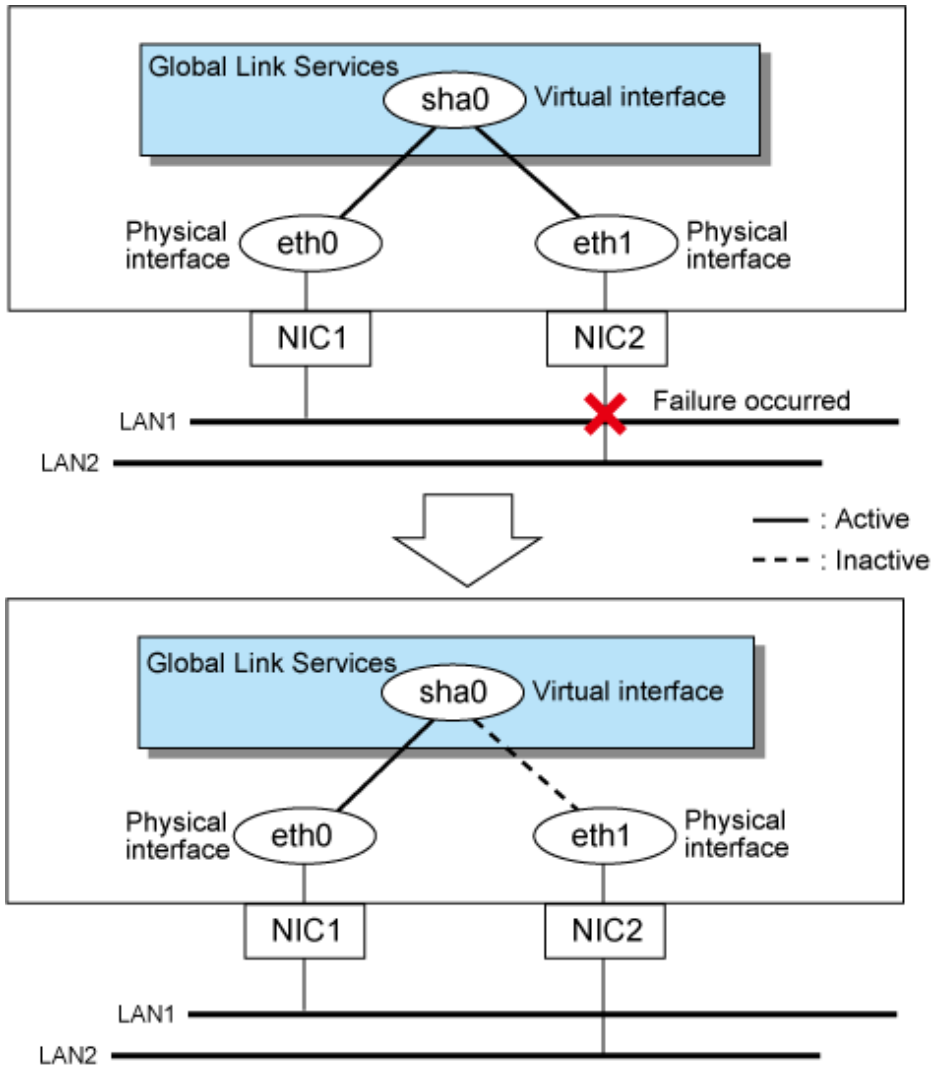
Monitoring is started automatically when the virtual interface is activated. Monitoring is automatically stopped when the virtual interface is inactivated. In cluster operation, the system allows each node to be started or stopped independently.

### 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

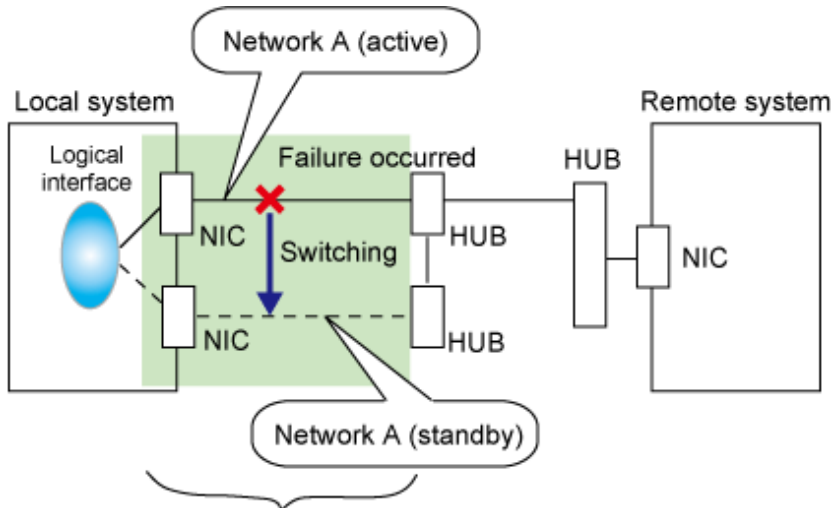


#### Note

This version does not support IPv6 addresses for the 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



Range of reliability improvement in NIC switching mode



#### Information

The NIC switching mode handles the logical interface as a takeover interface. Note that it is possible to take over the physical interface without using the logical interface. For details, see "[2.1.2.2 Switching function](#)".

When using the physical interfaces eth0 and eth1, the takeover interfaces are displayed as the secondary addresses of eth0 and eth1 by the ip command.

#### 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.

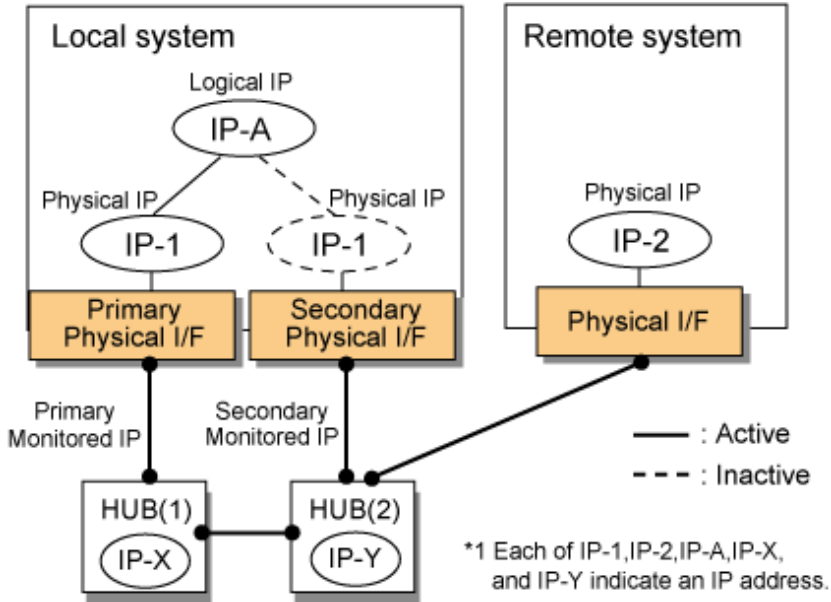
## Recommended application areas

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

In the NIC switching mode, the transmission route is monitored in the following two functions.

- Ping response 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").

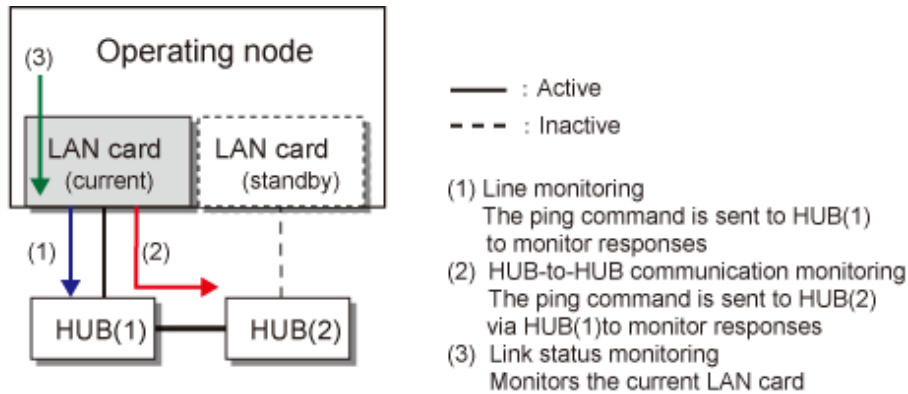
- Link status monitoring

Monitors the link status for the NIC currently operating.

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



#### Fault detection time

The fault detection time will be one of the following:

- The fault detection time by ping response monitoring  
 [monitoring interval (sec) x monitoring count (count)]
- The fault detection time by link status monitoring  
 [1 (sec) + (0 to monitoring interval (sec))]

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 HUB monitoring function detects failure 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 (count)], the time set for linkup is ignored and the time set by this [monitoring interval (sec) x monitoring count (count)] is adopted.

Figure 2.9 Fault detection time by ping response monitoring for NIC switching mode

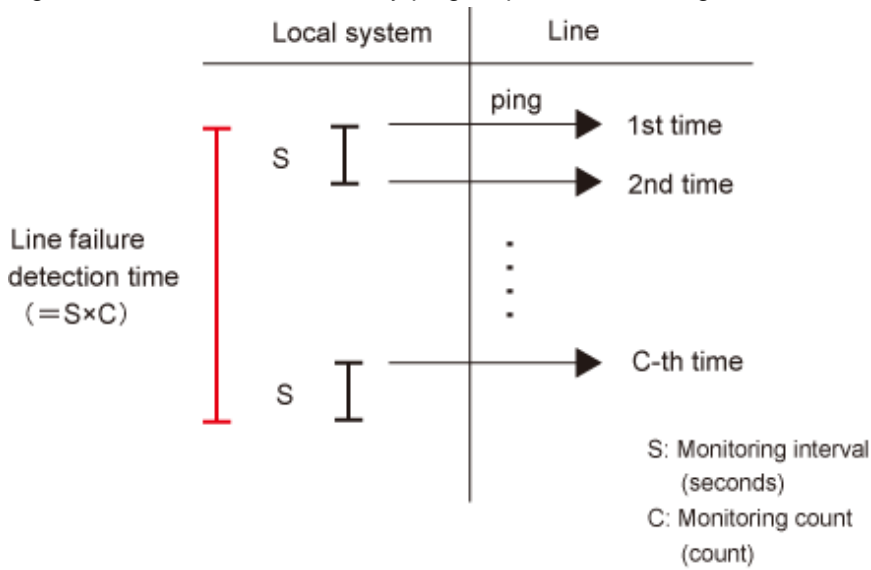
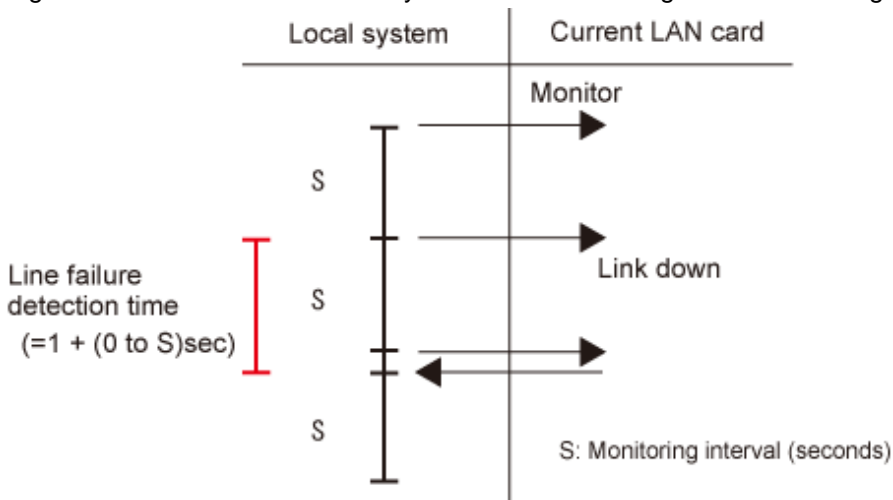


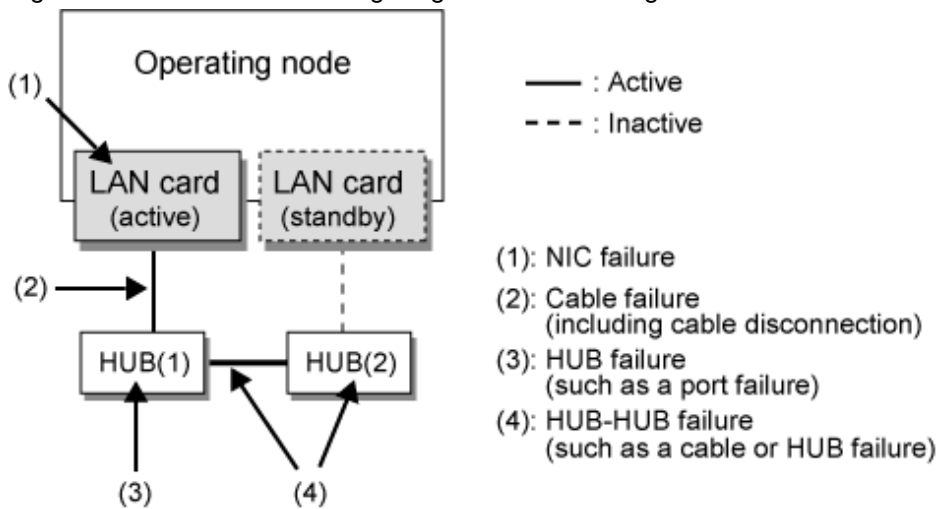
Figure 2.10 Fault detection time by link status monitoring for NIC switching mode



Detectable failures

The following failures can be detected:

Figure 2.11 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.

(4) is the monitoring range only when HUB-HUB monitoring is enabled.

#### 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

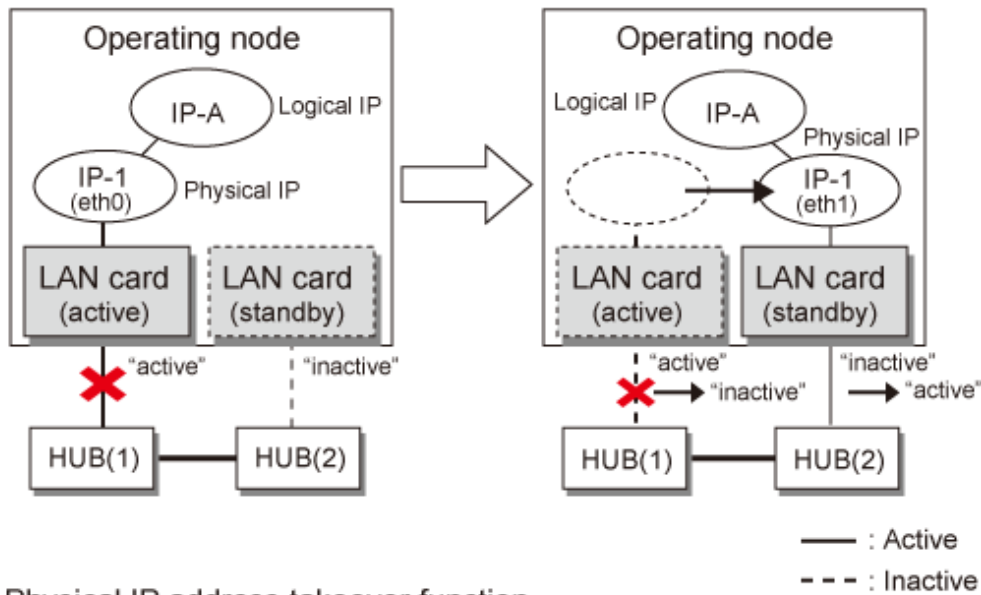
Switching operation changes the status of an active NIC into "inactive" state and then changes the status of standby NIC to "active" so that standby NIC can run as a new active device. At this point, the MAC address and IP addresses (physical IP and logical IP) are taken over and then an ARP request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

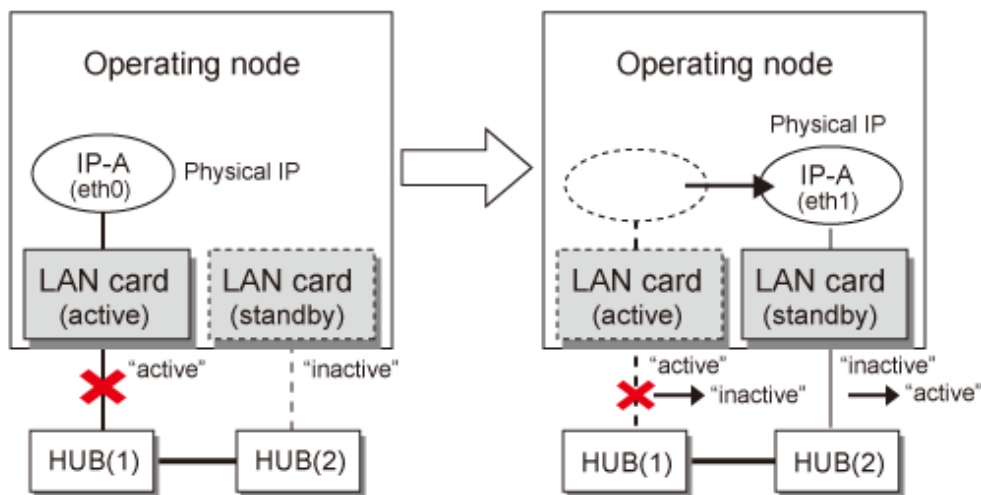
[Figure 2.12 Outline of switching operation performed when a failure occurs in NIC switching mode](#) shows an example of node internal switching.

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 2.12 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

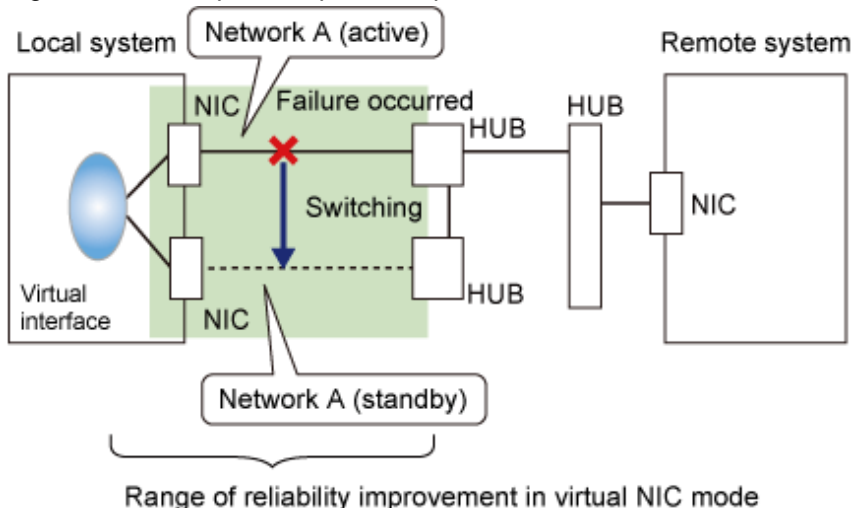
- If assigning IPv4 address to the virtual interface, physical IP address must be assigned to the redundant primary interface.
- No multi-cast IP address can be used.
- If a UDP application uses a virtual IP address of GLS, you have to be cautious about the following points.
  - If, when switching NICs, 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 2.13 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.

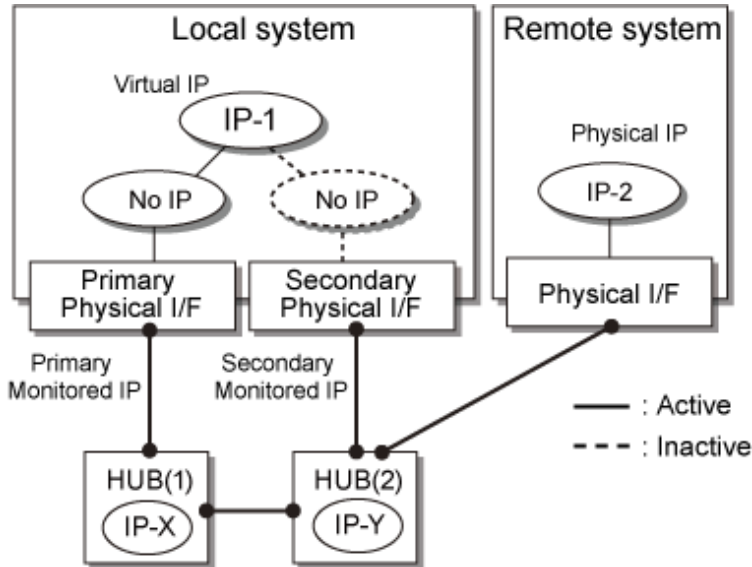
## Recommended application areas

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 2.14 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.

## Point

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.

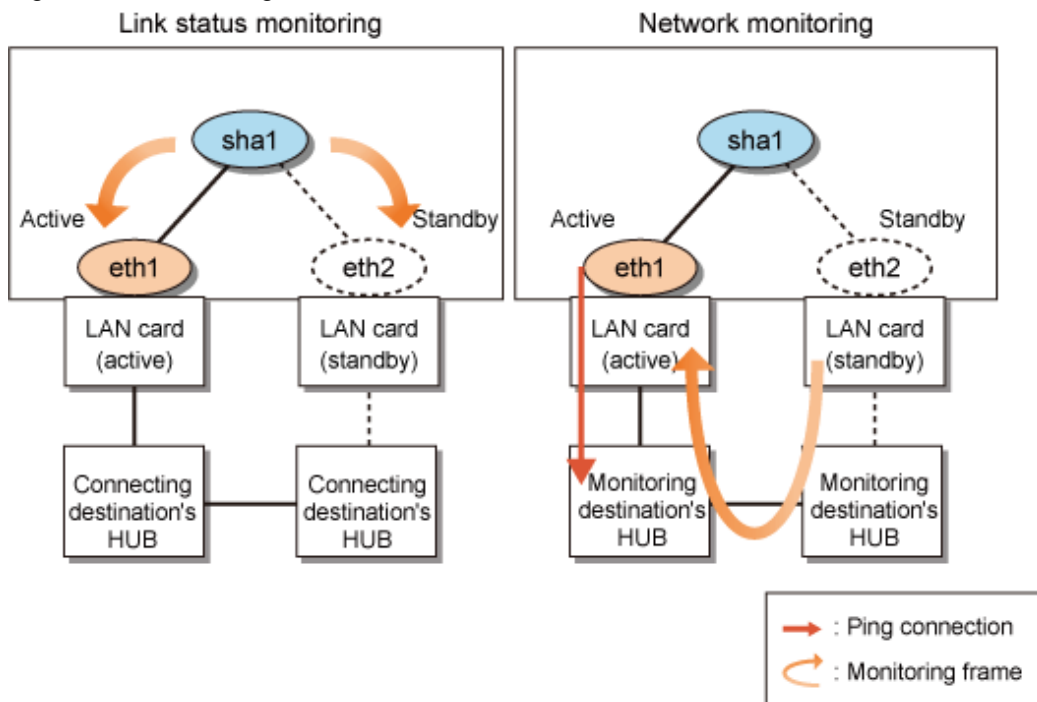
- Network monitoring function

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 2.15 Monitoring method in Virtual NIC mode



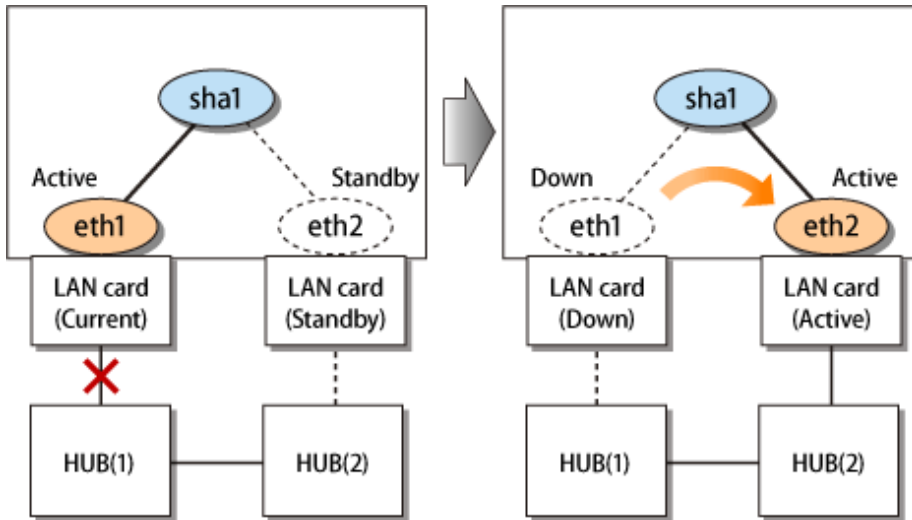
### 2.1.3.2 Switching function

#### 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 2.16 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 2.17 Example of duplicated operation in GS linkage mode

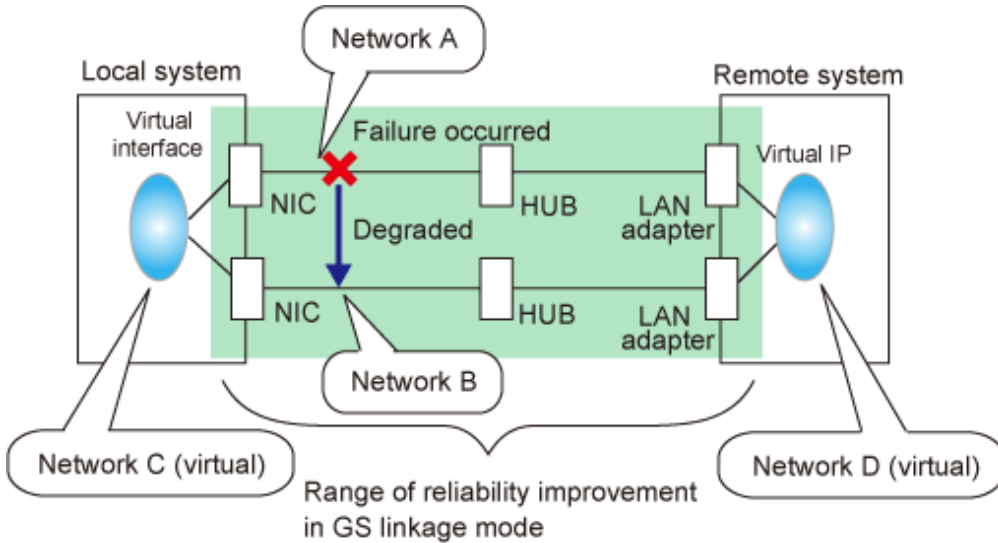
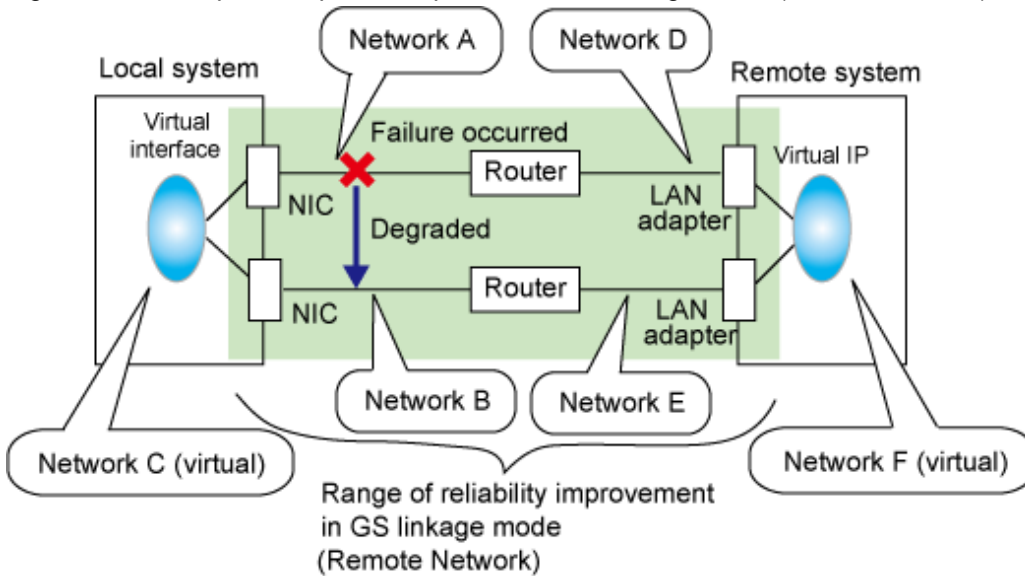


Figure 2.18 Example of duplicated operation in GS linkage mode (Remote network)



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 2.19 System configuration in GS linkage mode and Figure 2.20 System configuration in GS linkage mode show a system configuration of GS linkage mode.

Figure 2.19 System configuration in GS linkage mode

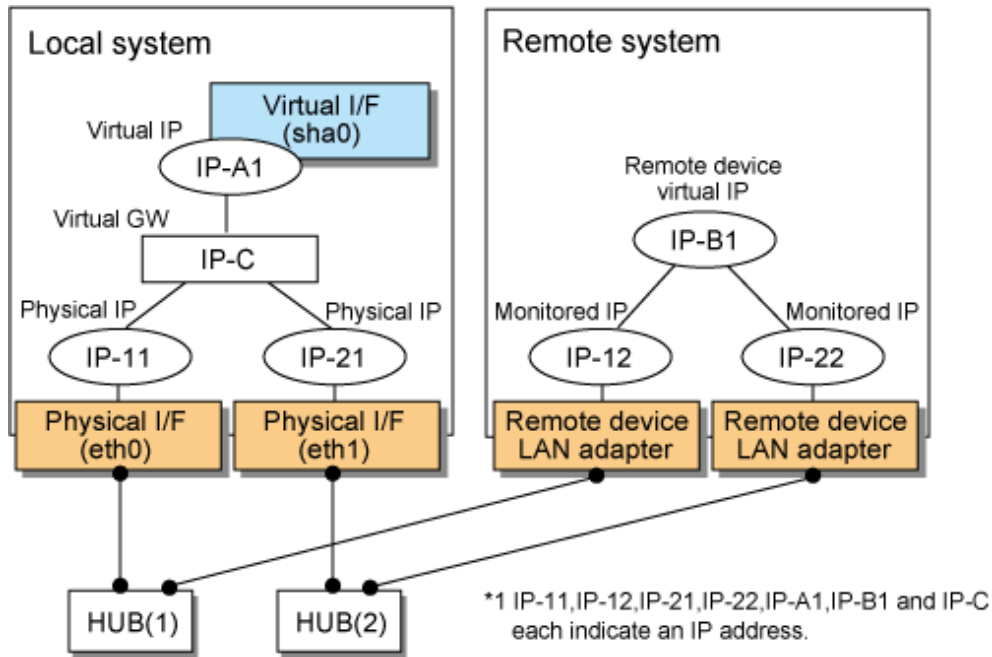
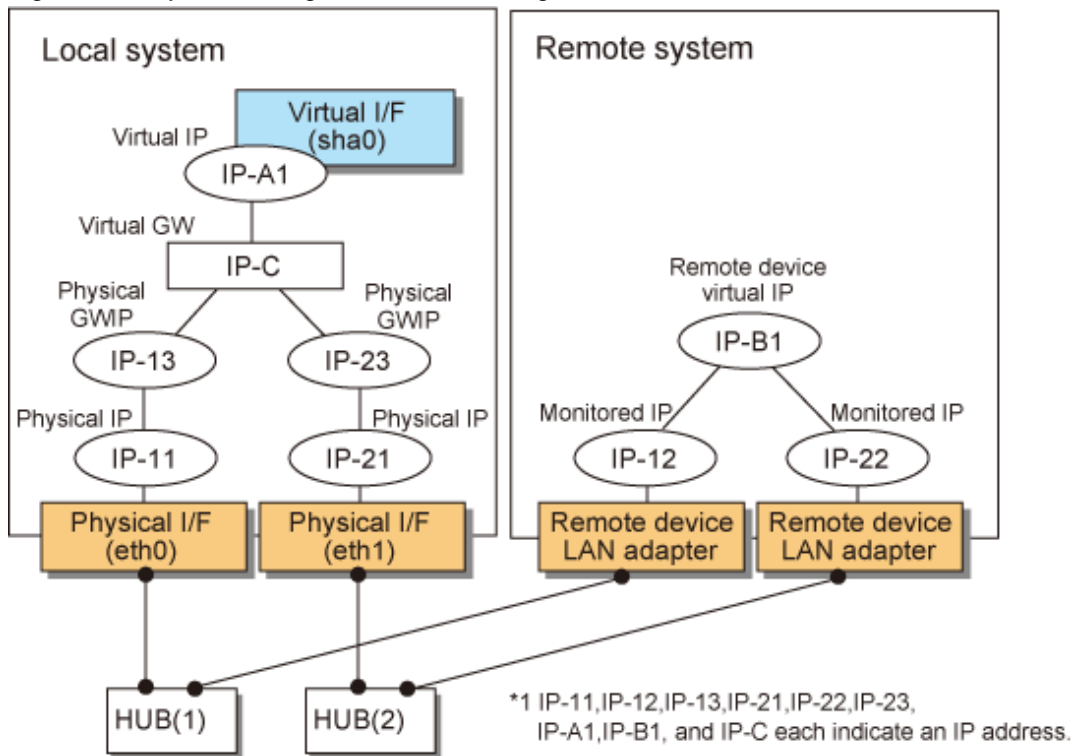


Figure 2.20 System configuration in GS linkage mode



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

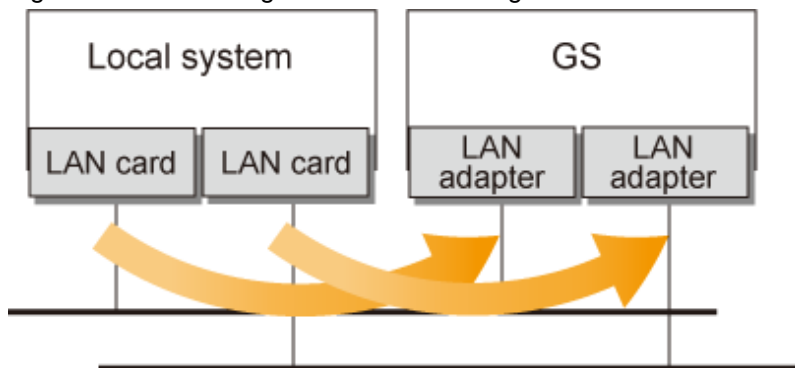
Indicates a virtual IP of the remote device with which communication should be carried out. IPv4 address can be used for a physical interface. IPv6 addresses cannot be used.

## 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 2.21 Monitoring method in GS linkage mode



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

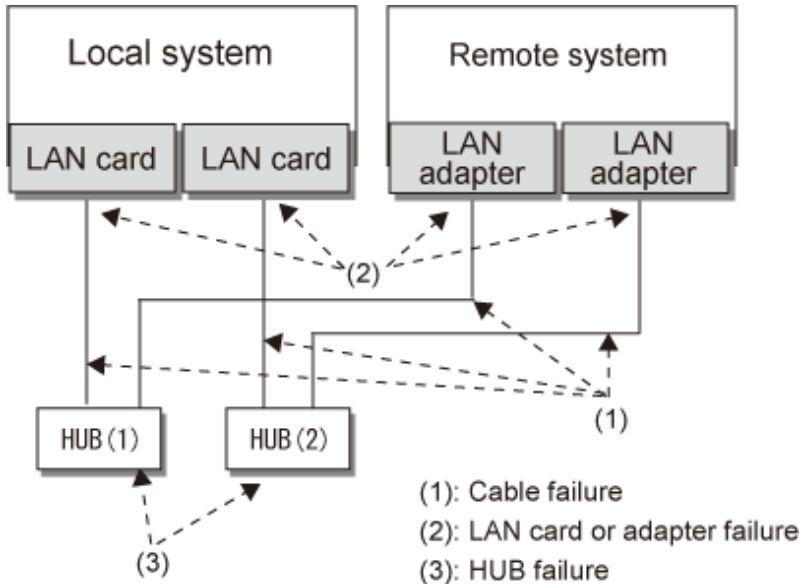
### Fault detection time

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

### Detectable failures

The following failures can be detected:

Figure 2.22 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

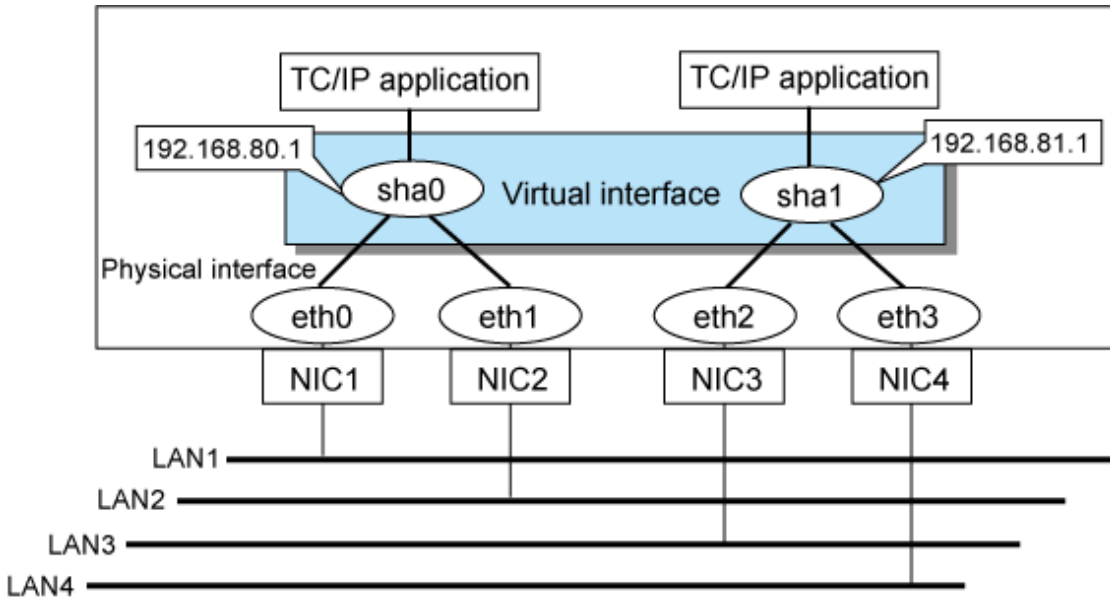
### 2.2.1 Configuring multiple virtual interfaces

---

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.

Figure 2.23 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 2.23 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

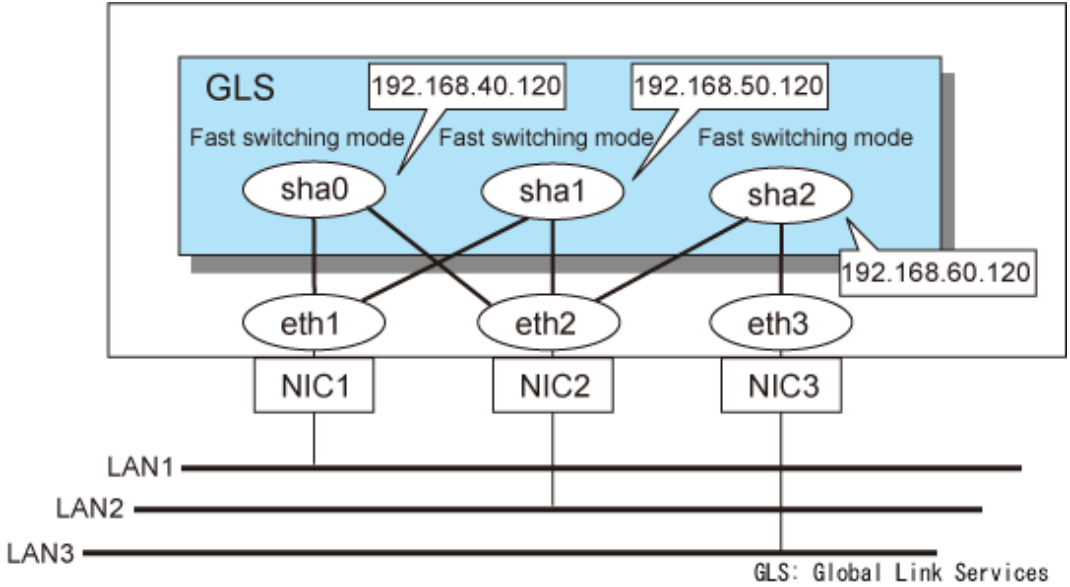
One portion or entire physical interfaces can be shared by the virtual interfaces which institute Fast switching mode. Though, it is not possible to share the physical interface and virtual interface of NIC switching mode and GS linkage mode.

#### Note

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

Figure 2.24 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 2.24 Example of sharing physical interface (1)



### 2.2.2.2 Using NIC switching mode

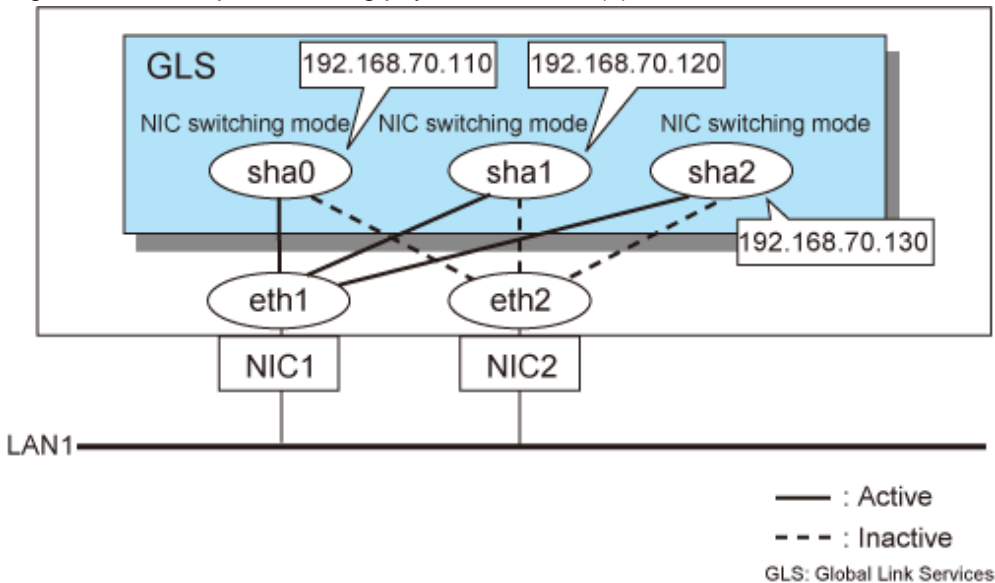
Within several virtual interfaces of NIC switching mode (logical IP takeover), if all the name of the physical interfaces and the value of the physical IP addresses are equivalent, then it is possible to share the physical interface. Sharing a portion of physical interface is not allowed. Nevertheless, 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 2.25 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 2.25 Example of sharing physical interface (2)



### 2.2.2.3 Using GS linkage mode

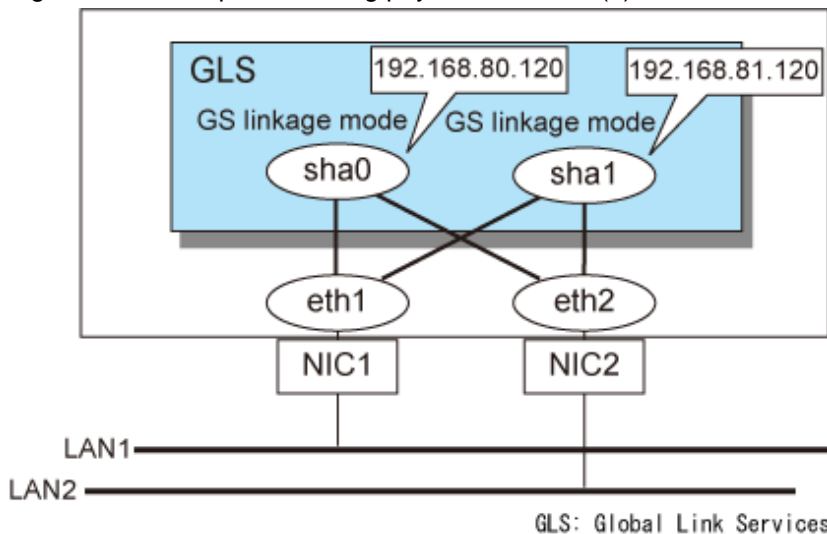
Within several virtual interfaces of GS linkage mode, it is possible to share the physical interface. Sharing a portion of physical interface is not allowed. Nevertheless, sharing physical interface with the virtual interface is not possible for Fast switching mode and NIC switching mode.

#### Note

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

Figure 2.26 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 2.26 Example of sharing physical interface (3)



### 2.2.3 Configuring multiple logical virtual interfaces

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

#### Note

Virtual IP addresses allocated to the logical virtual interfaces must be on the same subnet as the virtual interfaces.

As shown in Figure 2.27 Logical virtual interfaces being defined, when defining two logical virtual interfaces (sha0:2 and sha0:3) on a virtual interface sha0, you must configure the IP address of the same subnet on sha0, sha0:2, and sha0:3.

#### Information

When configuring logical virtual interfaces (two logical virtual interfaces, sha0:2 and sha0:3, in Figure 2.27 Logical virtual interfaces being defined) on a virtual interface sha0, the logical virtual interfaces are displayed as the secondary addresses of sha0 by the ip command.

An example of a display is as follows:

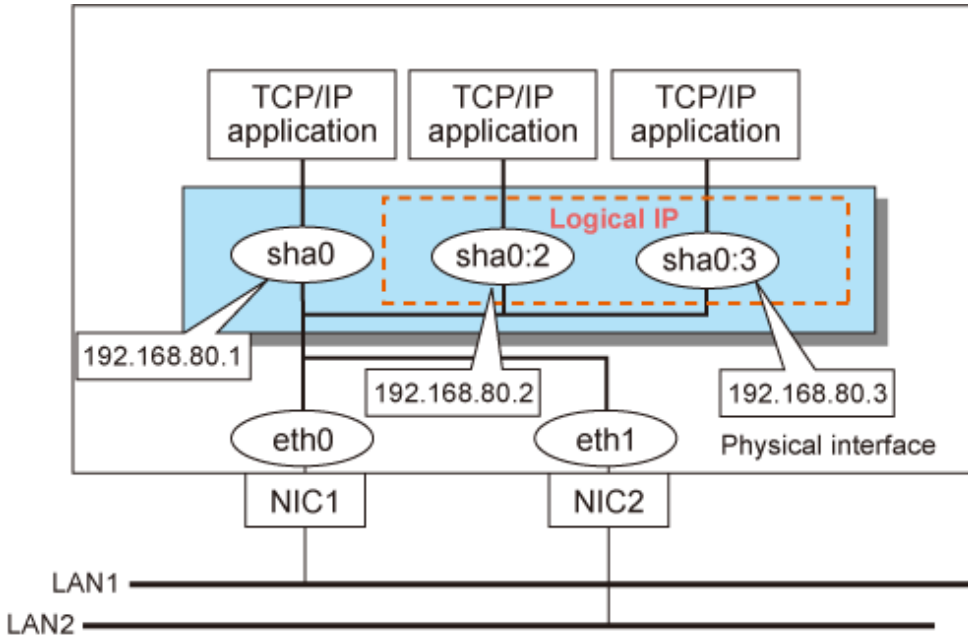
```
# ip addr show sha0
N: sha0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.1/24 brd 192.168.80.255 scope global sha0
        valid_lft forever preferred_lft forever
    inet 192.168.80.2/24 brd 192.168.80.255 scope global secondary sha0
        valid_lft forever preferred_lft forever
```

```

inet 192.168.80.3/24 brd 192.168.80.255 scope global secondary sha0
valid_lft forever preferred_lft forever

```

Figure 2.27 Logical virtual interfaces being defined

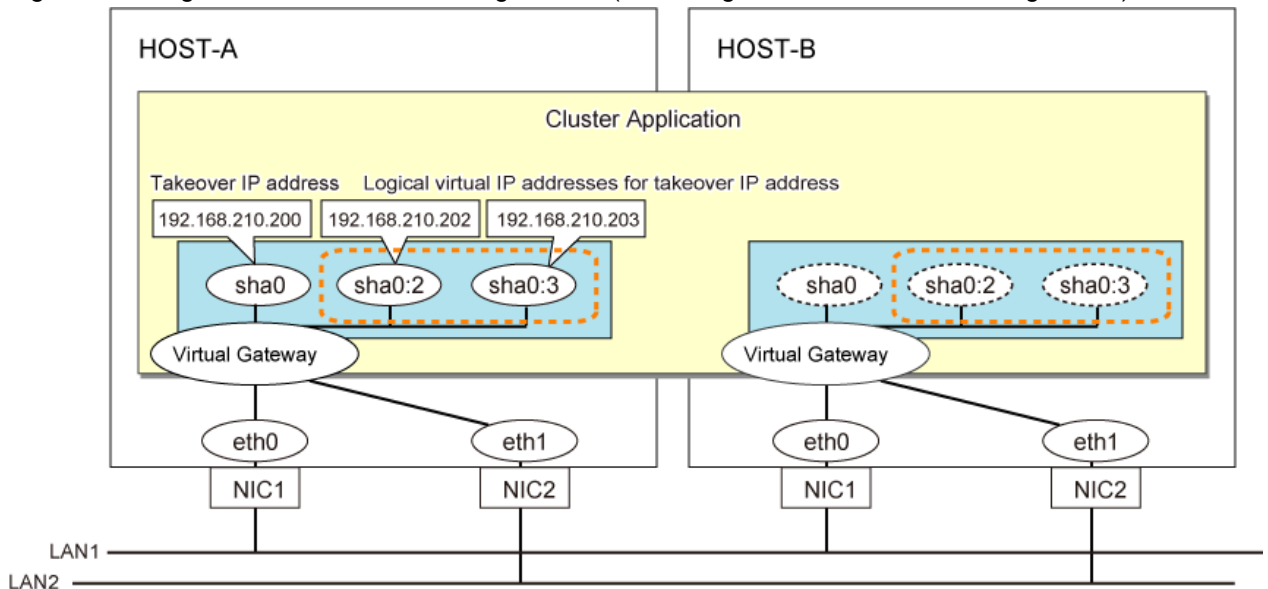



The total number of interfaces can be created as a logical virtual interface is 63 (from 2 to 64). The logical virtual interfaces greater than 65 will be used as takeover virtual interface upon Cluster configuration.

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



 Logical virtual IP addresses are started and stopped in conjunction with a takeover IP address.

## Note

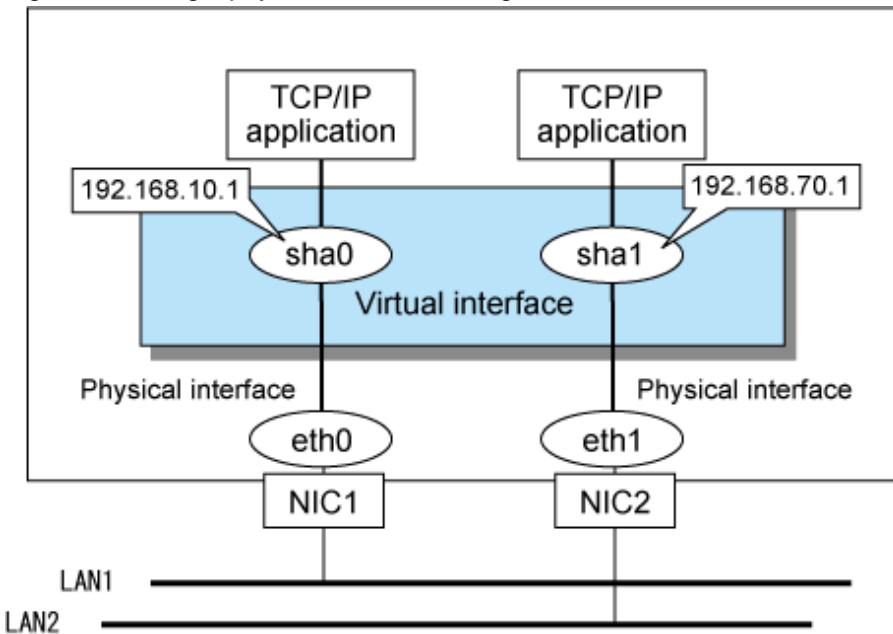
- This function is only available for the Fast switching mode, the Virtual NIC mode, and the GS linkage mode.
- For the NIC switching mode, if using the physical interface sharing function, it can process (a process of allocating multiple IP addresses to one physical interface) equally as this function.
- For the Virtual NIC mode in RHEL8, set the logical virtual interfaces as the secondary addresses of `/etc/sysconfig/network-scripts/ifcfg-sha0`. For RHEL9, set them as additional addresses with the `nmcli` command.  
You do not need to create the OS definition file (`/etc/sysconfig/network-scripts/ifcfg-sha0:2`, etc.).

## 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 2.29 Single physical interface configuration shows an example of single physical interface configuration.

Figure 2.29 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.

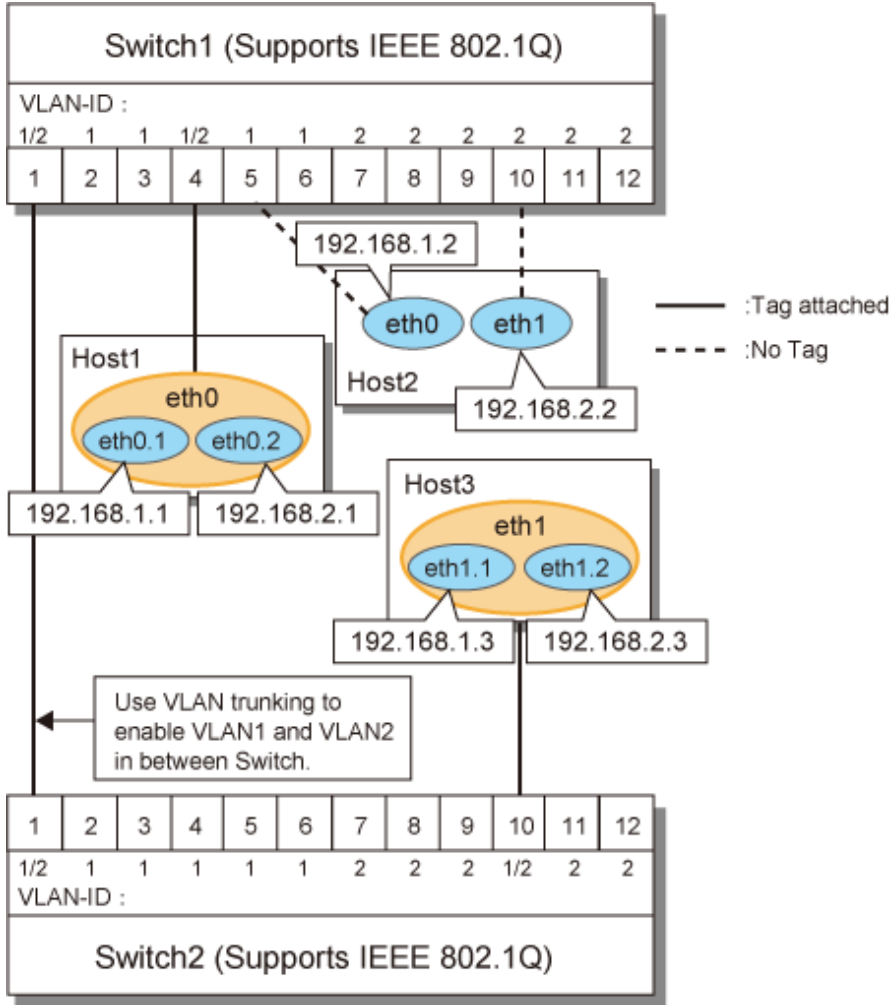
## 2.2.5 Configuring Tagged VLAN interfaces

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 2.30 Network structure using Tagged VLAN



In Figure 2.30 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 2.31 Using Tagged VLAN Interface architecture in NIC switching mode

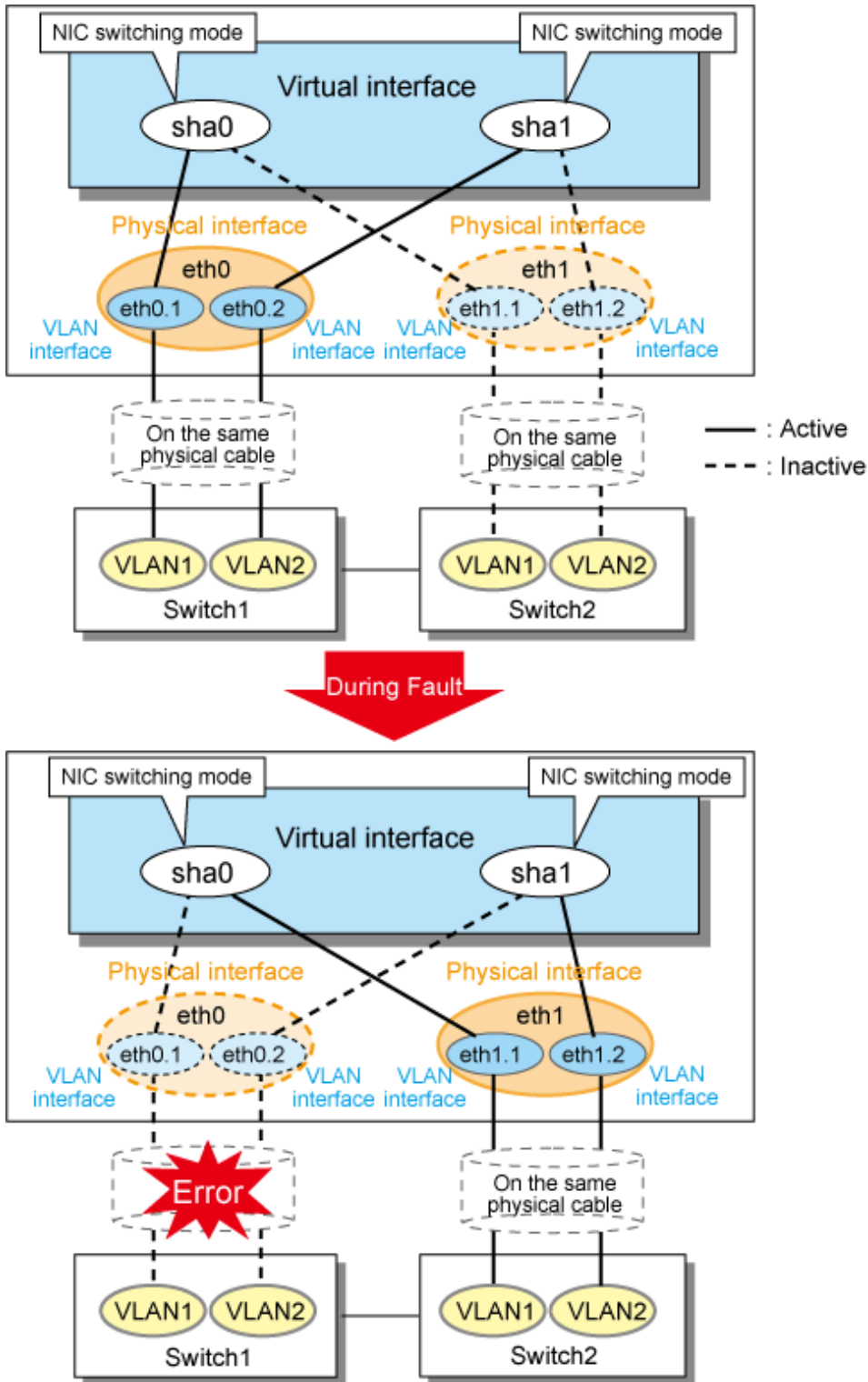
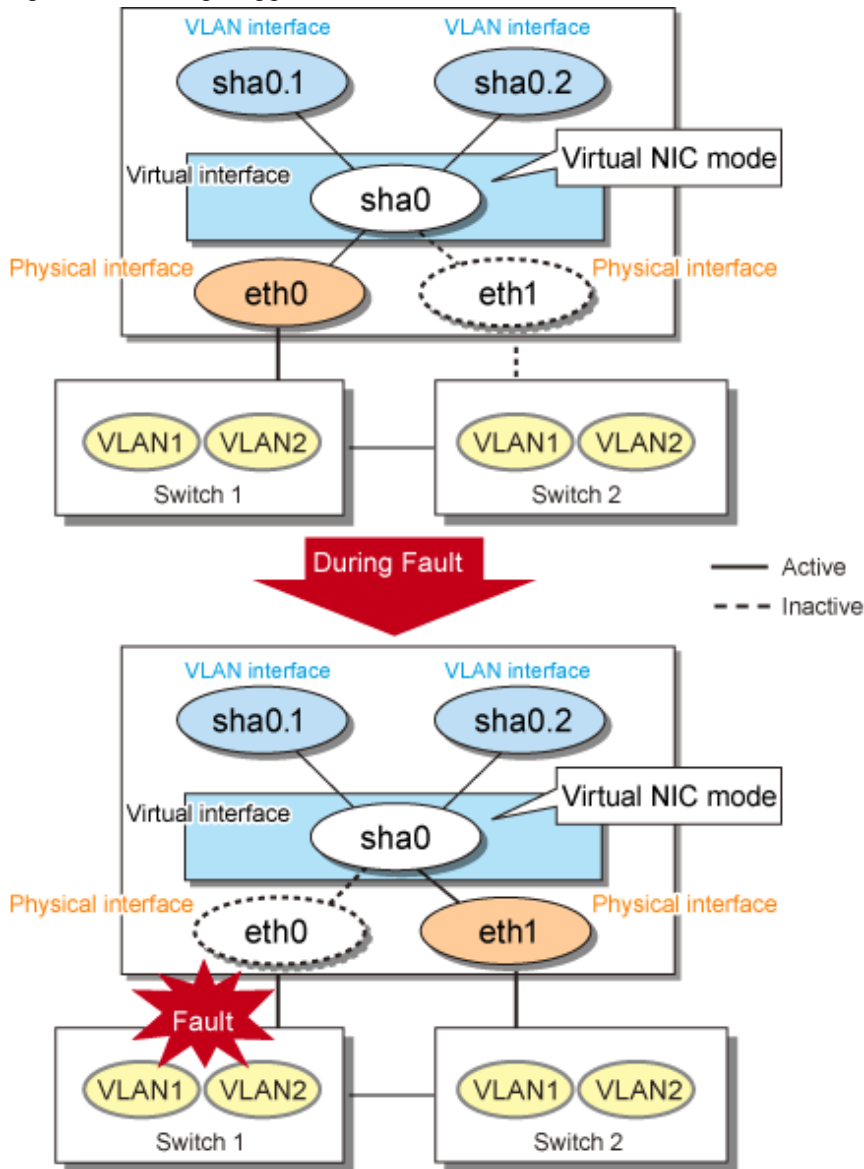


Figure 2.32 Using Tagged VLAN Interface architecture in Virtual NIC mode

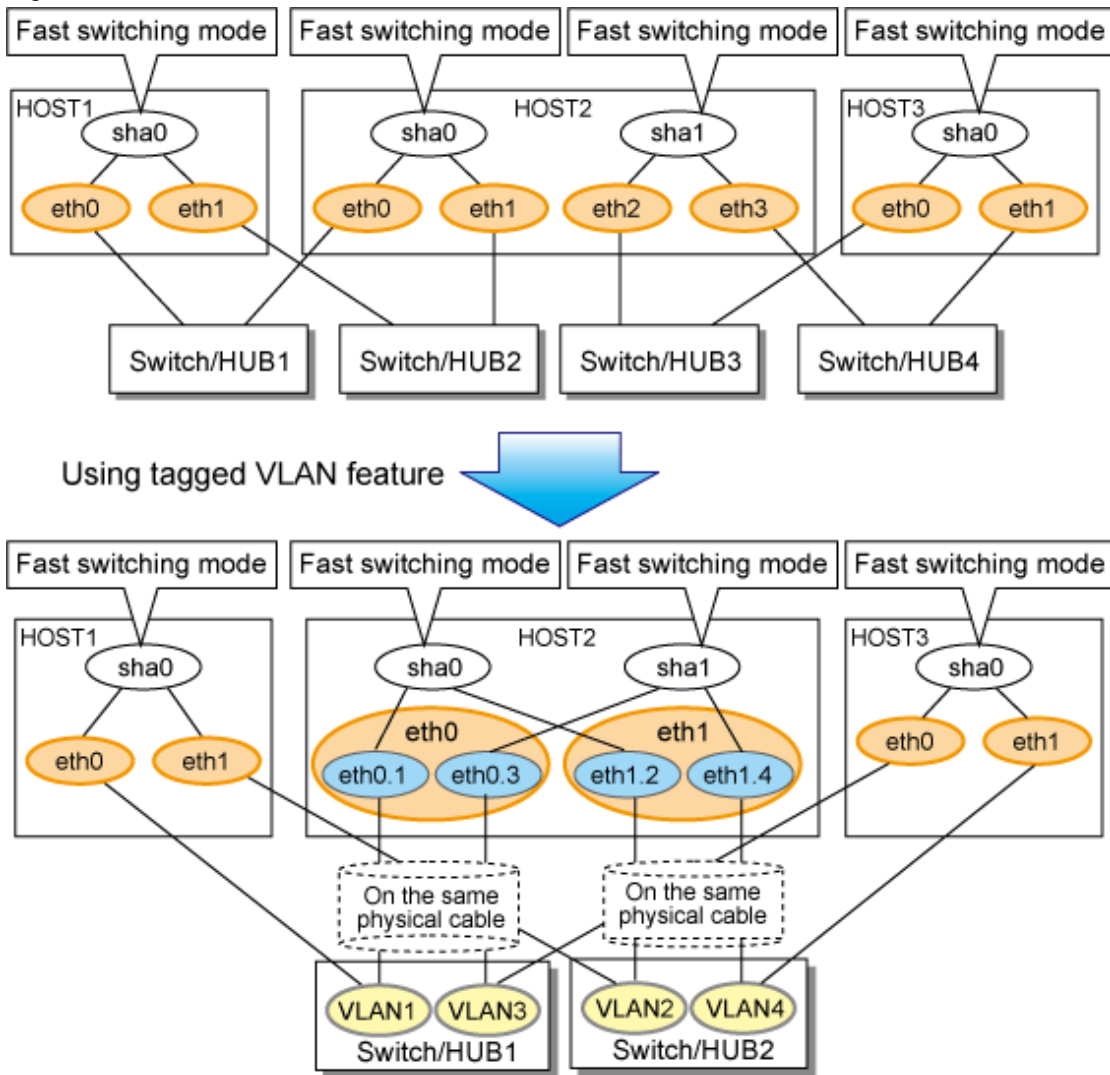


**P Point**

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

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

Figure 2.33 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.

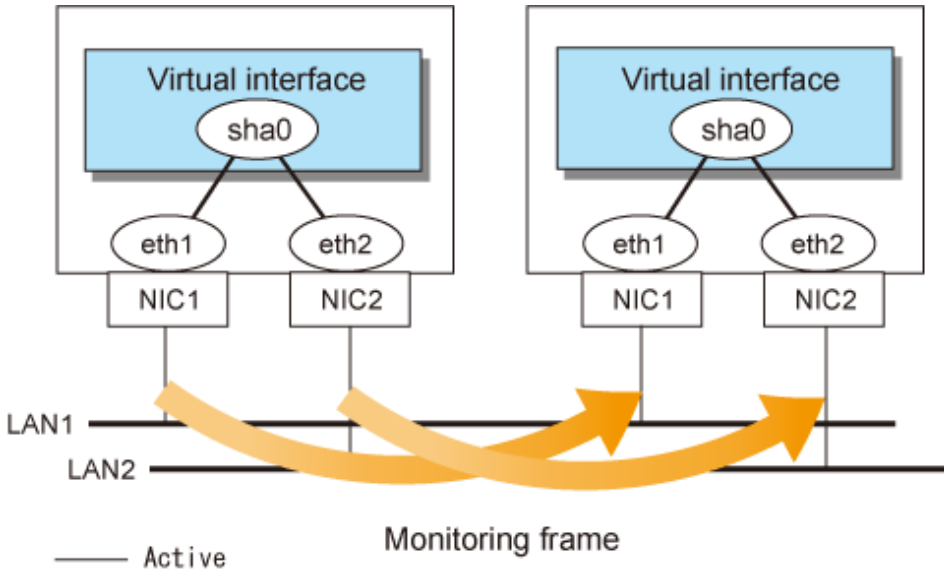
Table 2.2 Available option functions in each mode

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 2.34 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 HUB status using the following 2 methods. <ul style="list-style-type: none"> <li>- Network monitoring by ping</li> <li>- Monitors link status of NIC</li> </ul> If an error is detected in any of the monitoring functions, 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 switches the interface to be used when a transmission route failure is detected to the adjacent HUB or a hang-up of the ping command is detected. This function is available exclusively for NIC switching mode.

There are two monitoring methods that can be set in combination; HUB monitoring by ping command and monitoring link status of the interface.

In monitoring by ping, up to two monitoring target HUBs can be registered per virtual interface.

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

## Note

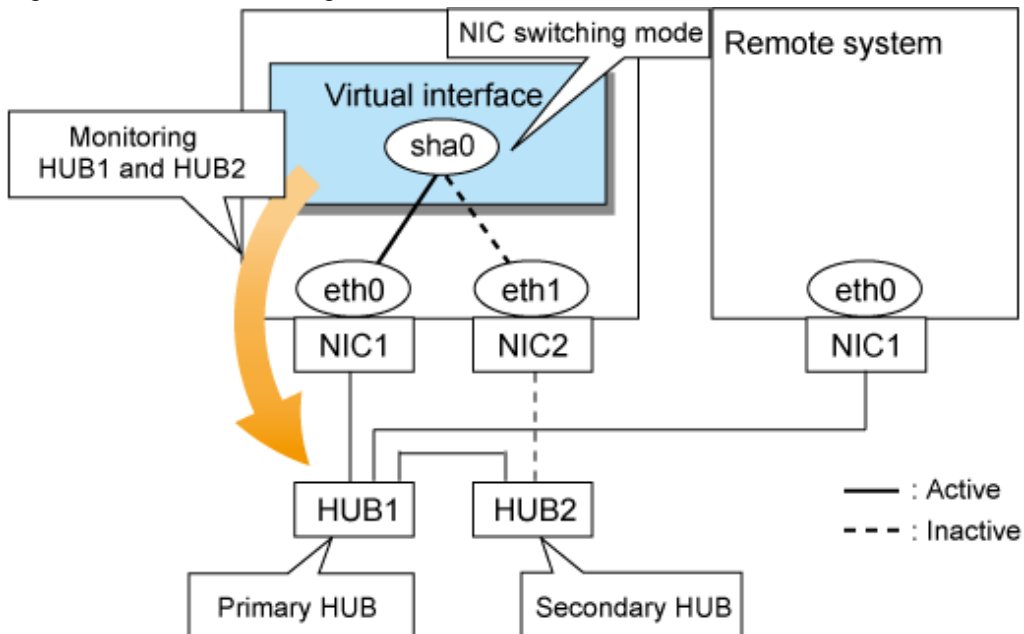
If no response after the ping command run for 30 seconds, the hang-up will be detected.

## Information

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

Figure 2.35 HUB monitoring function shows an outline of the HUB monitoring function

Figure 2.35 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.
- If the settings are incorrect as follows, the HUB monitoring function detects a route error even communication with the monitoring destination IP address is enabled.

- The network segment is not consistent between the IP address of the monitoring target and the IP address of the virtual interface.
- Communication with the IP address of the monitoring target is enabled by other interfaces except the virtual interface of GLS.

An error in the settings can be found earlier when a route error is detected.

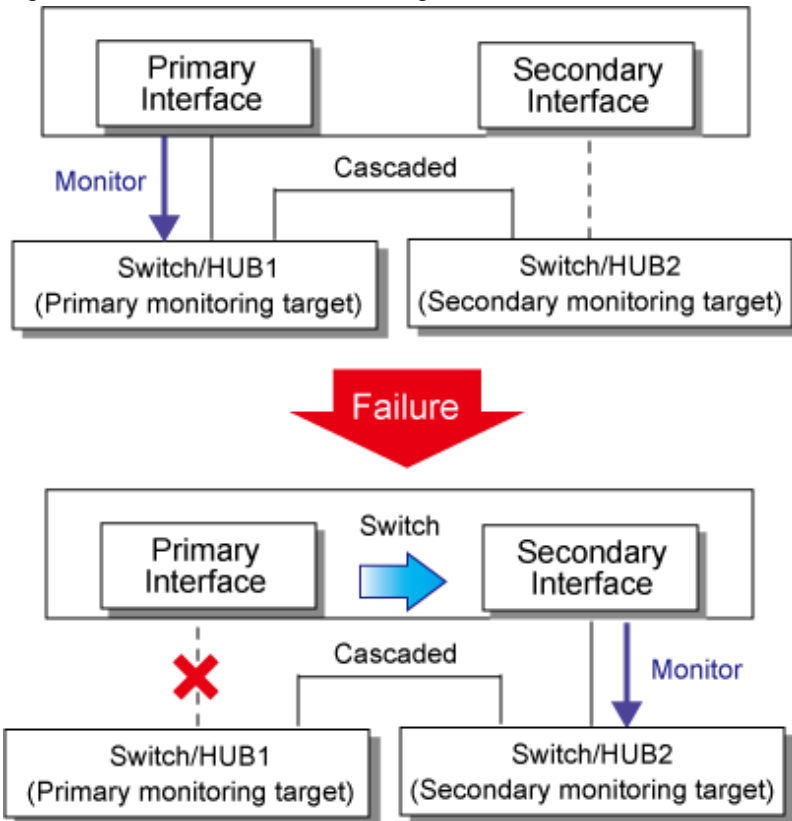
## Note

- 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 2.36 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 2.36 HUB-to-HUB monitoring disabled](#)) is monitored using the ping command.

Figure 2.36 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 2.37 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 2.37 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 2.37 HUB-to-HUB monitoring enabled (failure on the secondary monitoring)

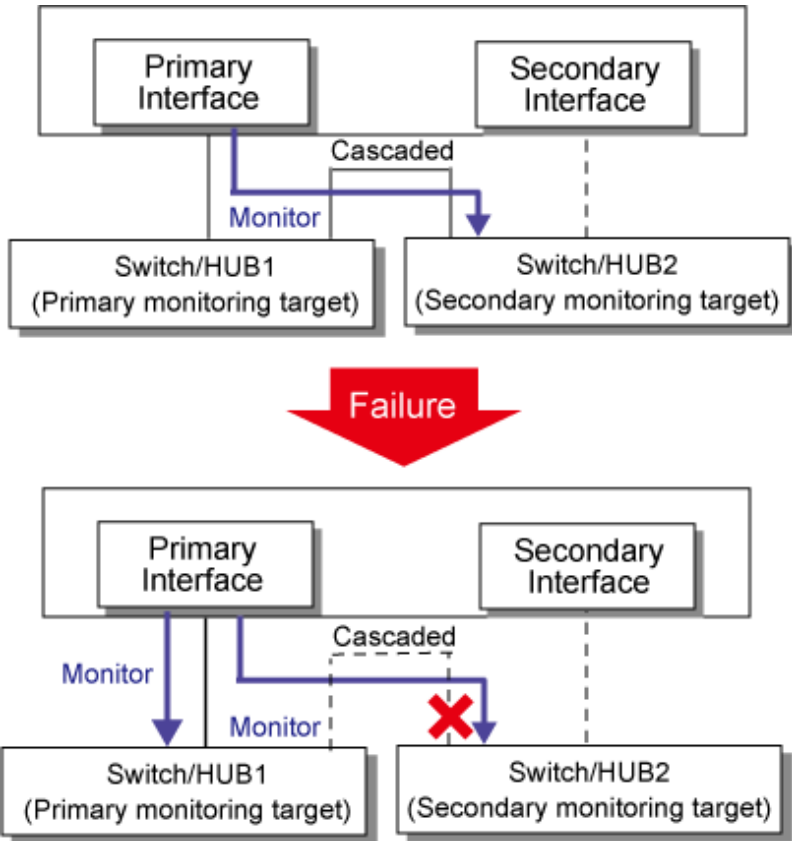
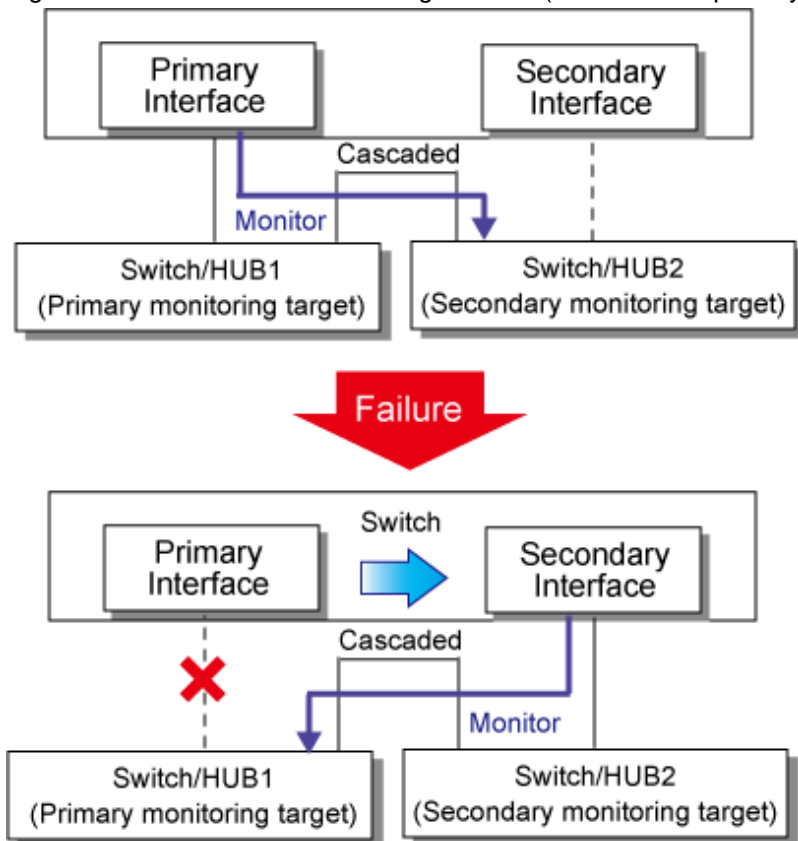


Figure 2.38 HUB-to-HUB monitoring enabled (failure on the primary monitoring)



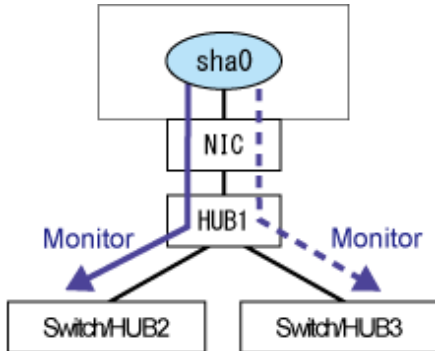


### 2.4.1.3 Multiple HUB monitoring on a single interface

Ping monitoring is performed for both the primary HUB and the secondary HUB (Figure 2.39 Multiple monitoring on a single physical interface for Switch/HUB2 and Switch/HUB3).

If failure is detected on both HUBs, transmission route failure is determined and monitoring is stopped to switch the cluster application. However, when monitoring is started only the primary HUB is monitored. If ping monitoring fails even once, this function in parallel with the monitoring of the primary HUB starts the monitoring of the secondary HUB.

Figure 2.39 Multiple monitoring on a single physical interface



### 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.

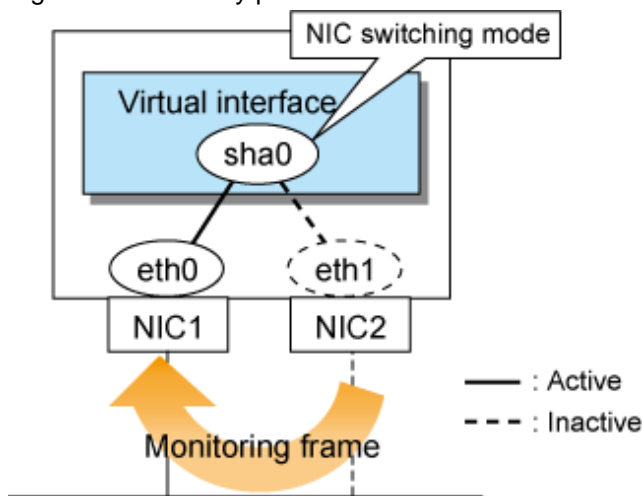
This brings the following effects:

- A message will be reported to an administrator when a failure occurs in standby interface. Therefore, standby interface failure can be detected.
- 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 or "7.11 stpptl Command" for stopping standby patrol.

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

Figure 2.40 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.

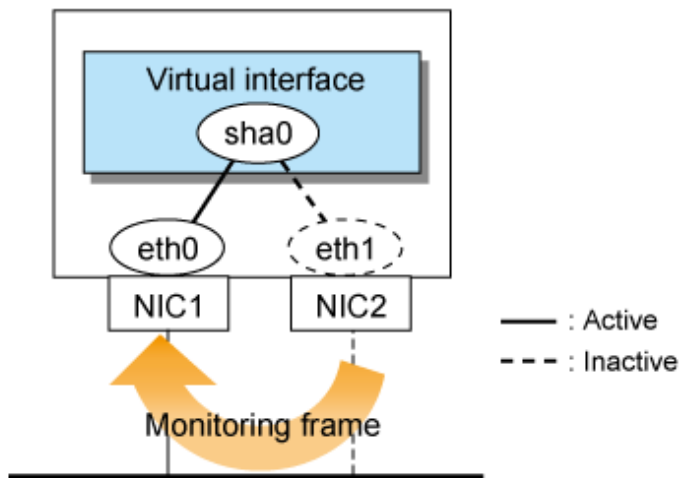
### 2.4.3 Automatic fail-back function

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.

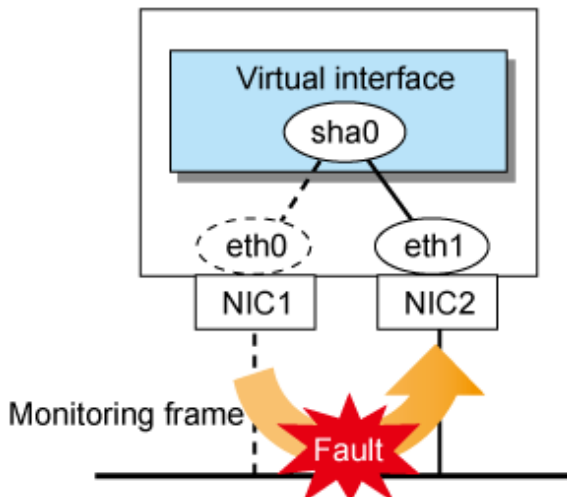
For information on the setup, [Figure 2.41 Automatic fail-back function](#) shows the outline of the automatic fail-back function.

Figure 2.41 Automatic fail-back function

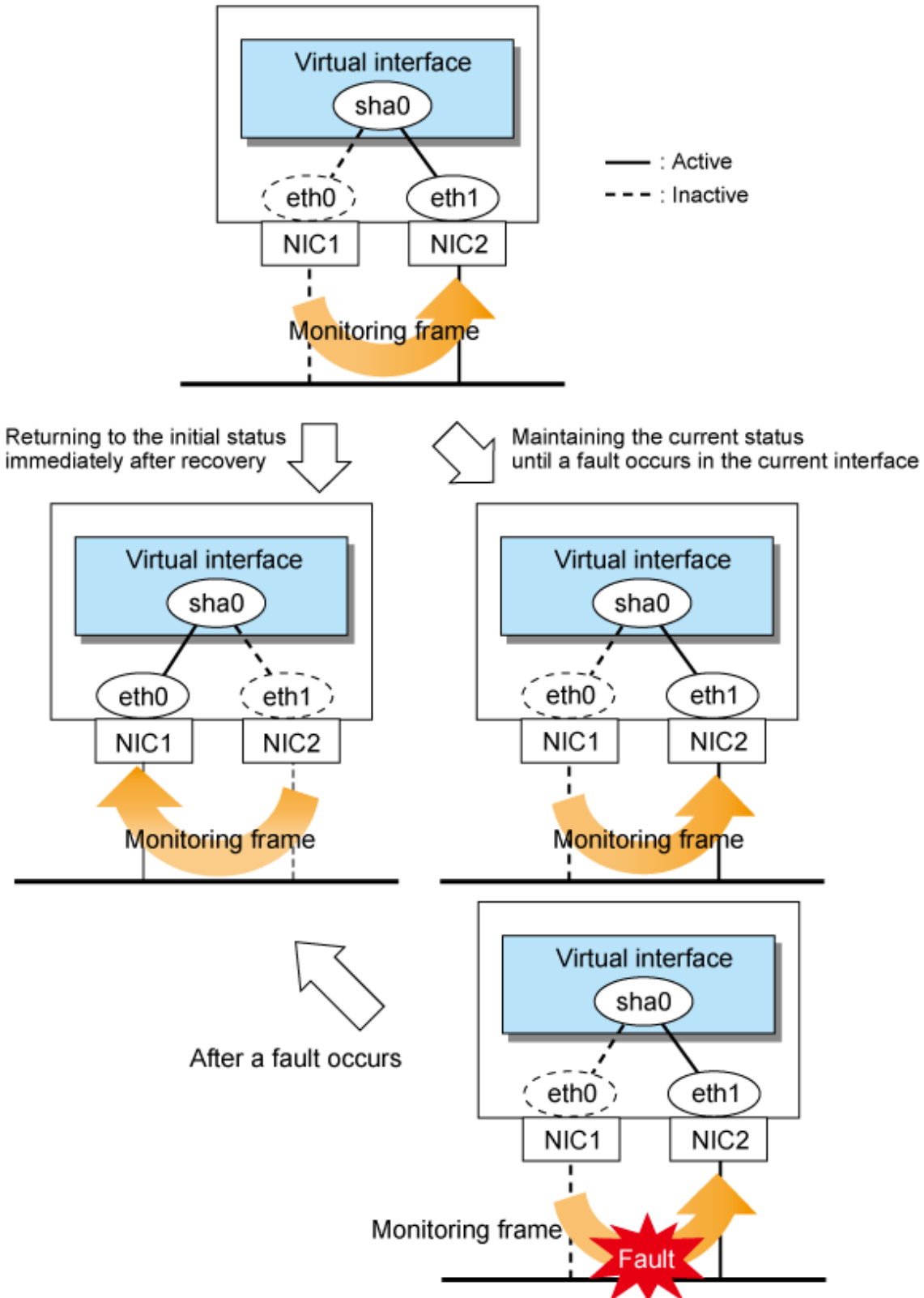
#### Initial status



#### After a fault occurs



## Recovery from a fault



When a device other than HUB is specified as a monitoring target device, the automatic fail-back may not be immediately executed after the primary interface is recovered, depending on where an error occurred in a transfer route. Therefore, make sure to specify HUB as a monitoring target device to execute the immediate automatic fail-back.

 **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.

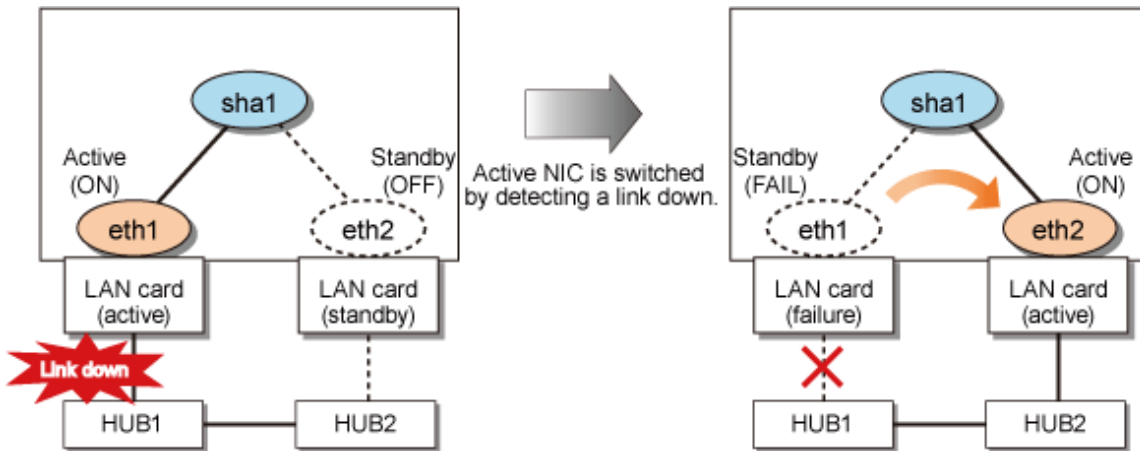
Table 2.4 Available option functions in each mode

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 2.42 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.

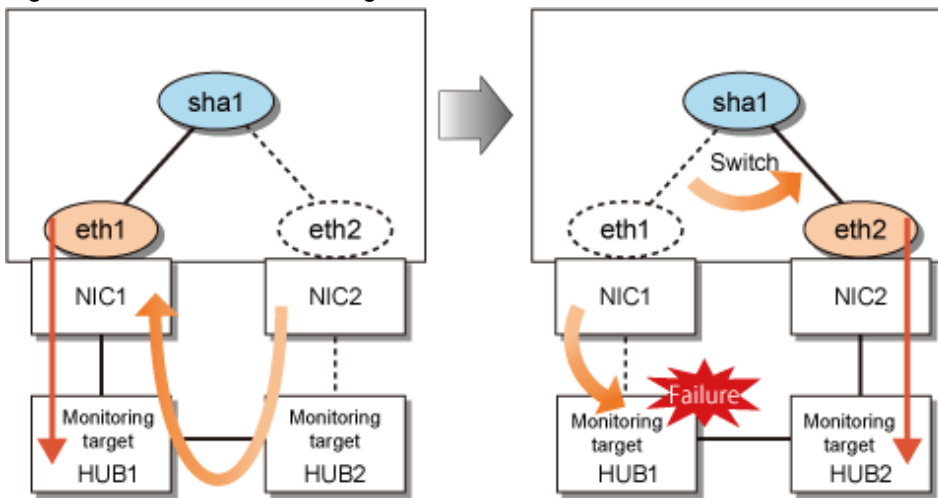
Monitoring type	Monitoring method
HUB monitoring	A ping command is sent periodically to the switch/HUB to which the NIC is connected to check whether the device responds normally.
Standby patrol	An Ethernet frame for monitoring is sent periodically from the standby NIC to the active NIC to check the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

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 2.43 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.
- If the settings are incorrect as follows, the HUB monitoring function detects a route error even communication with the monitoring destination IP address is enabled.
  - The network segment is not consistent between the IP address of the monitoring target and the IP address of the virtual interface.
  - Communication with the IP address of the monitoring target is enabled by other interfaces except the virtual interface of GLS.

An error in the settings can be found earlier when a route error is detected.

## 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. In any one of the following cases, the route is switched and a reporting message will be output:

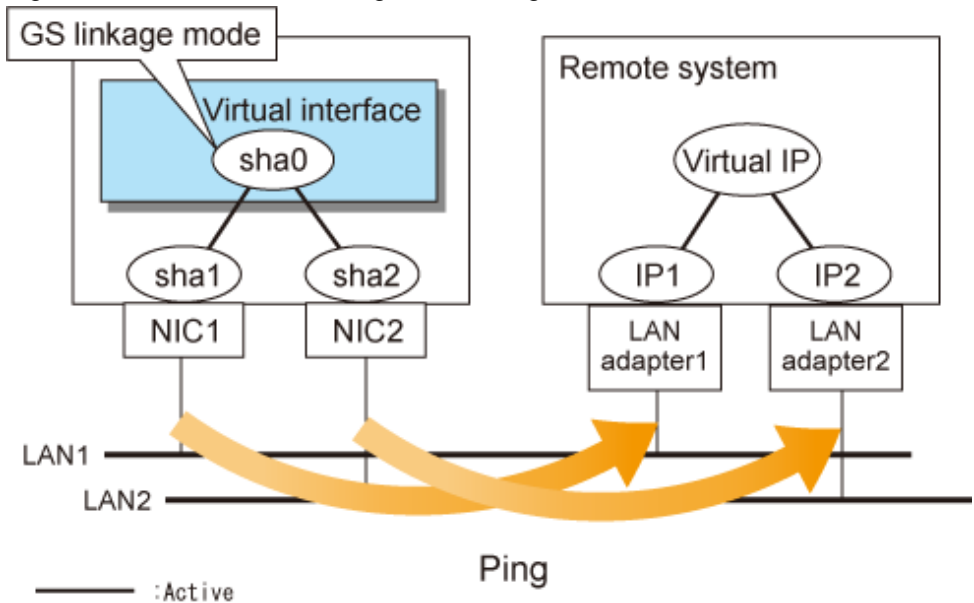
- A transfer path failure is detected.
- A hang-up of the ping command is detected.
- A failure notification is received from the remote system.

Then, communication is continued using other transfer path. 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.

### Note

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

Figure 2.44 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 an interface using a command such as the ip command.

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

Table 2.7 Recoverable interfaces using interface status monitoring feature

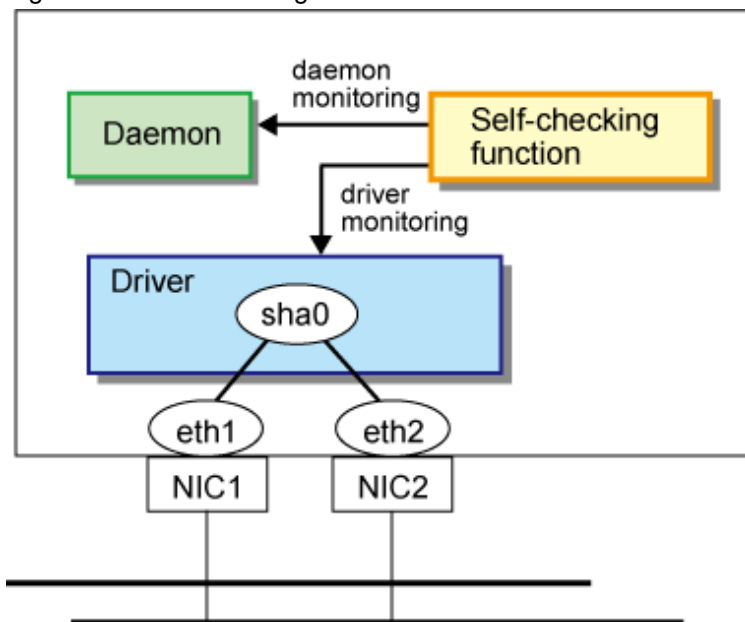
Mode	Single System			Cluster System		
	Virtual I/F (logical I/F)	Logical virtual I/F	Physical I/F	Virtual I/F (logical I/F)	Logical virtual I/F	Physical I/F
Fast switching	N	N	N	A	A	N
NIC switching	A	-	A	A	-	A
Virtual NIC mode	N	N	N	N	N	N
GS linkage	N	-	N	A	A	N

[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 2.45 Self-checking function





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
User command execution function	A	A	A	A
Suppression of stopping userApplication when entire transfer routes fails	X	A	X	X

[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.

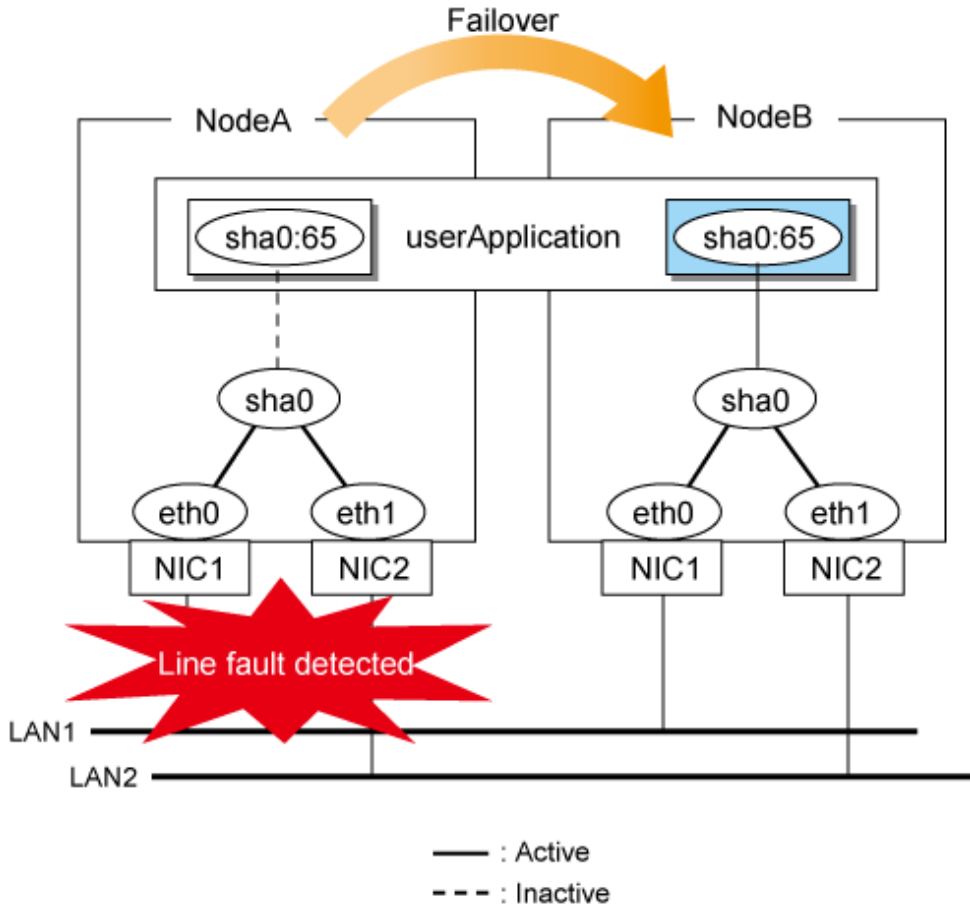
[Figure 2.46 Cluster failover due to line fault](#) shows an example of fail-over to node B when communication is disabled via both eth0 and eth1 bundled with virtual interface sha0 on node A.



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.



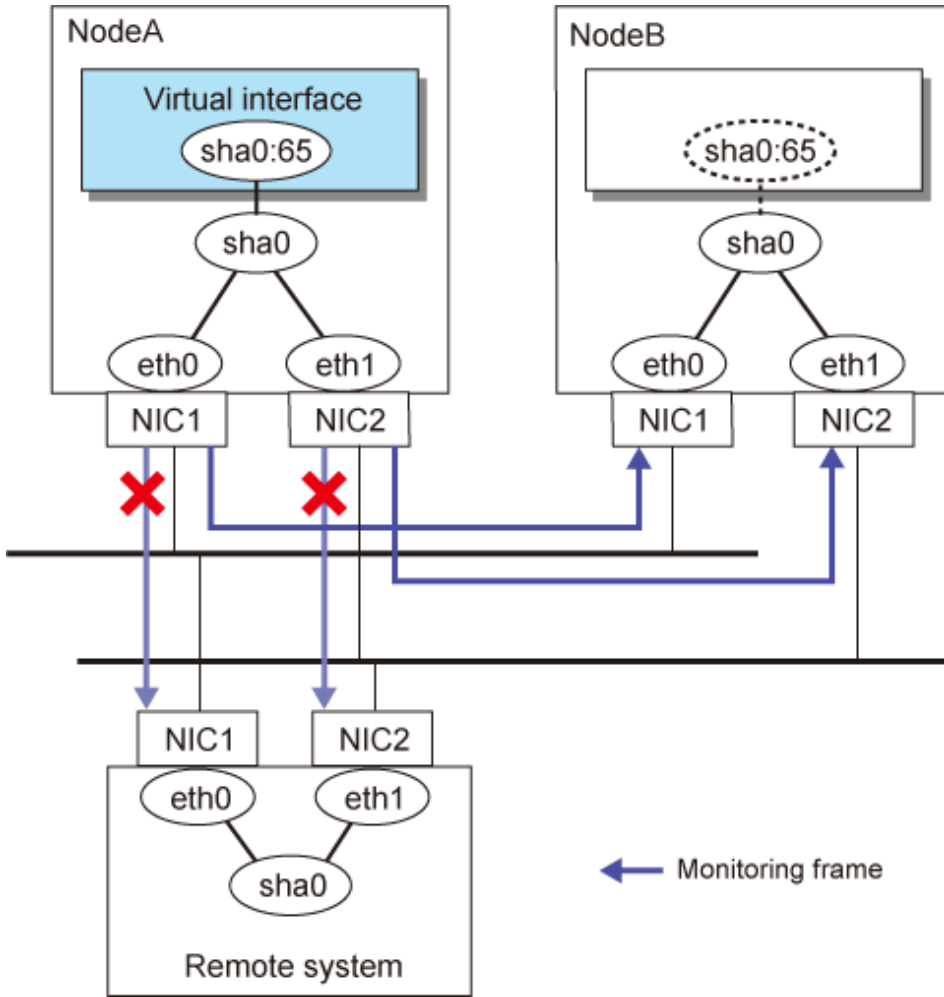
Figure 2.46 Cluster failover due to line fault



### 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 2.47 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.

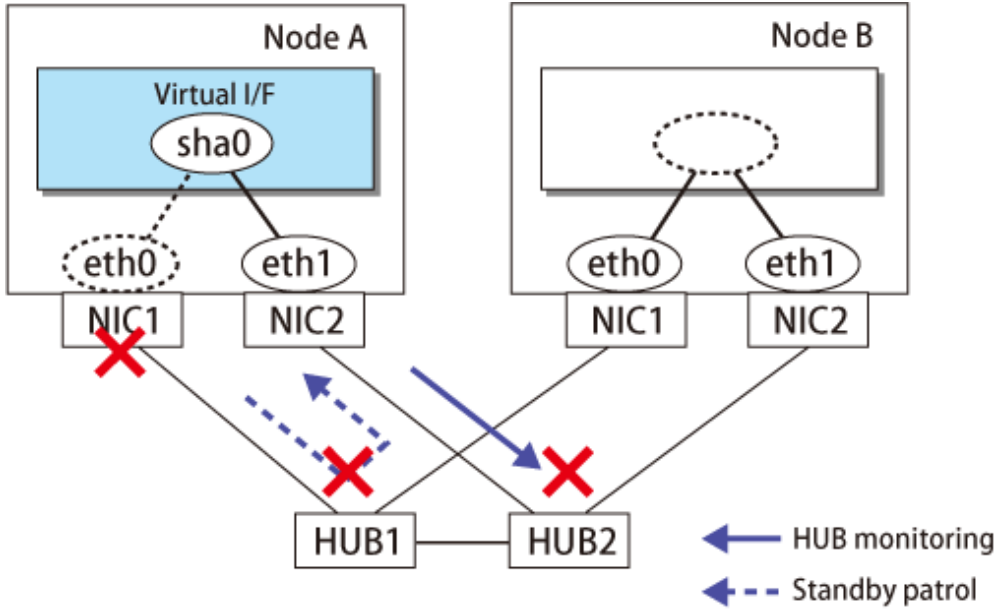
### Information

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 2.48 Error detection on a node in NIC switching mode



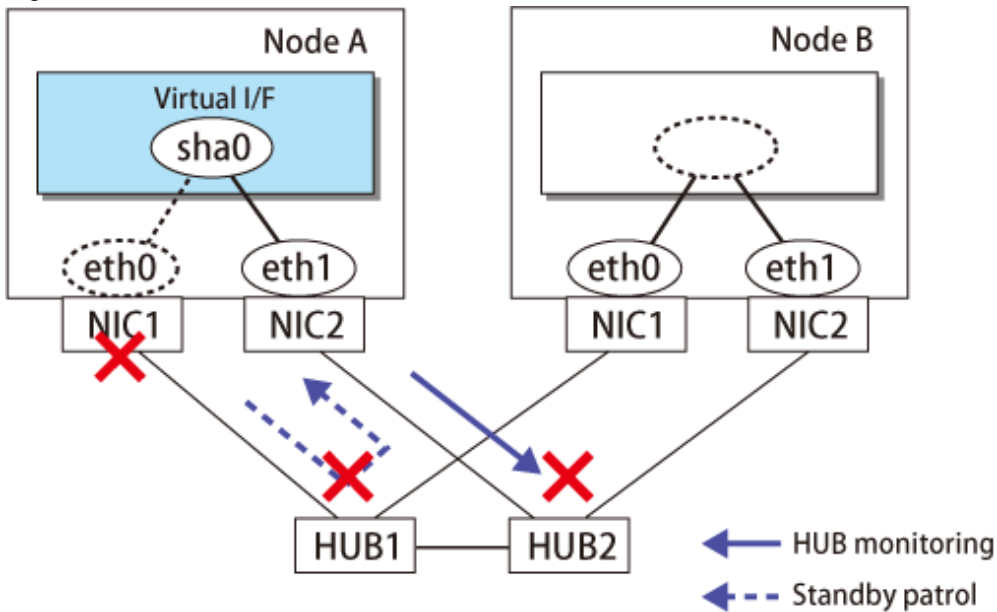
 Information

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 2.49 Error detection on a node in Virtual NIC mode



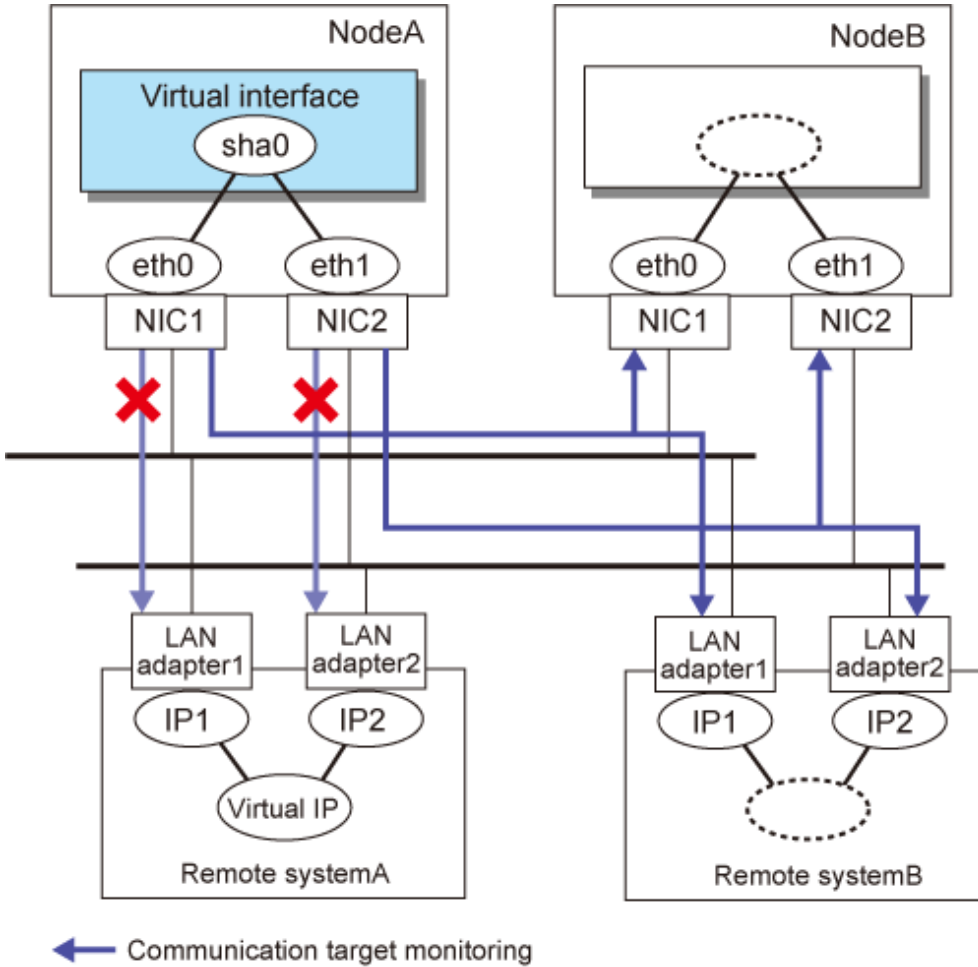
## Information

In network monitoring, HUB monitoring is performed for the IP address that is set by the `-p` option of the `hanetpathmon` target 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 2.50 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](#)".

## 2.8.2.1 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 the logical IP address takeover function) or a physical IP address (when using the 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 the 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 the system administrator or an application of detecting an error or recovery. When set either of a monitoring interval ('-p' option) or the number of constant monitoring ('-o' option) of standby patrol to zero by the hanetparam command, it is not possible to use this user command execution function.

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

Figure 2.51 Timing of running user command when activating or deactivating IP address (Logical IP address takeover function) (Continued.)

[When activated a system or a cluster service]

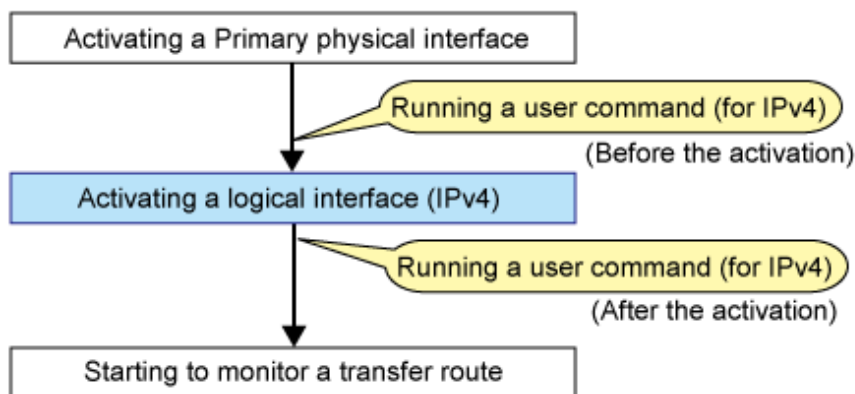


Figure 2.52 Timing of running user command when activating or deactivating IP address (Logical IP address takeover function) (End.)

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

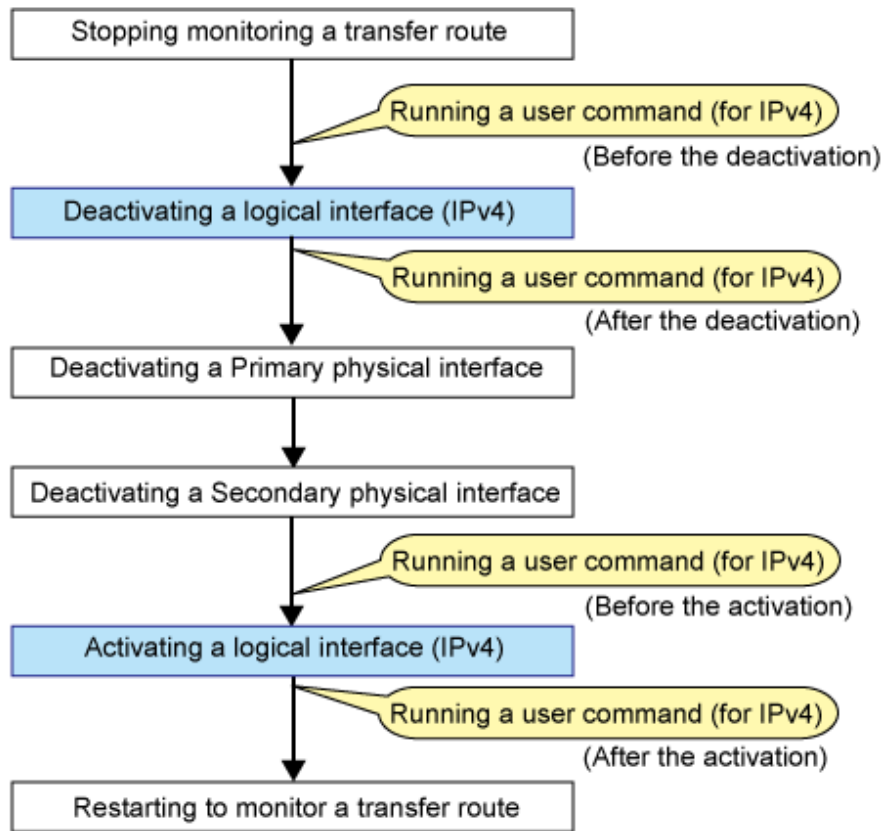
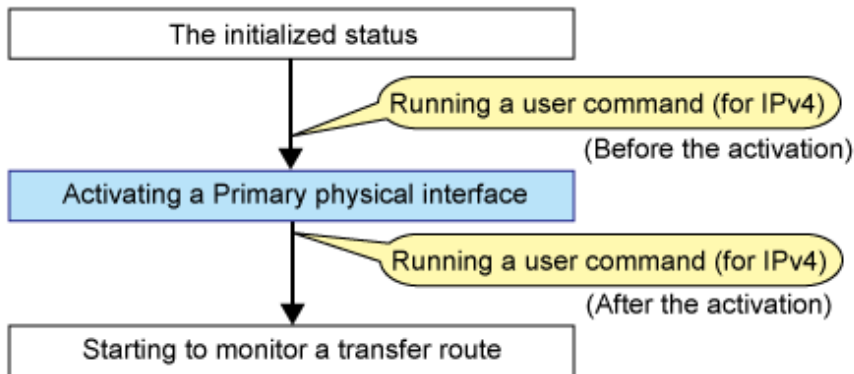


Figure 2.53 Timing of running user command when activating or deactivating IP address (Physical IP address takeover function) shows timing to run a user command when activated or deactivated an IP address in NIC switching mode (the physical IP address takeover function).

Figure 2.53 Timing of running user command when activating or deactivating IP address (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]

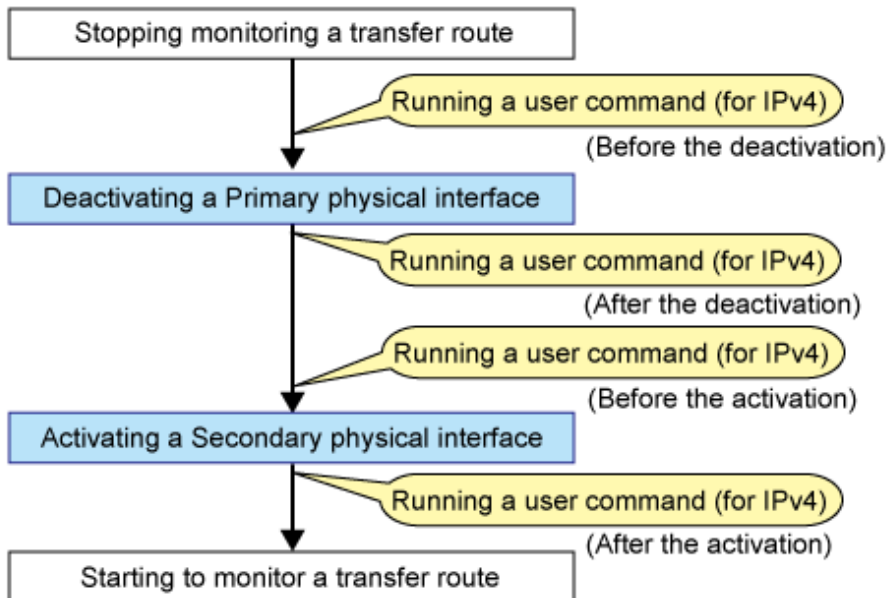
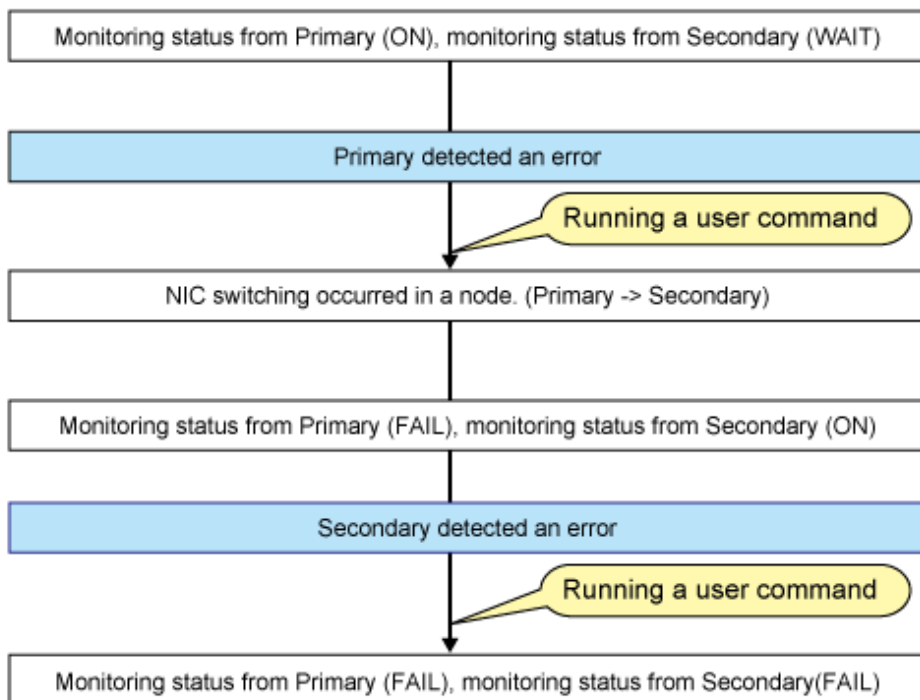


Figure 2.54 Timing of running user command when detected error in transfer route shows timing to run a user command when detected an error in a transfer route in NIC switching mode

Figure 2.54 Timing of running user command when detected error in transfer route  
 [When started to monitor a transfer route from a Primary interface]



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

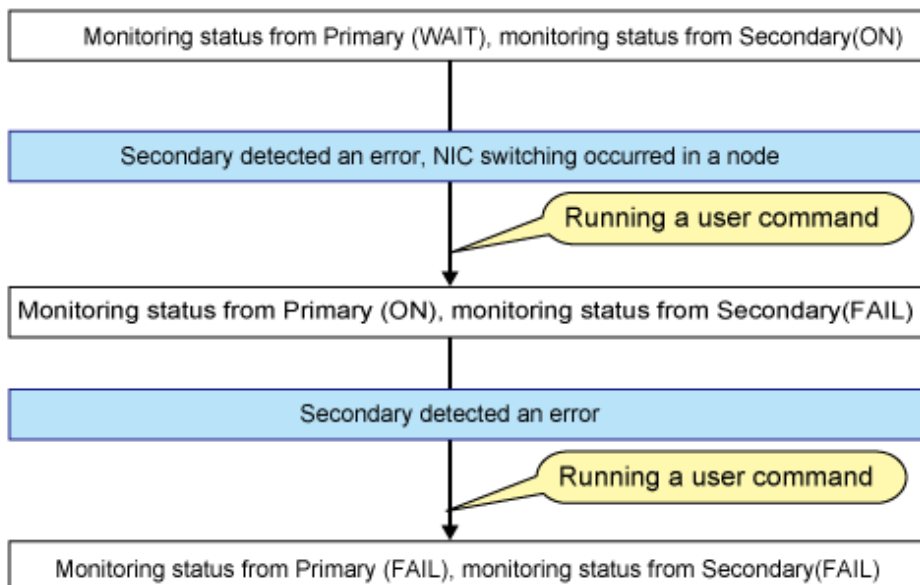
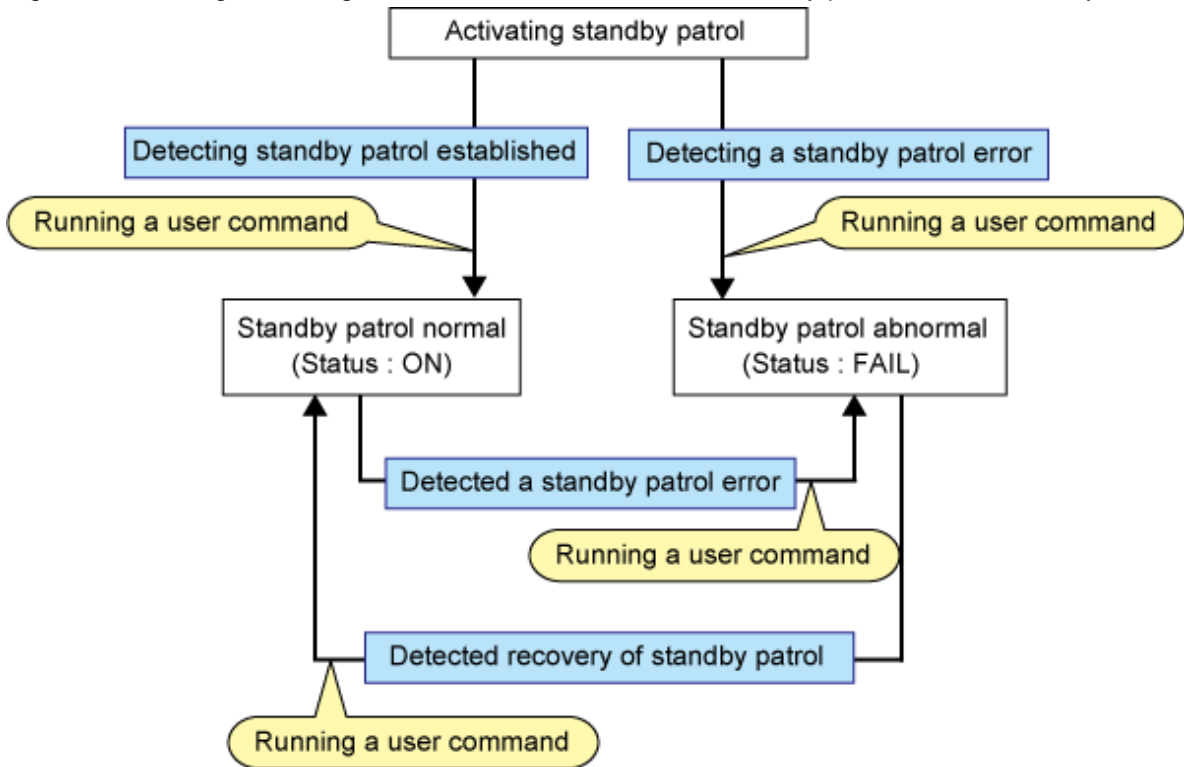


Figure 2.55 Timing of running user command when detected standby patrol error or recovery shows timing to run a user command when detected a standby patrol error or recovery in NIC switching mode.



Figure 2.55 Timing of running user command when detected standby patrol error or recovery



### 2.8.2.2 Virtual NIC mode

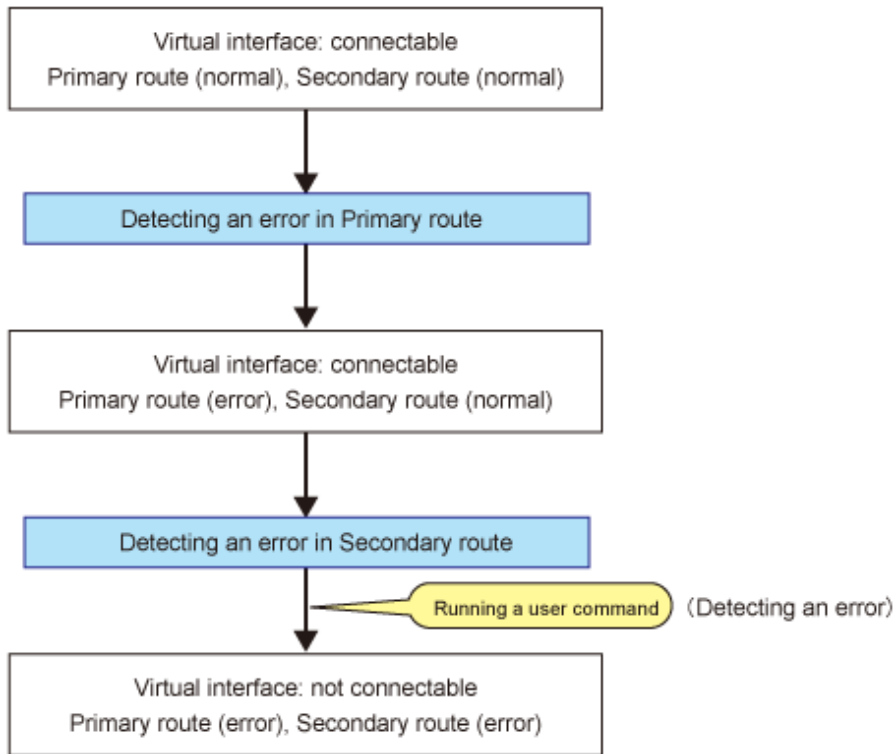
- Executing a user command when an error or a recovery is detected in the virtual interface

If errors are detected in both primary interface and secondary interface and the communication cannot be continued, execute the user-specified command. Execute the user-specified command also when either one of the interfaces is recovered from the above mentioned error.

This command is used to inform that the operation cannot be continued due to an error occurred in both routes.

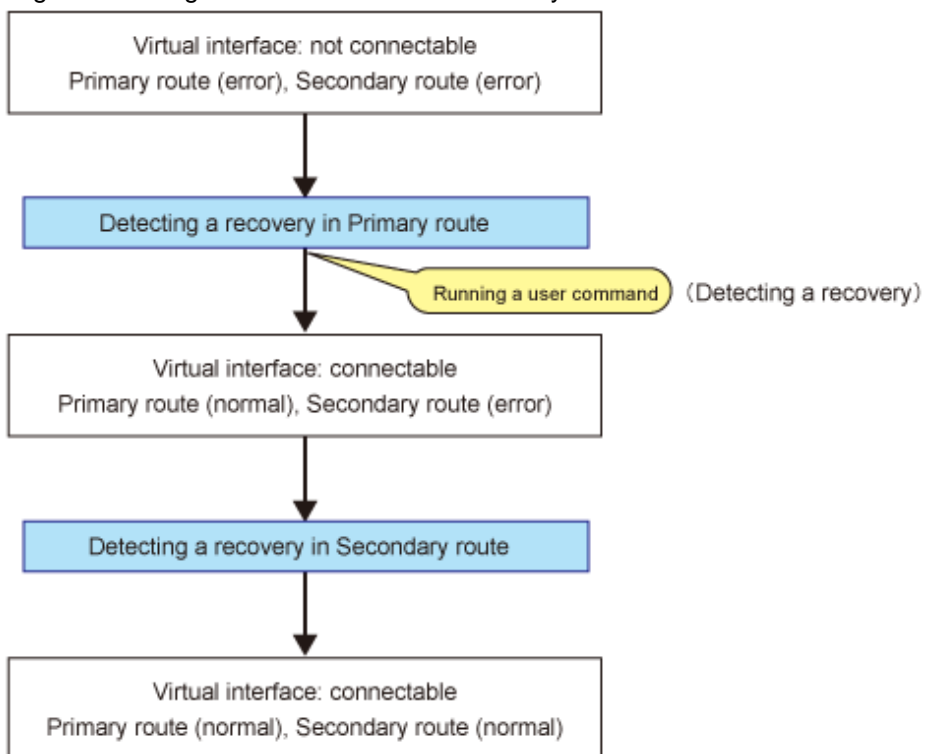
The following shows the timing for executing the user command when an error or a recovery is detected in the virtual interface.

Figure 2.56 Timing of executing user command when error is detected in virtual interface



The command is executed at the same timing as above if an error is detected in the secondary interface first, and then in the primary interface.

Figure 2.57 Timing of executing user command when recovery is detected in virtual interface



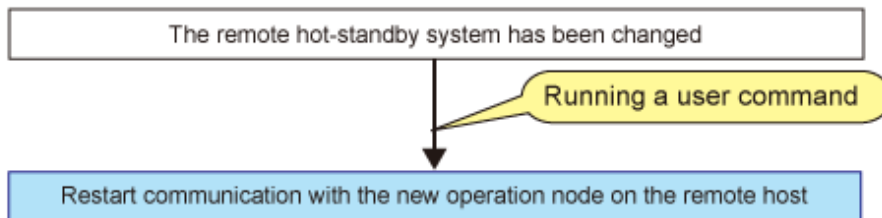
The command is executed at the same timing as above if a recovery is detected in the secondary interface first, and then in the primary interface.

### 2.8.2.3 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.

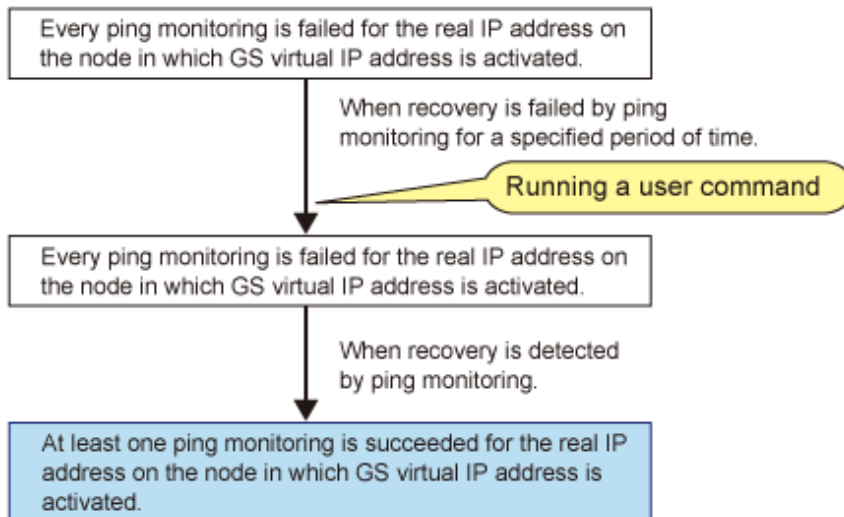
The following shows the timing for executing the user command in GS linkage mode.

Figure 2.58 Timing for executing user command in GS linkage mode  
[When changing the remote hot-standby system]

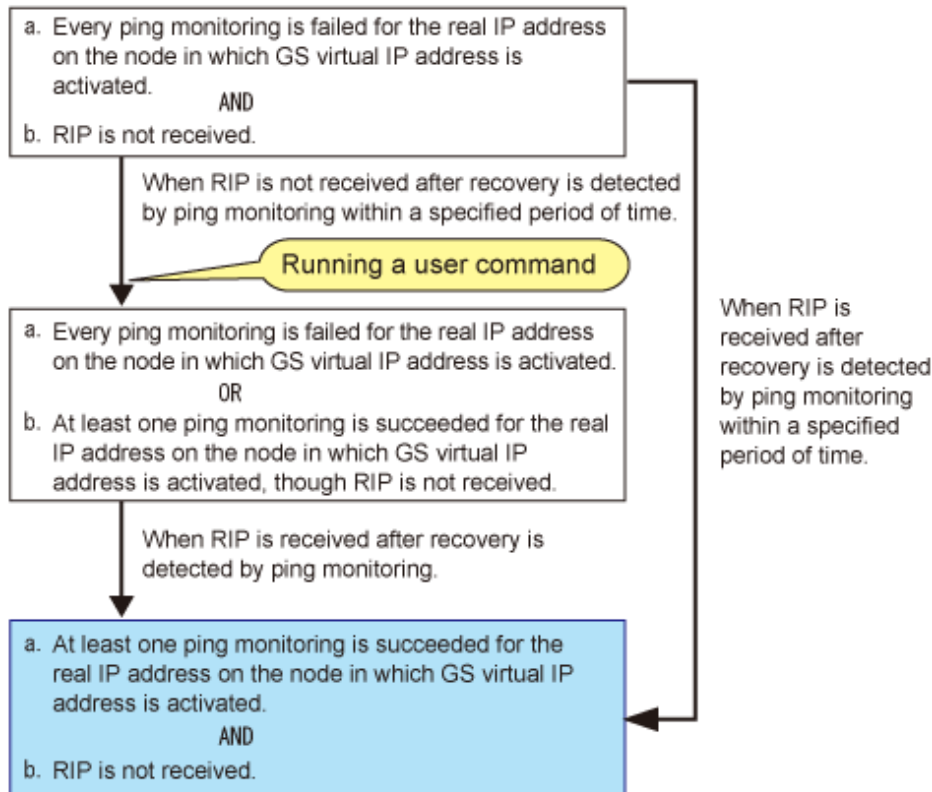


[When an error is detected in remote host monitoring]

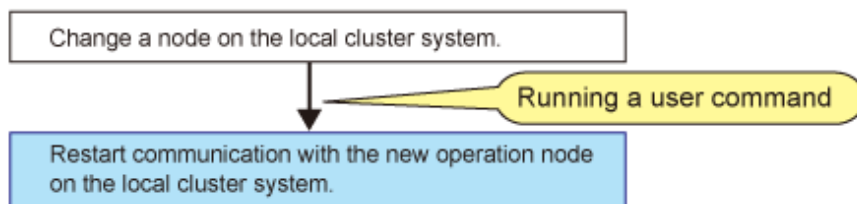
- When connecting to GS in the same network



- When connecting to GS in the different network



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



### 2.8.2.4 All of Fast switching mode, Virtual NIC mode, and GS linkage mode

- **Executing a user command when the takeover virtual interface is activated or deactivated**

In the cluster configuration, if the takeover virtual interface that is registered as a GIs resource is activated or deactivated, execute the user-specified command.

This command is used to perform an operation in synchronization with the activation and the deactivation of each takeover virtual interface.

The following shows the timing for executing the user command when activating and deactivating the virtual interface.

Figure 2.59 Timing of executing user command when activating virtual interface

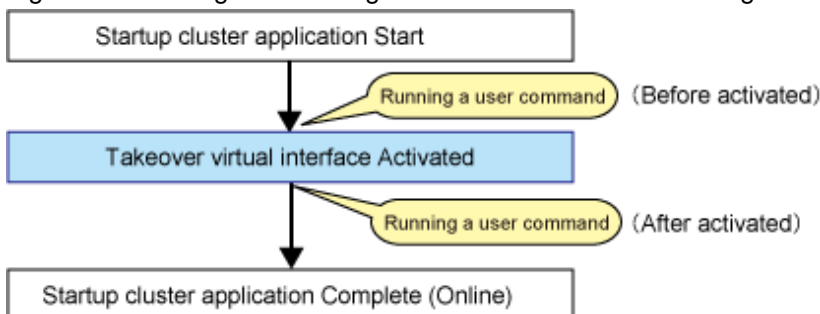
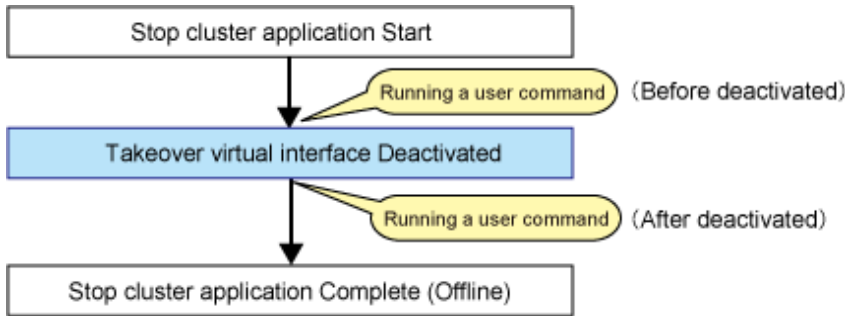


Figure 2.60 Timing of executing user command when deactivating virtual interface



### 2.8.2.5 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.

## 2.8.3 Suppression of stopping userApplication when entire transfer routes fails

When Cluster fail-over occurs, even if the HUB monitoring function of GLS detects failures in the entire transfer route on the node to be switched, the GLs resource does not become faulted and stopping userApplication can be suppressed.

With this capability, when entire transfer routes are recovered, communication can be recovered without recovery operation.

This function can be used in a configuration that satisfies all of the following conditions.

- 1:1 Standby Operation
- One userApplication
- NIC switching mode
- With the exception of the GLs resource, userApplication has no resources to detect network faults.
- The application that can restart operation when communication is recovered is used.

### See

For information on the setup, see Section "3.12.3 Setting suppression of stopping userApplication when entire transfer routes fails".

### Note

If userApplication is force started on the operation node, cluster fail-over does not take effect even if userApplication is started on the standby node. Make sure that run the following command on the operation node to enable cluster fail-over.

```
# /opt/FJShanet/usr/sbin/hanetpoll on -f yes
```

## 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
Hot 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 2.61 [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:

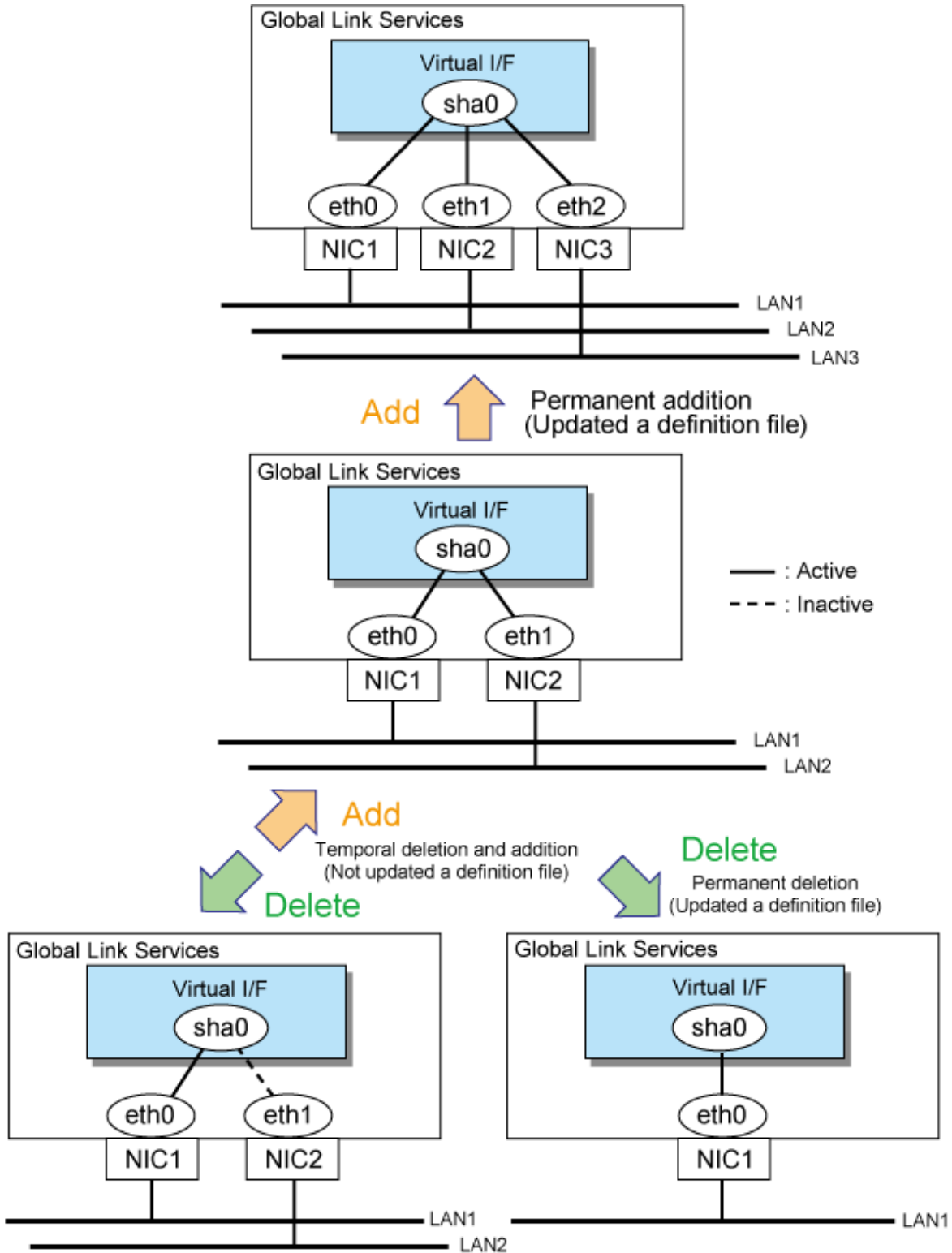
Edits a configuration information file. Therefore, changes are reflected even after operated a machine to reboot, etc. It is not possible to delete permanently when a virtual interface of Fast switching mode is registered to the cluster resource.



Note

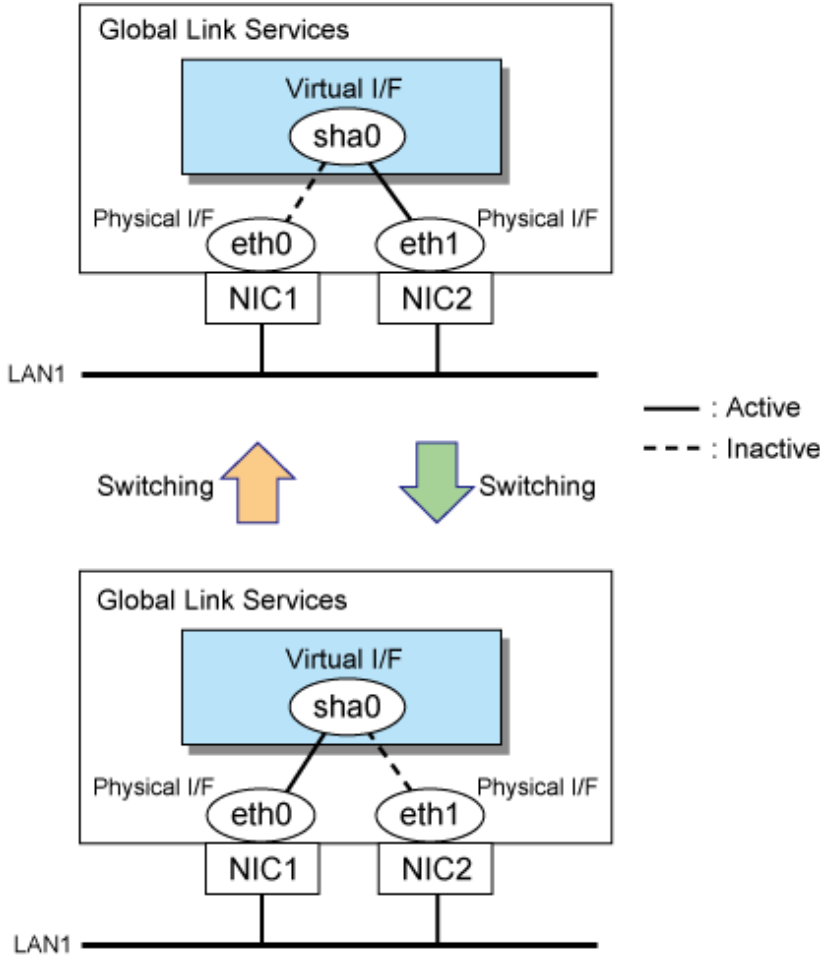
.....  
 In GS linkage mode, only temporary dynamic addition/deletion is possible.  
 .....

Figure 2.61 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 2.62 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 2.62 Dynamic switching function of physical interfaces used



## 2.9.2 Hot maintenance of NIC (PCI card)

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

### Note

The hot maintenance of NIC (PCI card) is enabled only when the main unit is PRIMEQUEST. The hot maintenance is disabled when the main unit is PRIMERGY.

For information about replacing the NIC used for the cluster interconnect, refer to "PRIMECLUSTER Installation and Administration Guide."

### See

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

- PRIMEQUEST 3000 Series

PRIMEQUEST 3000 Series Administration Manual

For information on how to perform the hot maintenance of the redundant line control function, see "6.3 NIC maintenance."



## 2.10 Notes

---

### 2.10.1 General

---

#### Notes on environment configuration:

- The maximum number of virtual interfaces and logical virtual interfaces that can be defined is 64.
- The maximum number of physical interfaces that can be used for redundancy on a single virtual interface is 8 for the Fast switching mode and the GS linkage mode. For the NIC switching mode, the maximum is 2.
- The maximum number of logical virtual interfaces that can be defined to a single virtual interface is 63.
- The maximum number of characters of each name for physical interfaces (including each VLAN ID for tagged VLAN interfaces) that can be bundled by a virtual interface is 15. When using the name of the interface that exceeds 15 characters, shorten the physical interface name. For details on changing the interface name, see "Linux documentation."
- The tagged VLAN interface name is available only by "interface name.VLAN-ID" format, such as eth0.1.
- If the interfaces bundled by GLS are not tagged VLAN interfaces, any interfaces that include periods in their names cannot be used.
- Set the switches and routers to be connected in order to enable the ARP cache update by GARP response.
- In RHEL 8 and later, NetworkManager may update the interface setting file (ifcfg-ethX, route-ethX, etc.).

#### Notes on the operation:

- Do not operate a virtual interface and physical interfaces that the virtual interface bundles with a command such as the ip command and the nmcli command while activating the virtual interface.
- Do not change the settings with the hantmask command while activating the virtual interface.
- Do not edit the physical interface setting file (ifcfg-ethX, etc.) and the virtual interface setting file (ifcfg-shaX, etc.), which are used by GLS, while activating the virtual interface.
- On the system that makes the transfer route redundant by the Redundant line control function, the user must not start, stop, and restart the network service.
- The following messages may be output to the system log during system startup. This does not disrupt ongoing operation.

```
kernel: Request for unknown module key 'FUJITSU Software: Fujitsu BIOS DB FJMW Certificate:
Hexadecimal, forty-digit' err -11
kernel: sha: module verification failed: signature and/or required key missing - tainting kernel
kernel: sha: loading out-of-tree module taints kernel.
```

- When performing network maintenance such as restarting or replacing a switch, switch NICs of GLS, stop the monitoring function, or suppress cluster switching in advance not to stop the operation due to a failure in the entire communication path.

#### 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

---

- Define all host names and IP addresses used in a Redundant line Control Function in the /etc/hosts files of the local system.
- The length of MTU cannot be modified.
- Multicast IP addresses cannot be used.
- 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.
- If the firewalld service is enabled, the virtual interface works in the default zone after the OS is restarted, depending on the OS version. Check the zone where the virtual interface works by using the firewall-cmd --get-active-zones command.

## 2.10.3 Duplicated operation via NIC switching mode

---

- Define all host names and IP addresses used in a Redundant line Control Function in the /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.
- 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](#)").
- It is necessary to use a HUB that can set an IP address when using an error monitoring using the ping command. 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.
- Do not configure the server running NIC switching mode as an IPv6 router.

- If the firewalld service is enabled, the virtual interface works in the default zone after the OS is restarted, depending on the OS version. Check the zone where the virtual interface works by using the firewall-cmd --get-active-zones command.

## 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 the active state even when restarting GLS by the resetnet command.
- In Virtual NIC mode, define the settings of IP addresses in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) in RHEL8, or define them with the nmcli command in RHEL9, same as for usual NICs. As in other communication modes, it is not required to set IP addresses by using the hantconfig command.
- The Virtual NIC mode cannot be used if the tagged VLAN interfaces are set for the physical interfaces.
- In Virtual NIC mode, the interface setting file of a virtual interface (/etc/sysconfig/network-scripts/ifcfg-shaX, etc.) 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.

- For RHEL8 or later, when the libvirtd service is started by starting OS, NIC (for example: 10G NIC) which supports LRO (large-receive-offload) function may link down temporarily. 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 the physical NIC settings are changed by using the ethtool command, the physical NIC driver is occasionally reset. At that time, the virtual interface detects a link down temporarily.
- When modifying the length of MTU for an interface, set the same value for the configuration of the primary interface and the secondary interface, and for the virtual interface configuration. The changed value is valid after a system reboot.
  - For RHEL8

```
# 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
```

- For RHEL9

Set the following parameter for primary, secondary, and virtual interface with the "nmcli connection modify" command.

```
802-3-ethernet: "9000"
```

- The interface created by SR-IOV cannot be used.
- The physical interface name that starts with capital or lower-case "a" - "r" can be used in the virtual NIC mode.
- When modifying MTU, make sure to set 1280 or more.

- For the configuration where the virtual bridge is connected with the virtual interface of the Virtual NIC mode, the following message may be output on the system log when activating the virtual interface or dynamically adding or deleting the interface. Ignore this message.

```
kernel: brX: received packet on shaX with own address as source address
```

- For the multiple configurations where the virtual bridge is connected with the virtual interface of the Virtual NIC mode, the following message may be output on the system log during communication. Ignore this message.

```
kernel: shaX: received packet with own address as source address
```

- If the firewalld service is enabled, the virtual interface works in the default zone after the OS is restarted, depending on the OS version. Check the zone where the virtual interface works by using the `firewall-cmd --get-active-zones` command.
- If the LLDP (Link Layer Discovery Protocol) function of the physical interface is enabled, set the MAC address or "auto" to SHAMACADDR.
- How to set SHAMACADDR depends on the OS. See "[3.3.3 Virtual NIC mode](#)" and "[7.1 hanetconfig Command](#)."
- If the following kernel parameters were set when using the Virtual NIC mode, delete the settings from the kernel parameters configuration files. Otherwise, the kernel parameters set by GLS are overwritten and GLS may not operate properly.

```
net.ipv6.conf.all.disable_ipv6 = X
net.ipv6.conf.default.disable_ipv6 = X
net.ipv6.conf.<dev>.disable_ipv6 = X
```

X: value

<dev>: NIC bundled by the virtual interface of GLS

Kernel parameters configuration files that the target value is set are as follows.

Table 2.10 Kernel parameters configuration files

OS	Kernel parameters configuration files
RHEL8/9	/etc/sysctl.conf /etc/sysctl.d/* /usr/lib/sysctl.d/*

## 2.10.5 Duplicated operation via GS linkage mode

- Define all host names and IP addresses used in a Redundant line Control Function in the /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 a 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.
- If the firewalld service is enabled, the virtual interface works in the default zone after the OS is restarted, depending on the OS version. Check the zone where the virtual interface works by using the firewall-cmd --get-active-zones command.
- 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](#)".
- In GS linkage mode, a message is exchanged between the host and the server by using "Fujitsu Hot Standby Protocol". This is the protocol of UDP communication that uses the port number 1807. Set the firewall to allow the communication by this protocol.

# Chapter 3 Environment configuration

This chapter discusses how to set up and configure GLS.

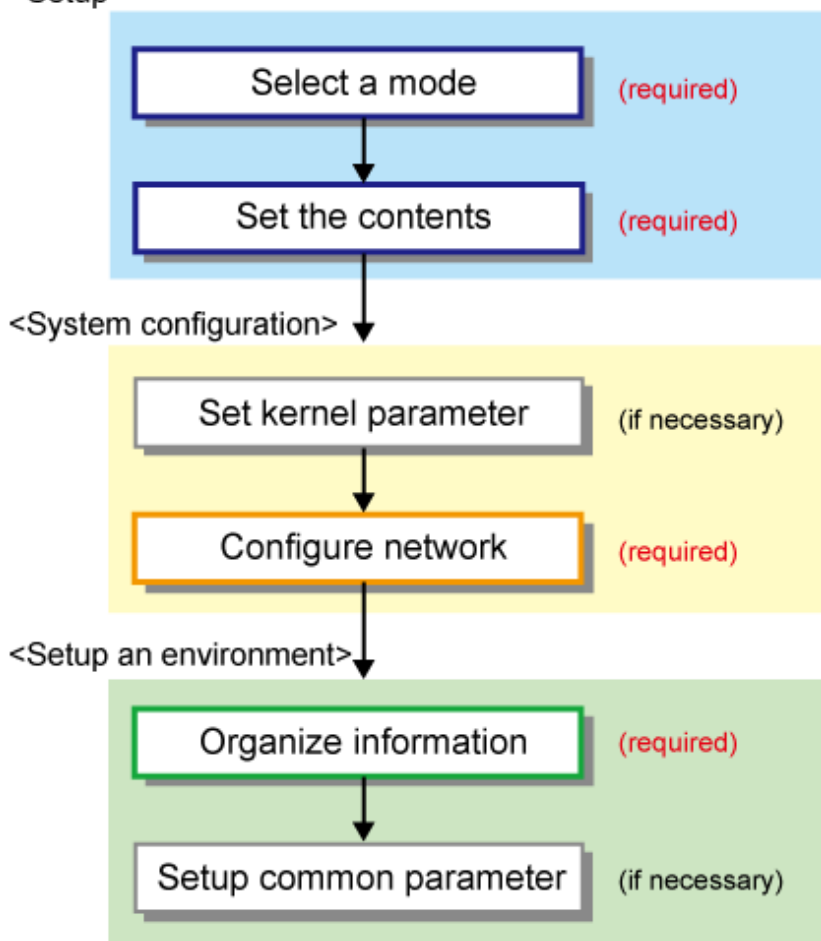
## 3.1 Setup

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

<Setup>



### 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 when deploying the Linux server on a network where there are various devices such as a hot-standby router, a network load balancer, or servers.

Mode	Selecting mode
Virtual NIC mode	Select this mode in the following cases: <ul style="list-style-type: none"> <li>- The Linux server is deployed on a network where there are various devices such as a hot-standby router, a network load balancer, or servers.</li> <li>- Multicast communication or IPv6 is used.</li> <li>- Communication of a guest OS is duplicated on the host OS when the virtual machine function is used.</li> </ul>
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



Note

This version does not support IPv6 addresses for the 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>

Set up 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 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.

### Subnet mask

When using an IPv4 address, specify the sub network mask value applied to the virtual IP address. If a subnet is not used, this configuration can be omitted. This component is set by using "hanetmask" command.

### <Physical interface information>

Set up 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 an 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 interfaces. To set up this component, create the "/etc/sysconfig/network-scripts/ifcfg-physical interface name" file, and then describe the IP address in the file.

### Subnet mask

If using an IPv4 address, specify a sub network mask value applied to the physical IP address. If a subnet is not used for allocation, this configuration can be omitted. This configuration is written in the "/etc/sysconfig/network-scripts/ifcfg-physical interface name" file. For RHEL8, set the subnet mask by using PREFIX, not NETMASK.

## 3.1.2.2 NIC switching mode



### Note

This version does not support IPv6 addresses for the 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>

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.

#### 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>

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)

#### 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, set up 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>

Set up 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. If monitoring by ping command is not used, specify "\_none\_".

#### 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. Do not specify if "\_none\_" is specified to the primary monitored remote system IP address.

#### 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	
	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

Specify an IP address 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		
	Static routing information for virtual gateways		
(Repeat for the number of the virtual interfaces)			
Remote node information	Remote node name		
	Virtual IP information	Virtual IP address or host name	
		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>

Set up 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 configuration can be omitted if not allocating a subnet. Set a subnet mask by using "hanetmask" command. When applying a subnet mask, apply the same mask value to all the virtual and physical IP addresses.

### <Physical interface information>

Set up 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. To set up this component, create the "/etc/sysconfig/network-scripts/ifcfg-physical interface name" file, and then describe the IP address in the file.

## Subnet mask

Specify a sub network value applied to the physical IP address. This configuration can be omitted if not allocating a subnet. This configuration is written in the "/etc/sysconfig/network-scripts/ifcfg-physical interface name" file. For RHEL8, set the subnet mask by using PREFIX, not NETMASK. If using a subnet mask, apply the same mask value to all the virtual and physical IP addresses.

### <Virtual gateway information>

Set up the following for the number of virtual interfaces.

#### Virtual gateway IP address

Specify the IP address of the remote virtual gateway required for communication with the remote host. The network (subnet) portion of the IP address should be the same as the IP address assigned to the virtual interface. Use the -g option of the hanetgw create command to specify this item.

#### Static routing information for virtual gateways

Use the following procedure to add static routing information for communicating with the remote host using the virtual gateway.

##### [RHEL8]

Create a "/etc/sysconfig/network-scripts/route-virtual-interface-name" file and configure static route information in the file.

##### [RHEL9]

Setting static routing information is automatic and unnecessary.

### <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>

Set up the following for the number of virtual IPs.

#### 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. 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	Yes (Virtual NIC mode: Already activated)
Hostname resolution function	A	A	N	A	Yes
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	Yes

[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 use node switching when a failure occurs to every transfer paths.

yes: Node switching is performed when a failure occurs to a whole transfer paths.

no: No node switching is performed when a failure occurs to a whole transfer path.

The default value 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. The default value is "yes". 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). The default value is "yes". This configuration is specified using "-h" option of the "hanetparam" command and 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. The default value is "yes". This configuration is specified by "-e" option of "hanetparam" command.



### 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

#### 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 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/FJShanet/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 to be used for the Redundant Line Control Function.

The physical interface settings vary depending on redundant network methods and configurations. For details on the differences of each setting, see the following [Table 3.8 Physical interface settings \(RHEL8\)](#) and [Table 3.9 Physical interface settings \(RHEL9\)](#).

#### Point

- For RHEL 7 or later, the naming conventions for NIC names are changed to generate device names based on the hardware locations of NICs (Predictable Network Interface Names).  
In an environment where Predictable Network Interface Names are enabled, interface names are displayed as enXXXXXX. In an environment where Predictable Network Interface Names are disabled, interface names are displayed as ethX.  
Replace the interface name (ethX) described in this manual with the interface name suitable for your environment. Replace the ifcfg-ethX file name with the file name suitable for your environment as well.
- Only the required parameters in the Redundant Line Control Function are described for the configuration file (ifcfg-ethX) of the network interface in this manual. Set other parameters according to your environment.

#### For RHEL8

Table 3.8 Physical interface settings (RHEL8)

Redundant network methods		Tagged VLAN disabled	Tagged VLAN enabled
Fast switching mode (IPv4)		<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>
Virtual NIC mode		<a href="#">Setup 5</a>	<a href="#">Setup 5</a>
GS linkage mode		<a href="#">Setup 1</a>	Not supported

#### Note

- For RHEL 7 or later, the naming conventions for NIC names are changed to generate device names based on the hardware locations of NICs (Predictable Network Interface Names).  
If you need to prevent device names of physical NICs from changing to unexpected names in an environment where traditional interface

names (ethX) for RHEL6 or earlier are used, describe the definition of "HWADDR=<MAC address>" in the settings for the physical interfaces (the /etc/sysconfig/network-scripts/ifcfg-ethX file). For details, see "Linux documentation."  
The setting "HOTPLUG=no" is not required.

- The tagged VLAN interface name is available only by "interface name.VLAN-ID" format, such as eth0.1.
- In the cluster environment of physical IP takeover II, set ONBOOT=no to ifcfg-ethX.
- In the settings for the tagged VLAN interface (/etc/sysconfig/network-scripts/ifcfg-ethX.Y file) "PHYSDEV=", describe the physical interface name that configure the tagged VLAN interface, such as ethX.

---

#### Setup 1

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.XXX
PREFIX=XX
DEVICE=ethX
ONBOOT=yes
```

#### Setup 2

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.XXX
PREFIX=XX
DEVICE=ethX
ONBOOT=no
```

#### Setup 3

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

```
TYPE=Ethernet
DEVICE=ethX
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=ethX
VLAN_ID=Y
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.XXX
PREFIX=XX
ONBOOT=yes
```

#### Setup 4

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

```
TYPE=Ethernet
DEVICE=ethX
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=ethX
VLAN_ID=Y
BOOTPROTO=none
IPADDR=XXX.XXX.XXX.XXX
PREFIX=XX
ONBOOT=no
```

Setup 5

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=ethX
ONBOOT=yes
```

 Information

If you want to use the NIC switching mode to share the same physical connection between two virtual interfaces (one that bundles physical interfaces and the other that 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.

**For RHEL9**

Table 3.9 Physical interface settings (RHEL9)

Redundant network methods		Tagged VLAN disabled	Tagged VLAN enabled
Fast switching mode (IPv4)		Setup 1	Setup 3
NIC switching mode (IPv4)	Primary interface	Setup 1	Setup 3
	Secondary interface	Setup 2	Setup 4
Virtual NIC mode		Setup 5	Setup 5
GS linkage mode		Setup 1	Not supported

 Note

- For RHEL 7 or later, the naming conventions for NIC names are changed to generate device names based on the hardware locations of NICs (Predictable Network Interface Names).  
If you need to use traditional interface name (ethX) for RHEL6 or earlier, set the traditional interface name (ethX) in "connection.id" and "connection.interface-name" with the nmcli connection modify command. Also, to prevent device names of physical NICs from changing to unexpected names, set the MAC address to "802-3-ethernet.mac-address" using the nmcli connection modify command.
- The tagged VLAN interface name is available only by "interface name.VLAN-ID" format, such as eth0.1.
- In the cluster environment of physical IP takeover II, set connection.autoconnect to "no" with the nmcli connection modify command.

Setup 1

Set the following parameters with the "nmcli connection modify" command.

- ipv4.method: "manual"
- ipv4.addresses: "XXX.XXX.XXX.XXX/XX"

- connection.autoconnect: "yes"

After configuration, confirm that the following parameters are set for ethX by using the nmcli connection show command.

- connection.type: "802-3-ethernet"
- connection.id: "ethX"
- connection.interface-name: "ethX"

#### Setup 2

Set the following parameters with the "nmcli connection modify" command.

- ipv4.method: "manual"
- ipv4.addresses: "XXX.XXX.XXX.XXX/XX"
- connection.autoconnect: "no"

After configuration, confirm that the following parameters are set for ethX by using the nmcli connection show command.

- connection.type: "802-3-ethernet"
- connection.id: "ethX"
- connection.interface-name: "ethX"

#### Setup 3

Set the following parameters with the "nmcli connection modify" command.

- ipv4.method: "disabled"
- ipv4.addresses: ""
- connection.autoconnect: "yes"

After configuration, confirm that the following parameters are set for ethX by using the nmcli connection show command.

- connection.type: "802-3-ethernet"
- connection.id: "ethX"
- connection.interface-name: "ethX"

Create a VLAN interface using the nmcli connection add command.

```
# /usr/bin/nmcli connection add type vlan con-name ethX.Y ifname ethX.Y  
vlan.parent ethX vlan.id Y
```

Set the following parameters for the created ethX.Y using the nmcli connection modify command.

- ipv4.method: "manual"
- ipv4.addresses: "XXX.XXX.XXX.XXX/XX"
- connection.autoconnect: "yes"

#### Setup 4

Set the following parameters with the "nmcli connection modify" command.

- ipv4.method: "disabled"
- ipv4.addresses: ""
- connection.autoconnect: "yes"

After configuration, confirm that the following parameters are set for ethX by using the nmcli connection show command.

- connection.type: "802-3-ethernet"
- connection.id: "ethX"

- connection.interface-name: "ethX"

Create a VLAN interface using the nmcli connection add command.

```
# /usr/bin/nmcli connection add type vlan con-name ethX.Y ifname ethX.Y
vlan.parent ethX vlan.id Y
```

Set the following parameters for the created ethX.Y using the nmcli connection modify command.

- ipv4.method: "manual"
- ipv4.addresses: "XXX.XXX.XXX.XXX/XX"
- connection.autoconnect: "no"

### Setup 5

Set the following parameters with the "nmcli connection modify" command.

- connection.interface-name: "ethX"
- connection.autoconnect: "yes"
- ipv4.method: "disabled"
- ipv6.method: "disabled"

After configuration, confirm that the following parameters are set for the ethX with the "nmcli connection show" command.

- connection.type: "802-3-ethernet"
- connection.id: "ethX"
- connection.interface-name: "ethX"

### Information

If you want to use the NIC switching mode to share the same physical connection between two virtual interfaces (one that bundles physical interfaces and the other that bundles tagged VLAN interfaces), you need to set up ifcfg-ethX the same as Setup 1 using the same IP address (ipv4.addresses:) and other values. For example, if sha0 bundles eth0 and eth1, and sha1 bundles eth0.2 and eth1.2, configure eth0 according to ethX in Setup 1, not according to that shown in Setup 3.

## (2) Verification of the physical interface

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

Also, if the physical interface is UP, check whether "LOWER\_UP" is displayed. If "LOWER\_UP" 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.

```
# ip addr show
eth0    <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
        link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
        inet 192.168.70.2/24 brd 192.168.70.255 scope global eth0
        valid_lft forever preferred_lft forever
        inet6 fe80::xxx:xxxx:xxxx:xxxx/64 scope link
        valid_lft forever preferred_lft forever
eth1    <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
        link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
        inet 192.168.71.2/24 brd 192.168.71.255 scope global eth1
        valid_lft forever preferred_lft forever
        inet6 fe80::xxx:xxxx:xxxx:xxxx/64 scope link
        valid_lft forever preferred_lft forever
```

In the above example, it is possible to use eth0 and eth1. For details on the ip 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) Route configuration

Route configuration is described below.

## Default gateway configuration

For RHEL8

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

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

```
DEVICE=ethX
(omitted)
GATEWAY=192.168.1.254
```



## 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](#)".

For RHEL9

Execute the following command to set the default gateway.

```
# /usr/bin/nmcli connection modify filename /etc/NetworkManager/system-connections/
ethX.nmconnection +ipv4.gateway "192.168.1.254"
```

## Static route configuration

For RHEL8

- NIC switching mode

To configure a static route on a routing table, use the nmcli command.

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



Example: Setting static route to ethX and ethY

```
#/usr/bin/nmcli connection modify filename /etc/sysconfig/network-  
scripts/ifcfg-ethX +ipv4.routes "192.168.100.0/24 192.168.40.10"  
#/usr/bin/nmcli connection modify filename /etc/sysconfig/network-  
scripts/ifcfg-ethY +ipv4.routes "192.168.100.0/24 192.168.40.10"
```

For information about configure static routes, refer to "Linux documentation".

When using source routing, the above configuration is not required.

Make sure that use "2.8.2 User command execution function" and execute the nmcli command to add or delete the setting of source routing.

Example: /etc/opt/FJSVhanet/script/interface/shaX

```
#!/bin/sh  
#  
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2004  
#  
#ident "%W% %G% %U% - FUJITSU"  
#  
(omitted)  
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 $INTERFACE  
#fi  
;;  
'after')  
#  
# script after activate interface  
#  
IFNAME=`/usr/sbin/ip addr show | /usr/bin/grep " 192.168.40.1/" | \  
/usr/bin/sed -e "s/.* //"`  
/usr/bin/nmcli connection modify \  
filename /etc/sysconfig/network-scripts/ifcfg-$IFNAME \  
+ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"  
/usr/bin/nmcli device modify $IFNAME \  
+ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"  
(omitted)  
'inactivate')  
#  
# inactivate interface  
#  
case "$2" in  
'before')  
#  
#
```

```
# script before inactivate interface
#
IFNAME=`/usr/sbin/ip addr show | /usr/bin/grep " 192.168.40.1/" | \
/usr/bin/sed -e "s/.*/ /"`
/usr/bin/nmcli connection modify \
filename /etc/sysconfig/network-scripts/ifcfg-$IFNAME \
-ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
/usr/bin/nmcli device modify $IFNAME \
-ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
(omitted)
```

#### - Virtual NIC mode and GS linkage mode

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

Make sure that configure it for the virtual interface (route-shaX).

Example: Setting `BOOTPROTO=none` to `ifcfg-shaX`

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

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

When using source routing, only the virtual NIC mode supports source routing using the `/etc/sysconfig/network-scripts/rule-shaX` file.

For details, refer to "Linux documentation".

For RHEL9

#### - NIC switching mode

To configure a static route on a routing table, use the `nmcli` command.

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

Example: Setting static route to `ethX.nmconnection`

```
#!/usr/bin/nmcli connection modify filename /etc/NetworkManager/
system-connections/ethX.nmconnection +ipv4.routes "192.168.100.0/24
192.168.40.10"
#!/usr/bin/nmcli connection modify filename /etc/NetworkManager/
system-connections/ethX.nmconnection +ipv4.routes "192.168.100.0/24
192.168.40.10"
```

When using source routing, the above configuration is not required.

Make sure that use "[2.8.2 User command execution function](#)" and execute the `nmcli` command to add or delete the setting of source routing.

Example: `/etc/opt/FJSVhanet/script/interface/shaX`

```
#!/bin/sh
#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2004
#
#ident "%W% %G% %U% - FUJITSU"
#
(omitted)
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 $INTERFACE
#fi
;;
'after')
#
# script after activate interface
#
IFNAME=`/usr/sbin/ip addr show | /usr/bin/grep " 192.168.40.1/" | \
/usr/bin/sed -e "s/.*/ /"`
/usr/bin/nmcli connection modify \
filename /etc/NetworkManager/system-connections/$IFNAME.nmconnection \
+ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
/usr/bin/nmcli device modify $IFNAME \
+ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
(omitted)
'inactivate')
#
# inactivate interface
#
case "$2" in
'before')
#
# script before inactivate interface
#
IFNAME=`/usr/sbin/ip addr show | /usr/bin/grep " 192.168.40.1/" | \
/usr/bin/sed -e "s/.*/ /"`
/usr/bin/nmcli connection modify \
filename /etc/NetworkManager/system-connections/$IFNAME.nmconnection \
-ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
/usr/bin/nmcli device modify $IFNAME \
-ipv4.routes "192.168.100.0/24 192.168.40.10 src=192.168.40.1"
(omitted)

```

#### - Virtual NIC mode

To configure a static route on a routing table, set the following parameter to the virtual interface with the "nmcli connection modify" command.

- ipv4.routes: "192.168.100.0/24 192.168.40.10"

When using source routing, set the following parameter to the virtual interface with the "nmcli connection modify" command.

- ipv4.routes: "192.168.100.0/24 192.168.40.10 src=192.168.40.1"

### 3.2.2.2 System setup in Fast switching mode



This version does not support IPv6 addresses for the Fast switching mode.

### When using an IPv4 address

- 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 configured in the redundant line control function in the /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.

### 3.2.2.3 System setup in NIC switching mode



#### Note

This version does not support IPv6 addresses for the NIC switching mode.

### When using an IPv4 address

- 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, monitored IP addresses to be specified in monitoring destination information) and a host name configured in the redundant line control function in the /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.

### 3.2.2.4 System setup in Virtual NIC mode

#### For RHEL8

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

The descriptions vary depending the OS. See "[Table 3.10 Configuration of physical interface](#)" for the differences in descriptions.

Table 3.10 Configuration of physical interface

Item	Value (Example)	Description
TYPE	Ethernet	Specify the device type. Set "Ethernet".
BOOTPROTO	none	Specify the protocol when getting the IP address. Set "none" or "static".
DEVICE	ethX	Specify the device name. Set "ethX".
ONBOOT	yes	Select whether to start the physical interface on startup of the OS. Set "yes".
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

```
TYPE=Ethernet
BOOTPROTO=none
```

```
DEVICE=ethX
ONBOOT=yes
```

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.

## For RHEL9

Set the following parameters to the physical interfaces with the `nmcli` command.

- `connection.interface-name`: `"ethX"`
- `connection.type`: `"802-3-ethernet"`
- `connection.autoconnect`: `"yes"`
- `802-3-ethernet.mtu`: the same value for the configuration of the primary, secondary and virtual interface.
- `ipv4.method`: `"disabled"` or `"manual"`



### Point

- An address such as `IPADDR` is not necessary. Do not set it.
- If you need to prevent device names of physical NICs from changing to unexpected names in an environment where traditional interface names (`ethX`) for RHEL6 or earlier are used, describe the definition of `"HWADDR=<MAC address>"` in the settings for the physical interfaces (the `/etc/sysconfig/network-scripts/ifcfg-ethX` file).
- When modifying MTU, make sure to set 1280 or more.

### 3.2.2.5 System setup in GS linkage mode

- 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.
- In RHEL8, be sure to define static route information in the `/etc/sysconfig/network-scripts/route-shaX` file to use the virtual gateway to communicate with the remote host. In RHEL9, static routing information is set automatically and does not need to be defined manually.
- You do not need to configure the routing daemon for the network setting when using this method.

## 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

When adding the settings of Fast switching mode and GS linkage mode, make sure to execute the configuration command 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. Setup 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

- Ensure to specify the same IP address configured in "/etc/sysconfig/network-scripts/ifcfg-ethX" in RHEL8 or in the "nmcli connection modify" command in RHEL9, 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.
- 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 "[H.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. There is no need to set the standby patrol function to each virtual interface.
- 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 the 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. Set up the monitoring destination information by using the "hanetpathmon target" command. For details, see "[7.12 hanetpathmon Command](#)".

- When setting the tagged VLAN interface on the virtual interface, describe the tagged VLAN interface name in `/etc/NetworkManager/NetworkManager.conf`.

Then, execute `systemctl reload NetworkManager.service`.

#### Configuration of virtual interface

##### For RHEL8

Edit the setting (`/etc/sysconfig/network-scripts/ifcfg-shaX` file) for a virtual interface. See "[Table 3.11 Configuration of virtual interface \(RHEL8\)](#)", and "[Table 3.12 Configuration of tagged VLAN interface set on virtual interface \(RHEL8\)](#)".

Table 3.11 Configuration of virtual interface (RHEL8)

Item	Value (Example)	Description
DEVICE	ethX	Specify the device name. Set "ethX".
IPADDR	192.168.1.1	Specify the IPv4 address.
IPADDR1	192.168.1.2	Specify this item when using multiple IPv4 addresses. IPADDR1 is the second IP address. When setting more addresses, specify this item as IPADDR2, IPADDR3.
PREFIX	24	Specify the prefix for the IPv4 address.
PREFIX1	24	Specify this item when using prefixes for multiple IPv4 addresses. PREFIX1 is the prefix for IPADDR1. When setting more prefixes, specify this item as PREFIX2, PREFIX3.
BOOTPROTO	none	Specify the protocol when getting the IP address. Set "none" or "static".
ONBOOT	yes	Select whether to start the virtual interface on startup of the OS. Set "yes". When the virtual interface is registered as a cluster resource, it is started regardless of this setting.
TYPE	Ethernet	Specify the device type. Set "Ethernet".
GATEWAY	192.168.1.254	Specify the IP address when setting the default gateway.
IPV6INIT	yes	Specify "yes" when assigning the IPv6 address.
IPV6_AUTOCONF	yes or no	Specify "yes" when the IPv6 address is automatically configured. Specify "no" when the IPv6 address is not automatically configured.
IPV6ADDR	fec0:1::1/64	Specify the IPv6 address.
IPV6ADDR_SECONDARIES	fec0:1::2/64	Specify this item when using multiple IPv6 addresses. When using two or more IPv6 addresses, specify this item as follows. IPV6ADDR_SECONDARIES="fec0:1::2/64 fec0:1::3/64"
IPV6_DEFAULTGW	fec0:1::3	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 ( <code>ifcfg-ethX</code> ) of the primary interface and the secondary interface, and for the virtual interface configuration file ( <code>ifcfg-shaX</code> ).
SHAMACADDR	XX:XX:XX:XX:XX:XX	Specify the MAC address.  - If specifying the MAC address The specified address is set.

Item	Value (Example)	Description
		- 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
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

[For IPv6]

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fec0:1::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

[For DualStack]

```
DEVICE=sha0
IPADDR=192.168.1.1
PREFIX=24
IPV6INIT=yes
IPV6ADDR=fec0:1::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

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

```
DEVICE=sha0
IPADDR=192.168.1.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
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.

Table 3.12 Configuration of tagged VLAN interface set on virtual interface (RHEL8)

Item	Value (Example)	Description
VLAN	yes	Specify this item when using VLAN. Set "yes".
TYPE	Vlan	Specify the device name. Set "Vlan".
PHYSDEV	sha0	Specify the interface to which VLAN is assigned. Specify the virtual interface of GLS.
VLAN_ID	2	Specify VLAN_ID.



Item	Value (Example)	Description
IPADDR	192.168.1.1	Specify the IPv4 address.
IPADDR1	192.168.1.2	Specify this item when using multiple IPv4 addresses. IPADDR1 is the second IP address. When setting more addresses, specify this item as IPADDR2, IPADDR3.
PREFIX	24	Specify the prefix.
PREFIX1	24	Specify this item when using prefixes for multiple IPv4 addresses. PREFIX1 is the prefix for IPADDR1. When setting more prefixes, specify this item as PREFIX2, PREFIX3.
BOOTPROTO	none	Specify the protocol when getting the IP address. Set "none" or "static".
IPV6INIT	yes	Specify "yes" when assigning the IPv6 address.
IPV6_AUTOCONF	yes or no	Specify "yes" when the IPv6 address is automatically configured. Specify "no" when the IPv6 address is not automatically configured.
IPV6ADDR	fec0:1::1/64	Specify the IPv6 address.
IPV6ADDR_SECONDARIES	fec0:1::2/64	Specify this item when using multiple IPv6 addresses. When using two or more IPv6 addresses, specify this item as follows. IPV6ADDR_SECONDARIES="fec0:1::2/64 fec0:1::3/64"

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

[For IPv4]

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=2
IPADDR=192.168.100.1
PREFIX=24
BOOTPROTO=none
```

[For IPv6]

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=2
IPV6INIT=yes
IPV6ADDR=fec0:100::1/64
BOOTPROTO=none
```

[For DualStack]

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=2
IPADDR=192.168.100.1
PREFIX=24
IPV6INIT=yes
IPV6ADDR=fec0:100::1/64
BOOTPROTO=none
```

Describe the tagged VLAN interface name in /etc/NetworkManager/NetworkManager.conf.

Example of /etc/NetworkManager/NetworkManager.conf

```
[main]
...
ignore-carrier=sha0.1, sha0.2, sha0.3
```

**For RHEL9**

Edit the setting for a virtual interface (shaX) with the nmcli command. See "[Table 3.13 Configuration of virtual interface \(RHEL9\)](#)", and "[Table 3.14 Configuration of tagged VLAN interface on virtual interface \(RHEL9\)](#)."

**Table 3.13 Configuration of virtual interface (RHEL9)**

Item	Value (Example)	Description
connection.id connection.interface-name	shaX	Specify the device name. Set "shaX".
connection.autoconnect	yes	Select whether to start the virtual interface on startup of the OS. Set "yes". When the virtual interface is registered as a cluster resource, it is started regardless of this setting.
connection.type	802-3-ethernet	Specify the device type. Set "802-3-ethernet".
connection.master	br0	Specify the name of the virtual bridge which is to be connected to the virtual interface.
connection.slave-type	bridge	Set "bridge" if the virtual bridge is to be connected to the virtual interface, otherwise, empty.
802-3-ethernet.mtu	9000	Specify the length of MTU. When specifying the length of MTU, set the same value for the configuration of primary, secondary, and virtual interface.
ipv4.method	manual	Specify the protocol when getting the IP address. Set "manual" or "disabled".
ipv4.addresses	192.168.1.1/24, 192.168.1.2/24	Specify the pairs of IPv4 address and prefix.
ipv4.gateway	192.168.1.254	Specify the IP address when setting the default gateway.
ipv6.method	manual	Specify the protocol when getting the IPv6 address. Set "manual" or "disabled".
ipv6.addresses	fec0:1::1/64, fec0:1::2/64	Specify the pairs of IPv6 address and prefix.
ipv6.gateway	fec0:1::3	Specify the IPv6 address when setting the default gateway if IPv6.

When creating a tagged VLAN interface (shaX.Y) of which VLAN-ID is Y on a virtual interface (shaX), edit the setting for a tagged VLAN interface (shaX.Y) with the nmcli command. The effective range of VLAN-ID which can be specified is from 1 to 4094.

**Table 3.14 Configuration of tagged VLAN interface on virtual interface (RHEL9)**

Item	Value (Example)	Description
connection.interface-name	sha0.2	Specify the device name. Set "shaX.Y".
connection.autoconnect	yes	Select whether to start the tagged VLAN interface on startup of the OS. Set "yes".
connection.type	vlan	Specify the device type. Set "vlan".

Item	Value (Example)	Description
vlan.parent	sha0	Specify the interface to which VLAN is assigned. Specify the virtual interface of GLS.
vlan.id	2	Specify VLAN ID. Set "Y".
ipv4.method	manual	Specify the protocol when getting the IP address. Set "manual" or "disabled".
ipv4.addresses	192.168.1.1/24, 192.168.1.2/24	Specify the pairs of IPv4 address and prefix.
ipv6.method	manual	Specify the protocol when getting the IPv6 address. Set "manual" or "disabled".
ipv6.addresses	fec0:1::1/64, fec0:1::2/64	Specify the pairs of IPv6 address and prefix.

Describe the tagged VLAN interface name in /etc/NetworkManager/NetworkManager.conf.

Example of /etc/NetworkManager/NetworkManager.conf

```
[main]
...
ignore-carrier=sha0.1, sha0.2, sha0.3
```

## Note

- In the Virtual NIC mode, you cannot share physical interfaces with other virtual interfaces.
- Just as for the standard interface of the operating system, define the settings of the IP address and the netmask in the interface setting file (/etc/sysconfig/network-scripts/ifcfg-shaX) in the 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 the 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 or Hyper-V, 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.
- When using the Virtual NIC mode on the guest OS of Hyper-V, check [Enable MAC address spoofing] when creating network adapters bundled by GLS on the Hyper-V Manager.
- When using the Virtual NIC mode on the guest OS of Hyper-V, a tagged VLAN interface cannot be used. For a tagged VLAN connection, specify the VLAN ID when setting the network adapter of a guest OS.
- 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).
- For RHEL9, use the "hanetconfig" command to specify SHAMACADDR. See "[7.1 hanetconfig Command](#)" for more information.

- For RHEL9, do not directly edit the virtual interface configuration file (/etc/NetworkManager/system-connections/shaX.nmconnection). Use the nmcli command to edit the settings.
- The setting of /etc/NetworkManager/NetworkManager.conf is required to control the processing of NetworkManager for tagged VLAN interfaces and manage the processing in GLS. Make sure to set /etc/NetworkManager/NetworkManager.conf.
- When modifying MTU, make sure to set 1280 or more.
- When setting a takeover IP address by using the hanethvrsc command, the name format "shaX-NN" cannot be used for the host name. (Example: sha0-65)

### 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

- When changing the interfaces bundled by Fast switching mode and GS linkage mode, make sure to execute the configuration command 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)	1-1	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
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 1-1

Perform one of the following procedures after changing settings.

- Deactivate the target virtual interface, execute `systemctl reload NetworkManager.service`, and then activate the target virtual interface.
- Reboot the system.
- Execute `systemctl reload NetworkManager.service`, and then 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.

## 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

- 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
```

- Change the monitoring destination.

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

- 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 the 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)	1-1	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
IP address to monitor HUB (-p)	4	4
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

hanetpoll command	Single	Cluster
Link up waiting period (-p)	3	3
Link status monitoring (-l)	3	3

Network configuration of OS	Single	Cluster
Connection profile and configuration file of NetworkManager (/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.

- Activate the target virtual interface.
- Reboot the system.
- Execute the "resethanet -s" command.

### Procedure 1-1

Perform one of the following procedures after changing settings.

- Execute systemctl reload NetworkManager.service, and then activate the target virtual interface.
- Execute systemctl reload NetworkManager.service, and then execute the "resethanet -s" command.
- Reboot the system.

### 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 the operations after executing the command to change settings. No distribution procedure is required. However, when the setting is changed by "hanetpoll devparam" command, perform one of the following procedures.

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

#### Procedure 6

Make sure to reboot the system instead of manually restarting the network service.

### 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 details.
2. Deactivate a virtual interface to change using a "stphanet" command. See "[7.3 stphanet Command](#)" for details.  
This step is not required if the IP address to monitor HUB is changed by the hanetpoll command.
3. Change the setup information and common parameter. (For changing monitoring period, the number of monitoring times, cluster switching, link up period, and link status monitoring, apply changes with "hanetpoll on" command.)  
See "[7.1 hanetconfig Command](#)," "[7.5 hanetmask Command](#)," and "[7.7 hanetpoll Command](#)" for details.
4. Activate the deactivated virtual interface in procedure 2 using a "strhanet" command. See "[7.2 strhanet Command](#)" for details.  
This step is not required if the IP address to monitor HUB is changed by the hanetpoll command.
5. Starts a function to monitor HUB using a "hanetpoll on" command.  
(For changing monitoring period, the number of monitoring times, cluster switching, link up period, and link status monitoring, apply changes with "hanetpoll on" command)  
See "[7.7 hanetpoll Command](#)" for details.

When changing only the parameter, change the monitoring period, the number of monitoring times, cluster switching, link up period, and link status monitoring with "hanetpoll on" command. For details, see "[7.7 hanetpoll Command](#)."

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
  - Cluster switching
  - Link up waiting time

- Link status monitoring

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

- Ensure to specify the same IP address configured in "/etc/sysconfig/network-scripts/ifcfg-ethX" in a RHEL8 environment or in the "nmcli connection modify" command in a RHEL9 environment when specifying physical IP address by "hanetconfig" command using '-i' or '-e' option. In a RHEL 9 environment, be sure to specify the same IP address that is configured in "/etc/NetworkManager/system-connections/ethX.nmconnection". 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.
- 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
  link detection    = YES
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 "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 "activate the target virtual interface" procedure is used.

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

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
  link detection    = YES
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/stpctl -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. Start HUB monitoring and the standby patrol.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
# /opt/FJSVhanet/usr/sbin/strctl -n sha1
```

6. Start the cluster operation.

### [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
link detection = YES
FAILOVER Status = YES
Name          HUB Poll Hostname
+-----+-----+-----+-----+-----+
sha0          OFF   192.168.10.250,192.168.10.251

```

2. Change the monitoring interval.

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

### 3.4.3 Virtual NIC mode

This section describes how to change the settings for the 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, etc.	1	1

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

hanetconfig command (for RHEL9)	Single	Cluster
SHAMACADDR (-s)	6	6

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.

### **Procedure 6**

Perform one of the following procedures after changing settings.

- Activate the target virtual interface.
- Reboot the system.

## **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

For RHEL8, 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 RHEL9, you can configure the same settings with the `nmcli` command. 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 IP address of the virtual interface by using the ip command.

```
# /usr/sbin/ip addr show sha0
sha0      <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 1000
         link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
         inet 192.168.80.10/24 brd 192.168.80.255 scope global sha0
         valid_lft forever preferred_lft forever
         inet6 fe80::XXXX:XXXX:XXXX:XXXX/64 scope link
         valid_lft forever preferred_lft forever
```

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. Change the IP address of the virtual interface.

- For RHEL8

Edit the network setting file of the virtual interface.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters with the "nmcli connection modify" comand.

- ipv4.method: "manual"
- ipv4.addresses: "192.168.80.1/24"

- 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
```

- 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
+-----+-----+---+---+-----+
```

- Check the IP address of the virtual interface by using the ip command.

```
# /usr/sbin/ip addr show sha0
sha0      <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 1000
         link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
         inet 192.168.80.1/24 brd 192.168.80.255 scope global sha0
         valid_lft forever preferred_lft forever
         inet6 fe80::XXXX:XXXX:XXXX:XXXX/64 scope link
         valid_lft forever preferred_lft forever
```

### [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.

- Check the virtual interface connected to the virtual bridge.

- For RHEL8

```
# ip link show master br0
N: sha0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master
br0 state UP mode DEFAULT group default qlen 1000
    link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
```

- For RHEL9

Execute the following command to display the virtual bridge interface connected to the virtual interface.

```
# nmcli -g connection.master connection show sha0
br0
```

- 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.

- For RHEL8

```
# ip link set dev sha0 nomaster
```

- For RHEL9

Set the following parameters to the virtual interface with the "nmcli connection modify" command.

- connection.slave-type: ""
- connection.master: ""

4. Check the status of the virtual bridge.

- For RHEL8

Execute the following command to make sure that sha0 is not displayed.

```
# ip link show master br0
```

- For RHEL9

Execute the following command to make sure that br0 is not displayed.

```
# nmcli -g connection.master connection show sha0
```

5. Deactivate the virtual interface.

```
# /opt/FJSSVhanet/usr/sbin/stphanet -n sha0  
# /opt/FJSSVhanet/usr/sbin/stphanet -n shal
```

6. Check the status of the virtual interface.

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

7. Edit the network setting of the virtual interface.

- For RHEL8

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

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

[Before modification]

```
DEVICE=sha0  
BOOTPROTO=none  
ONBOOT=yes  
TYPE=Ethernet  
BRIDGE=br0
```

[After modification]

```
DEVICE=sha0
IPADDR=192.168.80.10
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

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

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

[Before modification]

```
DEVICE=sha1
IPADDR=192.168.81.10
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

[After modification]

```
DEVICE=sha1
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br0
```

- For RHEL9

Set the following parameters to the virtual interfaces with the "nmcli connection modify" command.

[sha0]

- connection.slave-type: ""
- connection.master: ""
- ipv4.method: "manual"
- ipv4.addresses: "192.168.80.10/24"

[sha1]

- connection.slave-type: "bridge"
- connection.master: "br0"
- ipv4.method: "disabled"

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.

- For RHEL8

```

# ip link show master br0
N: sha1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master
br0 state UP mode DEFAULT group default qlen 1000
    link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff

```

- For RHEL9

```

# nmcli -g connection.master connection show sha1
br0

```

**[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 GIs 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 GIs 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 IP address of the virtual interface by using the ip command.

```

# /usr/sbin/ip addr show sha0
sha0      <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state

```

```
UNKNOWN qlen 1000
    link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.20/24 brd 192.168.20.255 scope global sha0
    valid_lft forever preferred_lft forever
    inet6 fe80::XXXX:XXXX:XXXX:XXXX/64 scope link
    valid_lft forever preferred_lft forever
```

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. Change the IP address of the virtual interface.

- For RHEL8

Edit the network setting file of the virtual interface.

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

```
DEVICE=sha0
IPADDR=192.168.20.10
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters with the "nmcli connection modify" command.

- ipv4.method: "manual"
- ipv4.addresses: "192.168.20.10/24"

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
+-----+-----+-----+-----+-----+
```

- Check the IP address of the virtual interface by using the ip command.

```
# /usr/sbin/ip addr show sha0
sha0    <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UNKNOWN qlen 1000
        link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
        inet 192.168.20.10/24 brd 192.168.20.255 scope global sha0
        valid_lft forever preferred_lft forever
        inet6 fe80::XXXX:XXXX:XXXX:XXXX/64 scope link
        valid_lft forever preferred_lft forever
```

- Start the cluster operation.

### [Example 6]

The following shows the procedure for changing SHAMACADDR of a virtual interface for RHEL9.

- 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
+-----+-----+-----+-----+-----+
```

- Deactivate the virtual interface.

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

- 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
+-----+-----+-----+-----+-----+
```

- Change SHAMACADDR of the virtual interface with "hanetconfig modify" command.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -s auto
```

- Confirm that the change is applied.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print -s
[IPv4,Patrol / Virtual NIC]
Name      Hostname      Mode Physical ipaddr  SHAMACADDR      Interface List
+-----+-----+-----+-----+-----+-----+-----+
sha0      v              auto          eth1,eth2
```

- Activate the virtual interface.

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

### 3.4.4 GS linkage mode

This section describes how to change the settings for the 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 in 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)	1-1	2

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

hanethvrsc 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 1-1

Perform one of the following procedures after changing settings.

- Deactivate the target virtual interface, execute `systemctl reload NetworkManager.service`, and then activate the target virtual interface.
- Deactivate all the virtual interfaces in the GS linkage mode, execute `systemctl reload NetworkManager.service`, and then activate the target virtual interface.
- Reboot the system.
- Execute `systemctl reload NetworkManager.service`, and then 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.



If you modified the `/etc/sysconfig/network-scripts/route-"interface name"` file, you must execute the `"/usr/bin/nmcli connection reload"` command before rebooting the system.

## 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
                                     192.168.10.11,192.168.20.11
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.



### 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](#)".
4. Reboot the system.

### 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 the 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](#)".

When setting a tagged VLAN interface on the target virtual interface

- For RHEL8
  3. Delete the target tagged VLAN interface (/etc/sysconfig/network-scripts/ifcfg-shaX.Y).
  4. Delete the target tagged VLAN interface name from /etc/NetworkManager/NetworkManager.conf.
  5. Reboot the system.
- For RHEL9
  3. Delete the target tagged VLAN interface (shaX.Y) with the nmcli command.
  4. Delete the target tagged VLAN interface name from /etc/NetworkManager/NetworkManager.conf.
  5. Reboot the system.

When not setting a tagged VLAN interface on the target virtual interface

3. Reboot the system.

## 3.5.4 GS linkage mode

---

The following shows the procedure for deleting the 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. In RHEL 8, "hanetconfig delete" deletes the 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 "hanethvsrc create" command. In order to delete the virtual interface, use "hanethvsrc 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 hanethvsrc 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.
- In RHEL8, when deleting the definition in the Virtual NIC mode and the GS linkage mode, the route-"interface name" file is deleted with the ifcfg-"interface name" file. If you need to use the route-"interface name" file again, back up the file.

## 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 the GS linkage mode, it is necessary to set the parameter (logical\_vip\_takeover) beforehand. In this case, perform the following procedure.



#### Information

When configuring the logical virtual interfaces of the GS linkage mode on a virtual interface shaX, the logical virtual interfaces are displayed as the secondary addresses of shaX by the ip command.

#### 1) Setting up the parameter

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

/etc/opt/FJSVhanet/config/ctdl.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

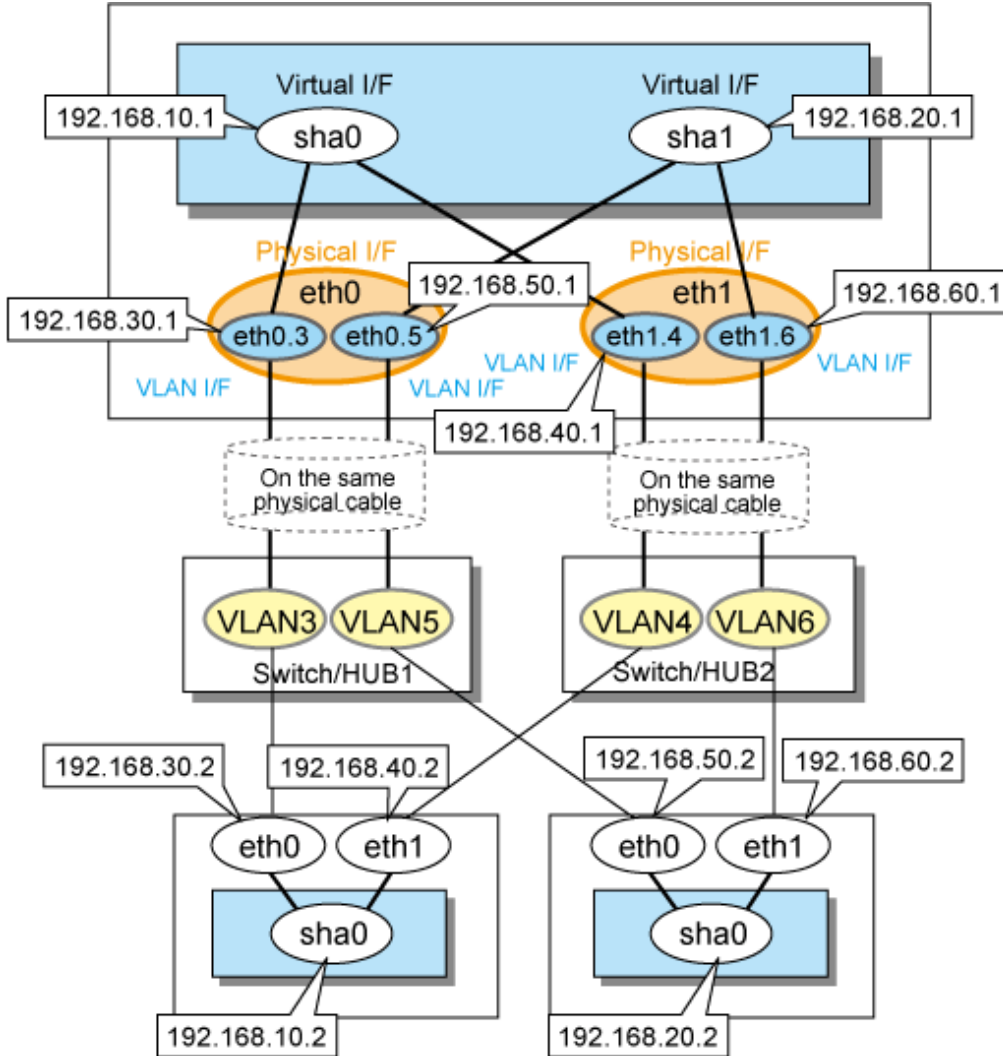
You cannot create a virtual interface by bundling two tagged VLAN interfaces emerged from a single physical interface. Please be sure to specify the tagged VLAN interfaces on disparate physical interfaces when creating a virtual interface for Fast switching mode.



Refer to "7.1 hnetconfig 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 3.15 Synchronous switching and asynchronous switching

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

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

 See

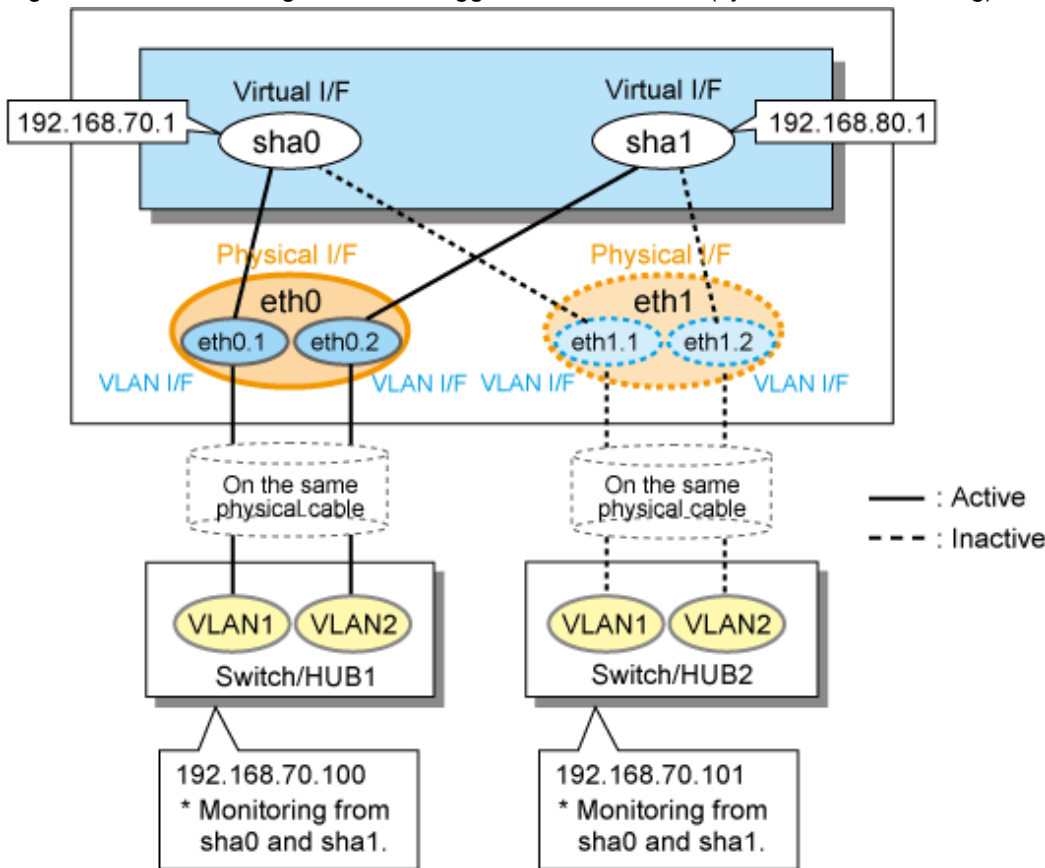
For configuration of monitoring target, refer to "7.7 hanetpoll Command".

### 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.





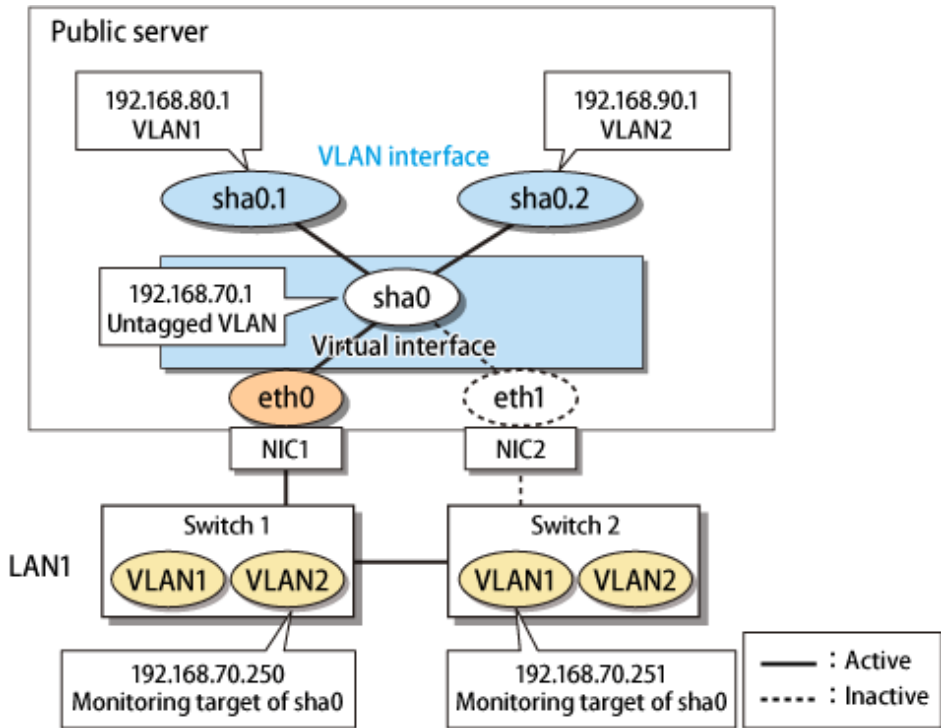
sha0	192.168.10.110	d	192.168.10.10	eth0,eth1
sha1	192.168.12.110	d	192.168.12.10	eth0.2,eth1.2
sha2	-	p	-	sha0
sha3	-	p	-	sha1

### 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

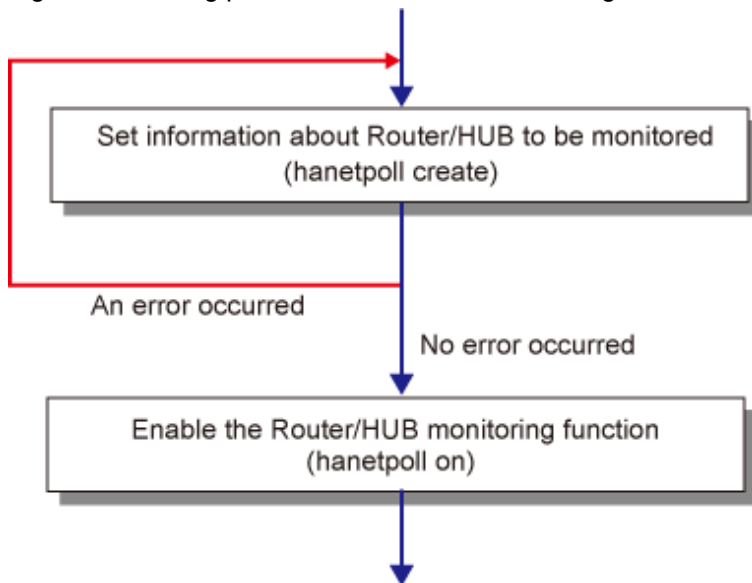
---

### 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.

For more information, see Section "7.7 hanetpoll Command".

---

Figure 3.7 Basic sequence of HUB monitoring

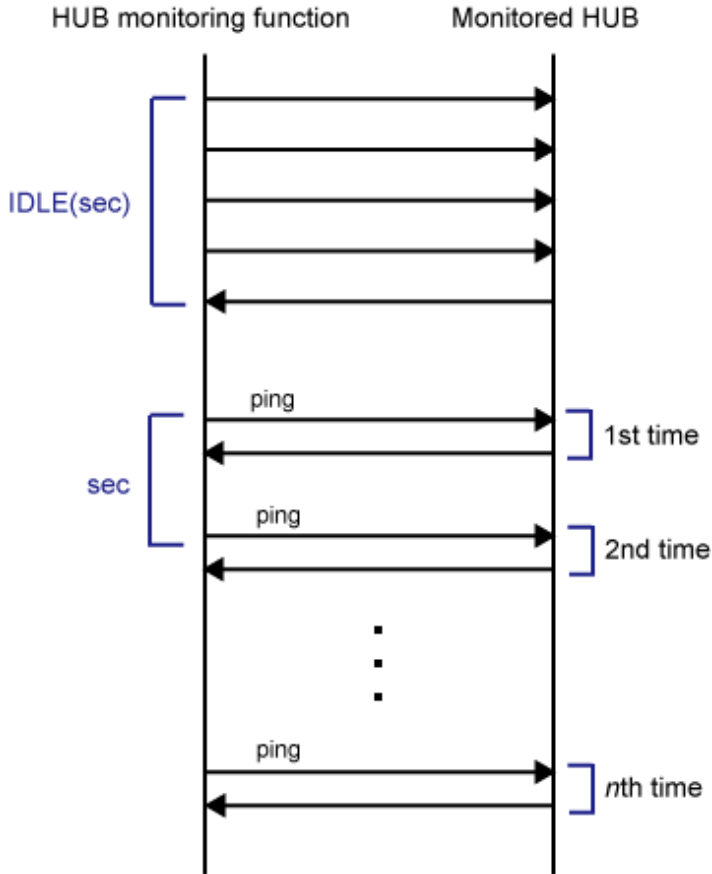
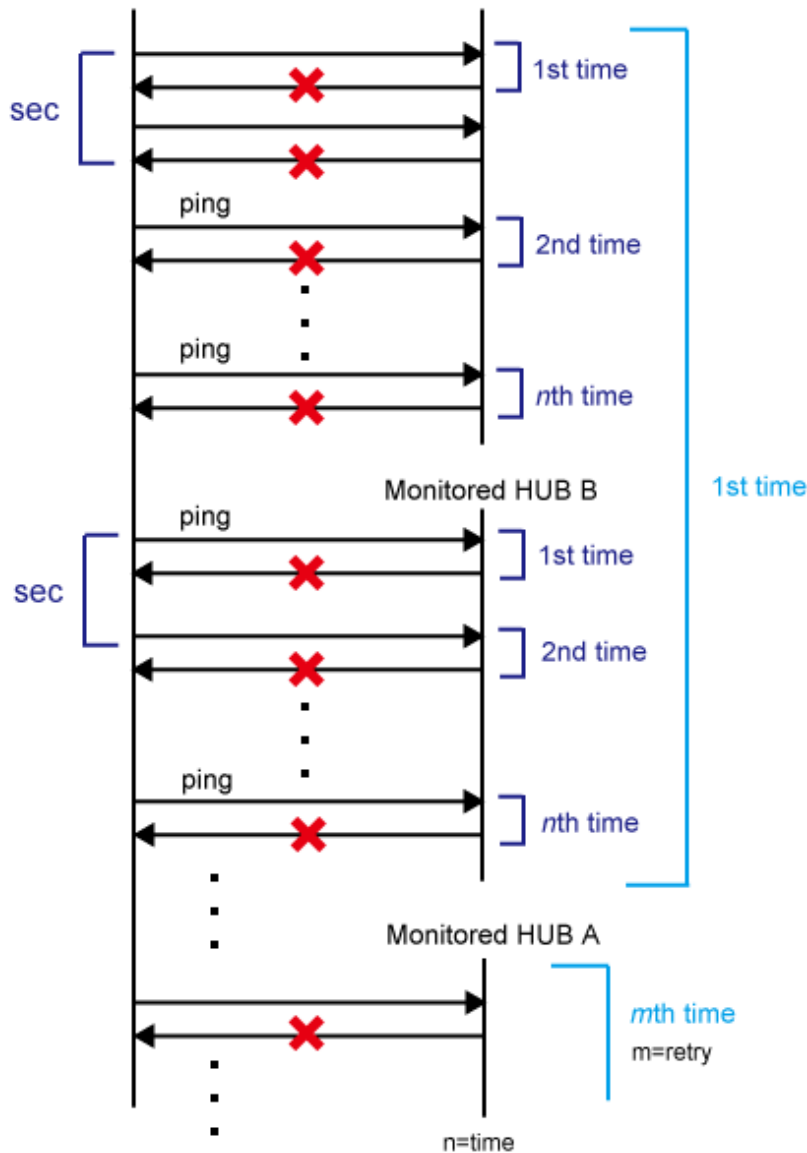


Figure 3.8 HUB monitoring sequence after detect line fault  
HUB monitoring function      Monitored HUB A



### 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. For one monitoring target, the HUB-to-HUB monitoring target is disabled in a NIC redundant configuration or one HUB monitoring target is set in a single physical interface configuration. For two monitoring targets, the HUB-to-HUB monitoring target is enabled in a NIC redundant configuration or two HUB monitoring targets are set in a single physical interface configuration.

#### One monitoring target:

$\text{Error detection time} = \text{monitoring interval (in seconds)} \times (\text{monitoring frequency} - 1) + \text{ping time out period}(*1) + (0 \text{ to monitoring interval (in seconds)})$
--

\*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 is as follows.

$$5 \text{ sec} \times (5 \text{ time} - 1) + 2 \text{ sec} + 0 \text{ to } 5 \text{ sec} = 22 \text{ to } 27 \text{ sec}$$

**Two monitoring targets:**

$$\text{Error detection time} = \text{monitoring interval(in seconds)} \times (\text{monitoring frequency} - 1) + \text{ping time out period} \times 2 \times (\text{0 to monitoring interval(in seconds)})$$

\*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 is as follows.

5 sec x (5 time - 1) + 2 sec x 2 time + 0 to 5 sec = 24 to 29 sec

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

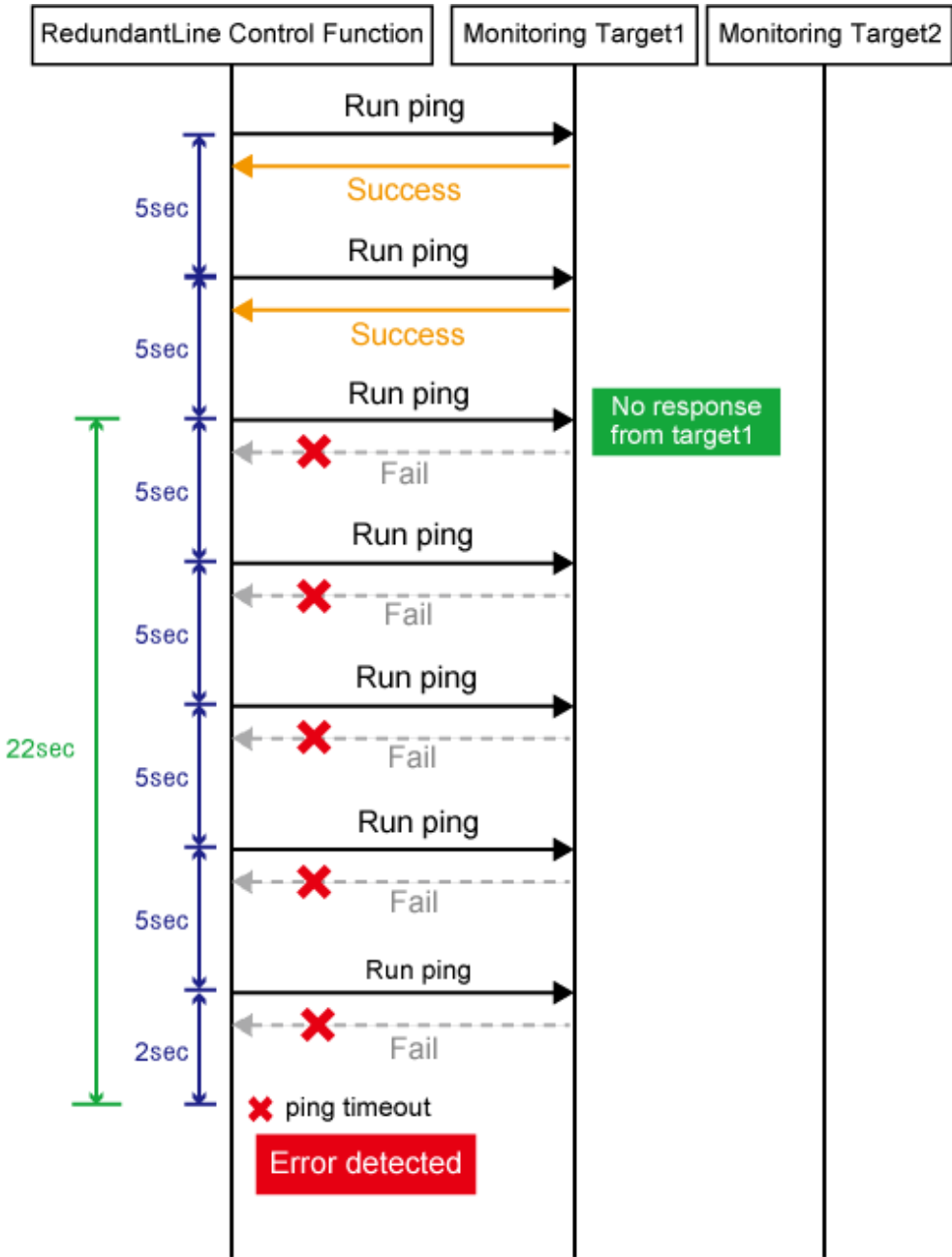
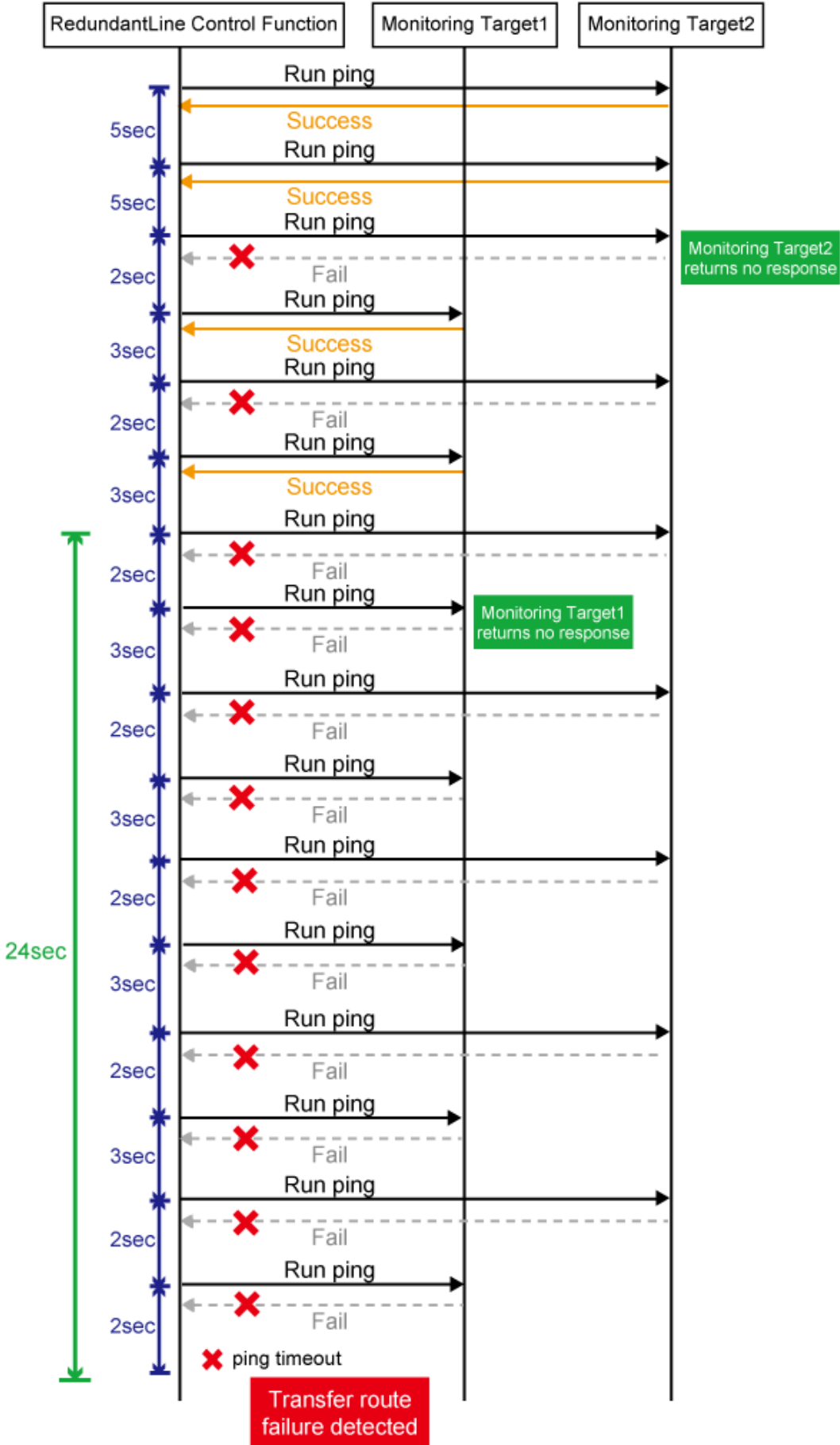


Figure 3.10 Transfer path error detection sequence (two monitoring target)



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 is as follows.

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

**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 is as follows.

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

**When not using monitoring by ping command:**

```
Error detection time = 1 sec + (0 to monitoring interval (in seconds))
```

The default value is as follows.

$$1 \text{ sec} + 0 \text{ to } 5 \text{ sec} = 1 \text{ to } 6 \text{ sec}$$

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

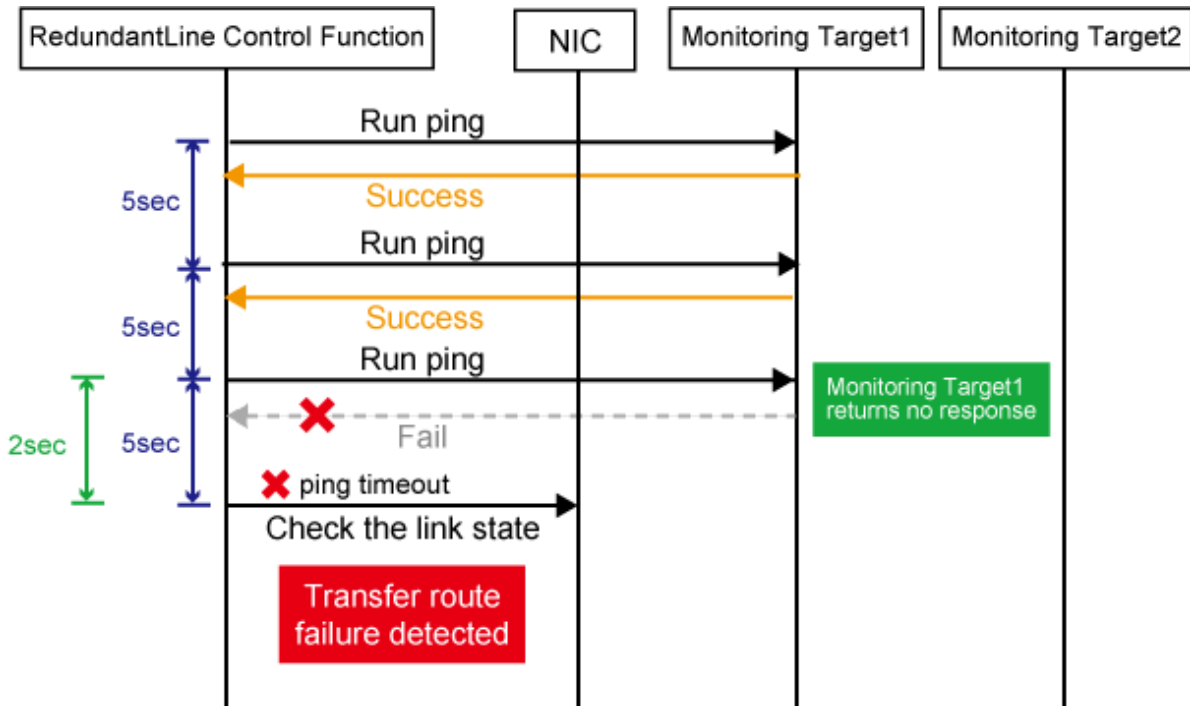




Figure 3.12 Transfer path error detection sequence with link down (two monitoring destinations)

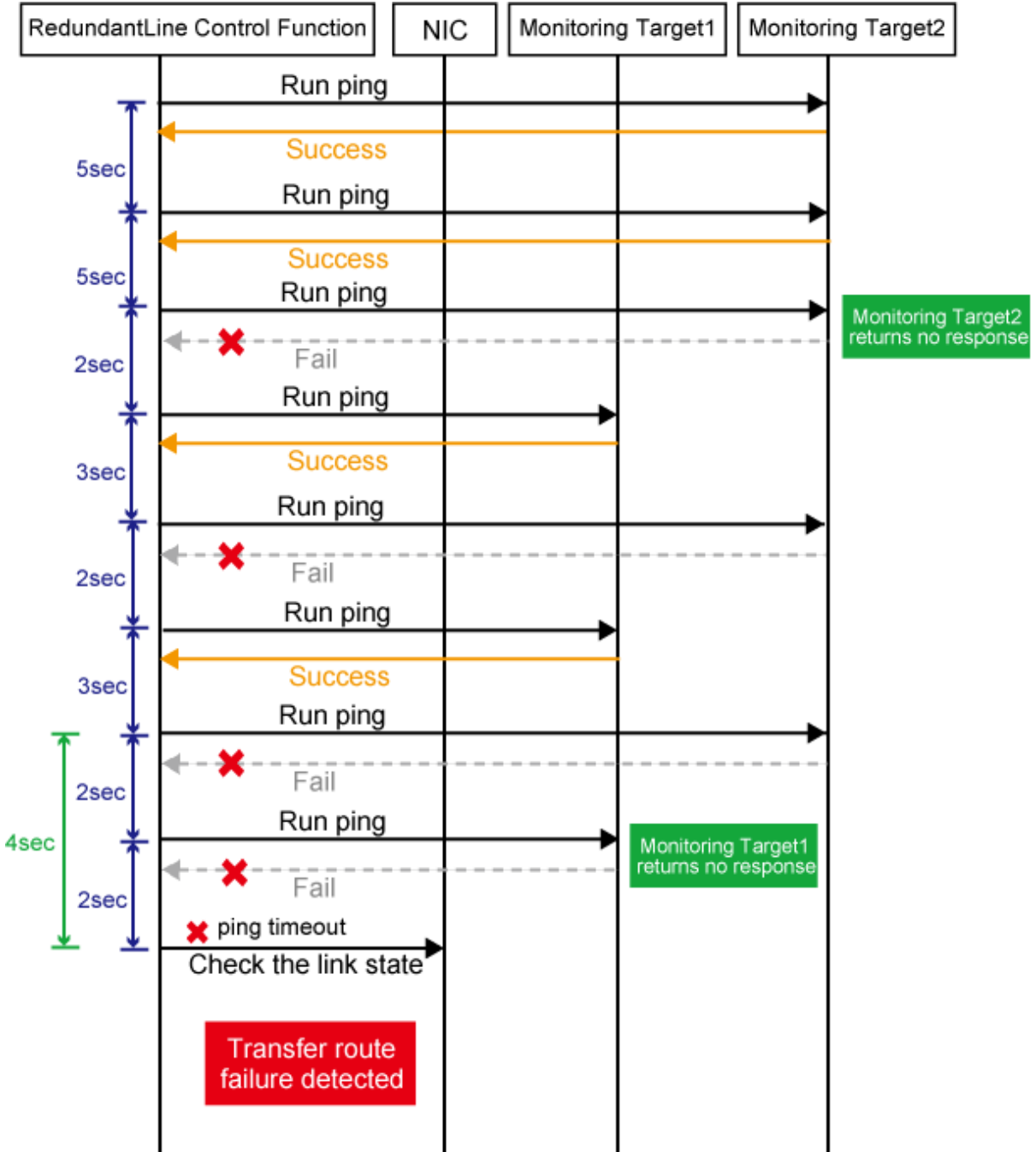
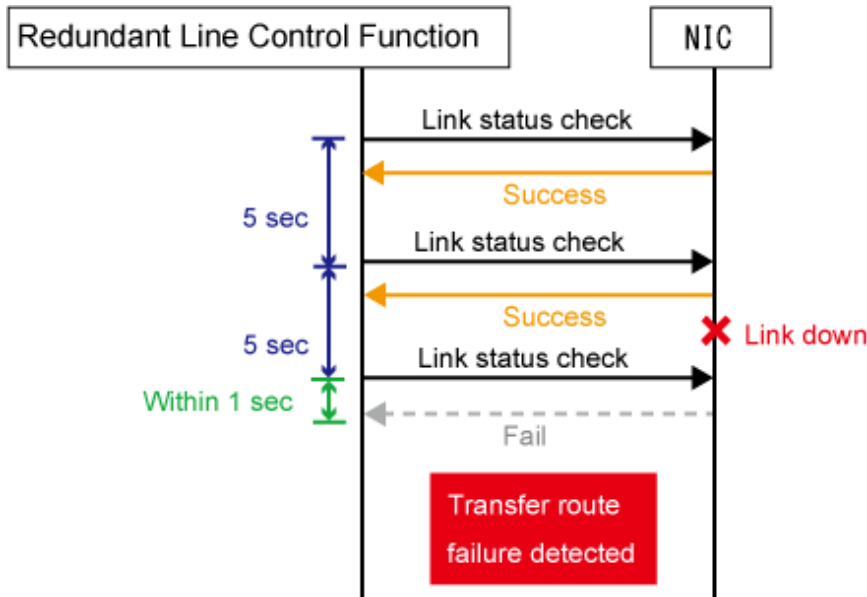


Figure 3.13 Transfer path error detection sequence with link down (when not using monitoring by ping command)



### 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.

### Note

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

## 3.8.2 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.

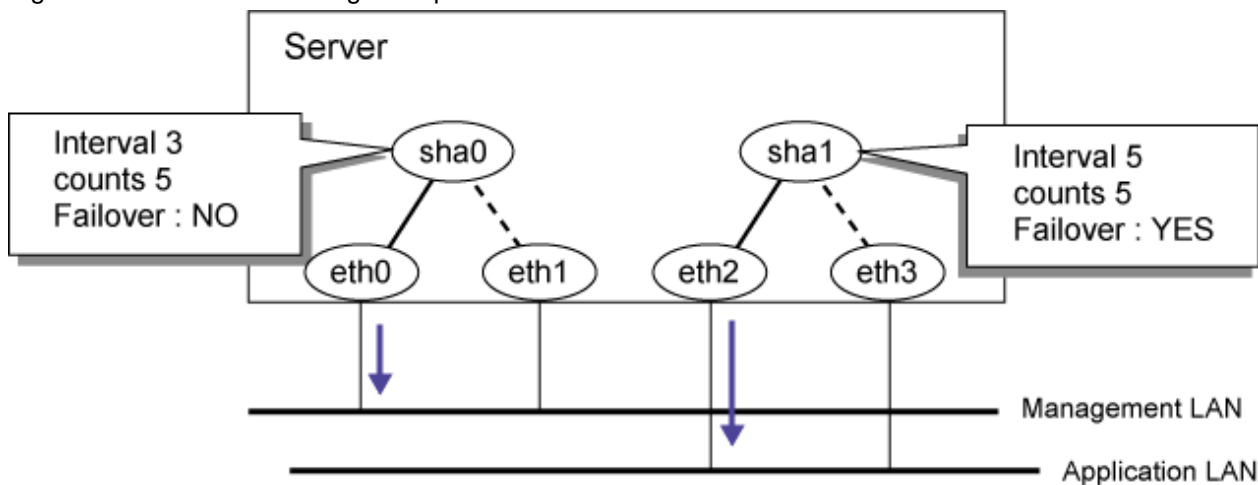
Table 3.16 Available option functions in each mode

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 3.14 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.



## 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.

.....

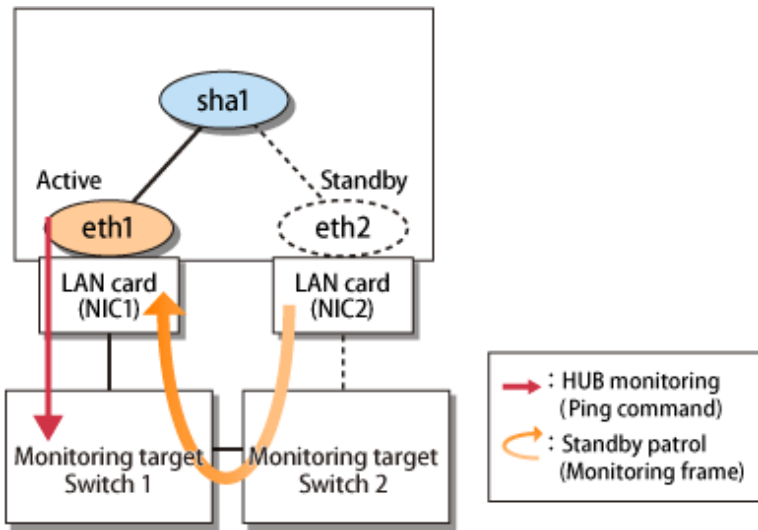
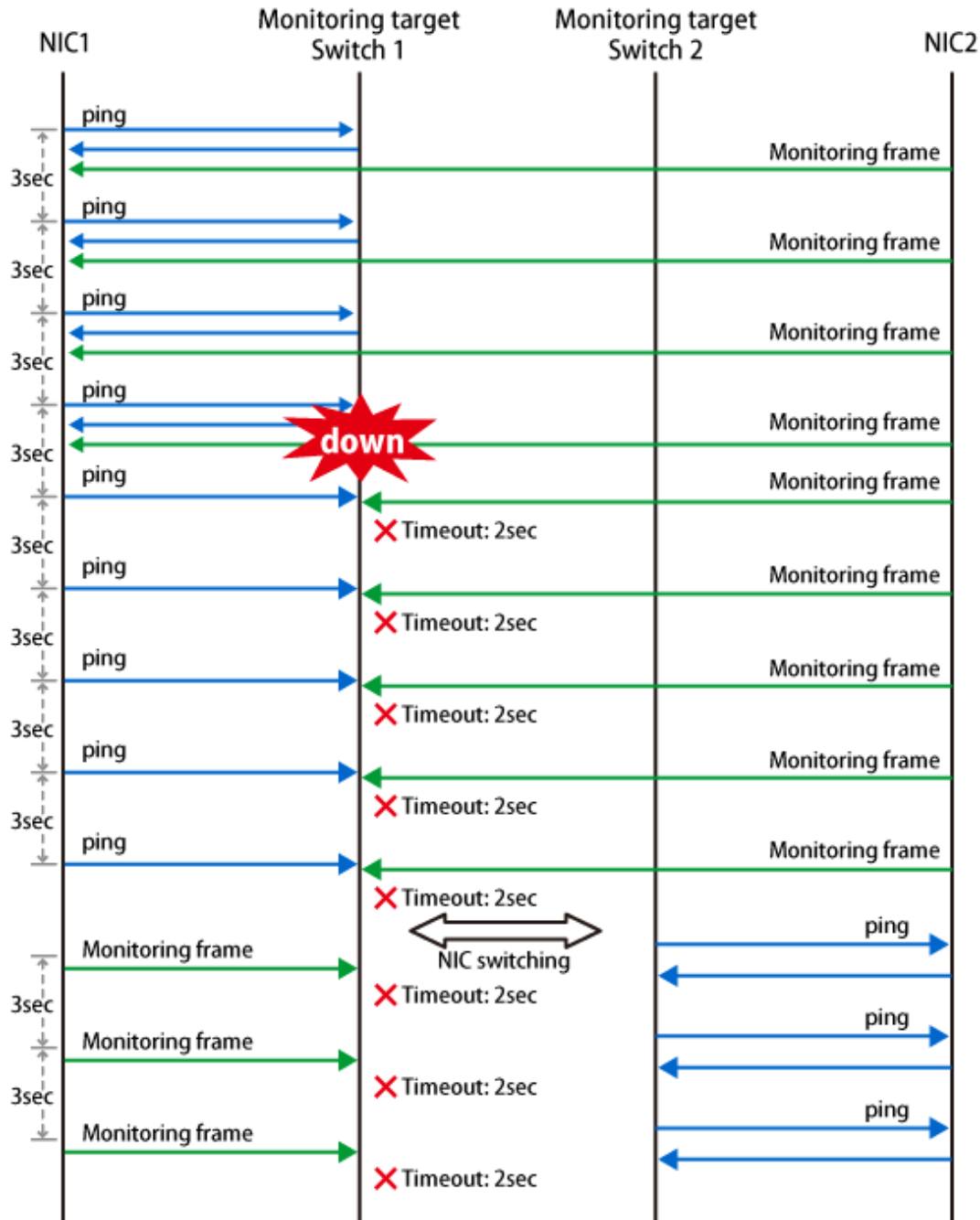


Figure 3.16 Transfer route error detection sequence by network monitoring function



### 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:

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

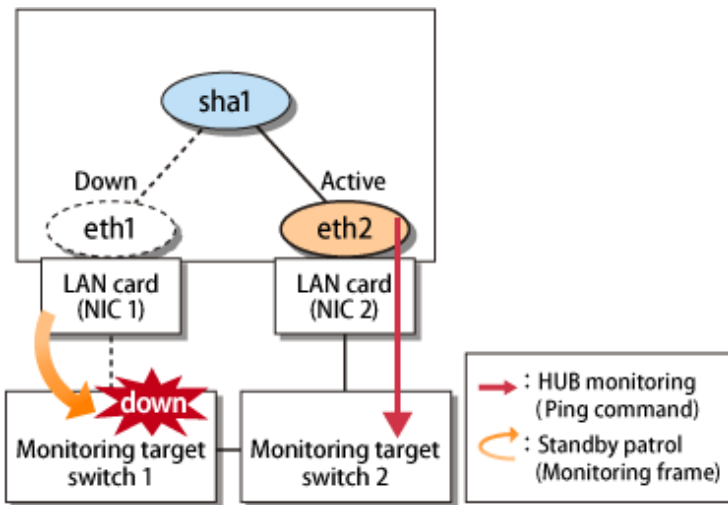
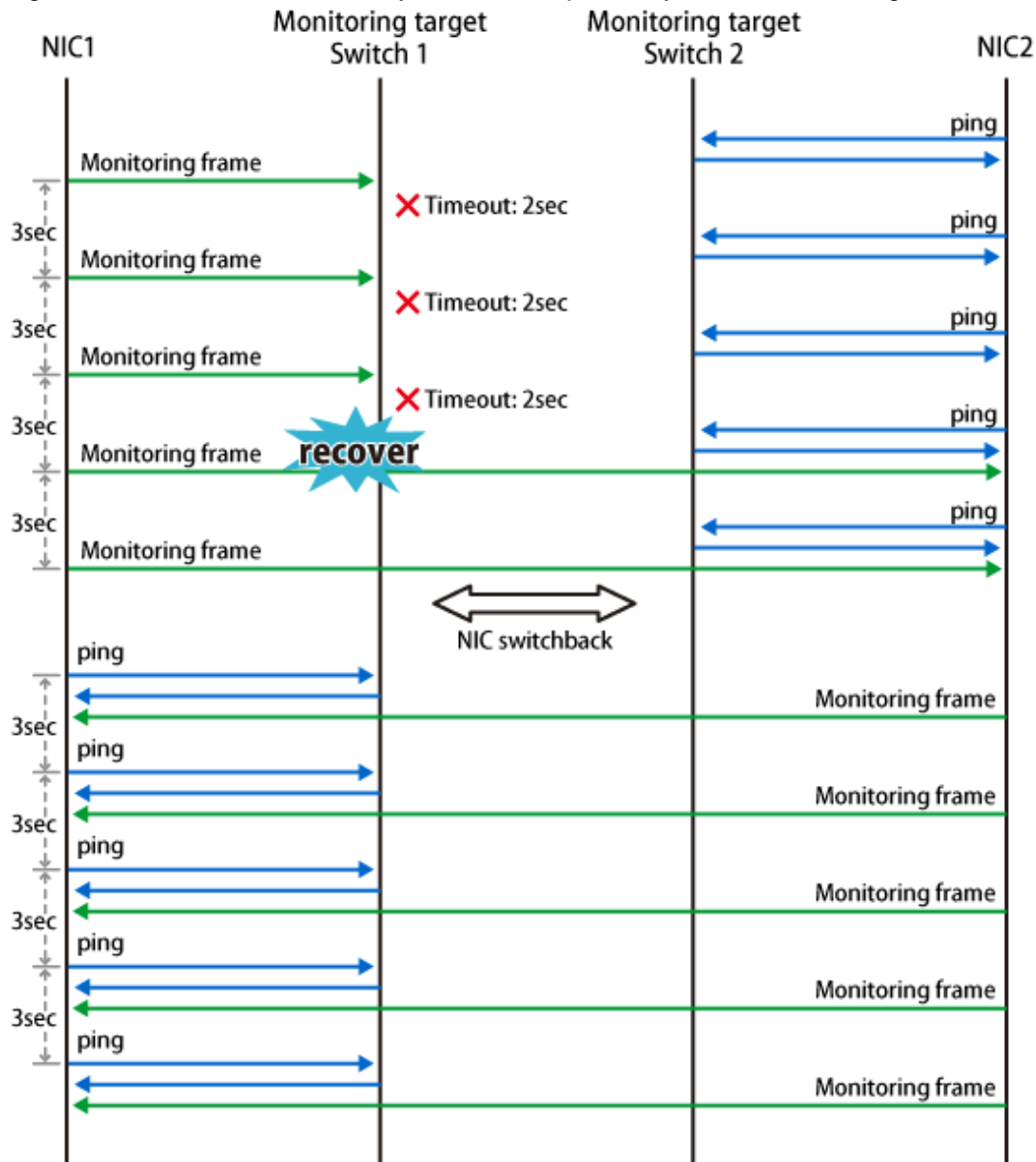




Figure 3.17 Transfer route recovery detection sequence by network monitoring function



## 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 settings when the targets have 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)

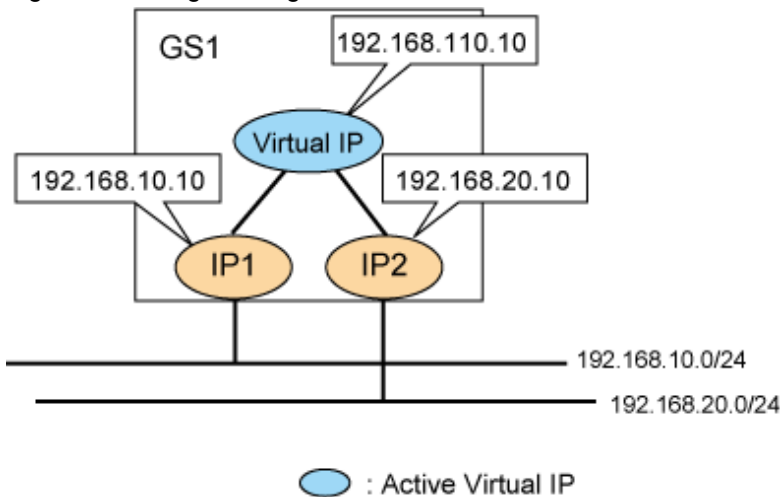
 **Note**

**When a communication target is a 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 virtual IP address.

Single configuration

Figure 3.18 Single configuration



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

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

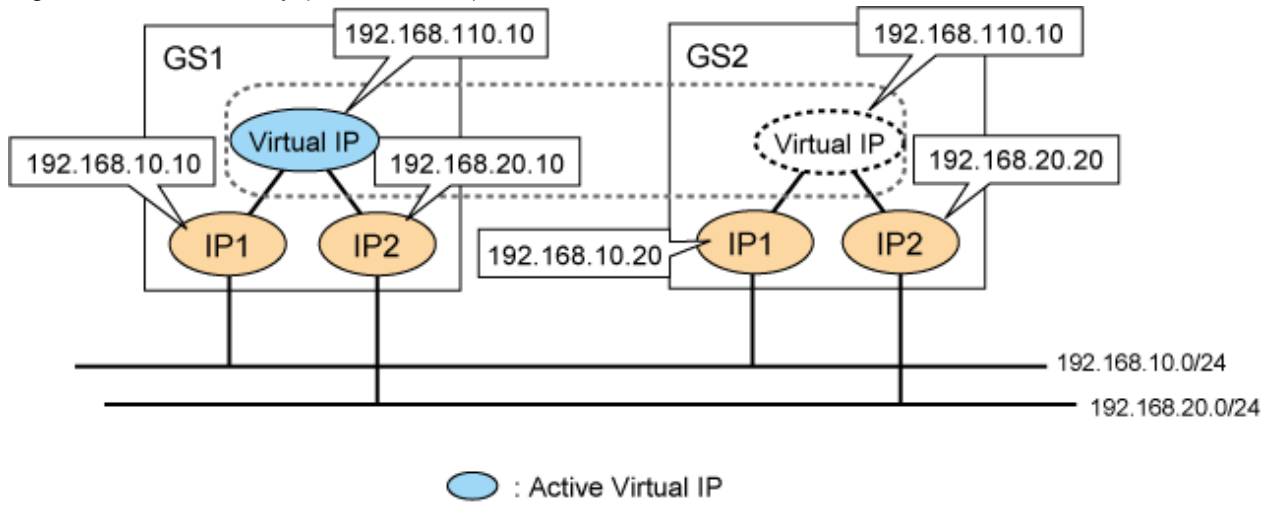
2. Check the settings.

```
# /opt/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) = YES

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 3.19 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
```

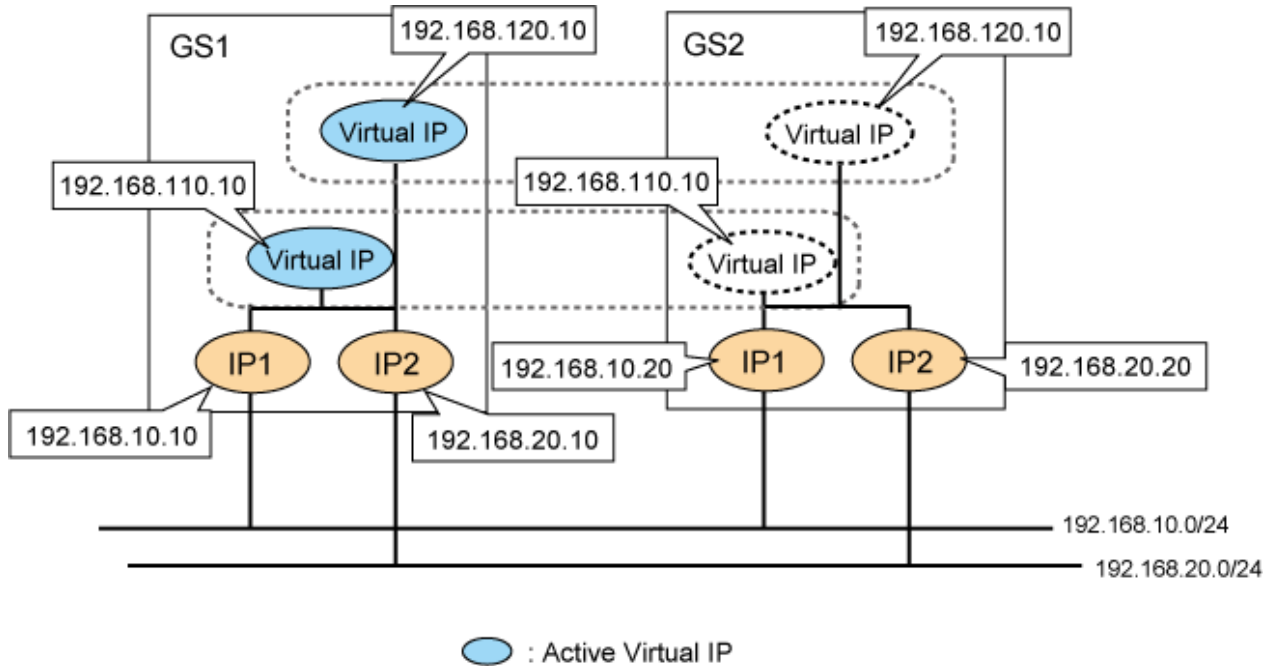
2. Check the settings.

```
# /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 3.20 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
```

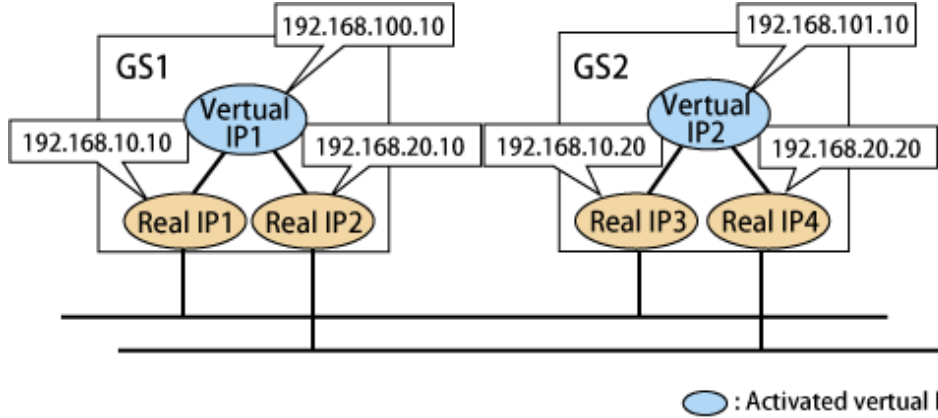
2. Check the settings.

```
# /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 3.21 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
```

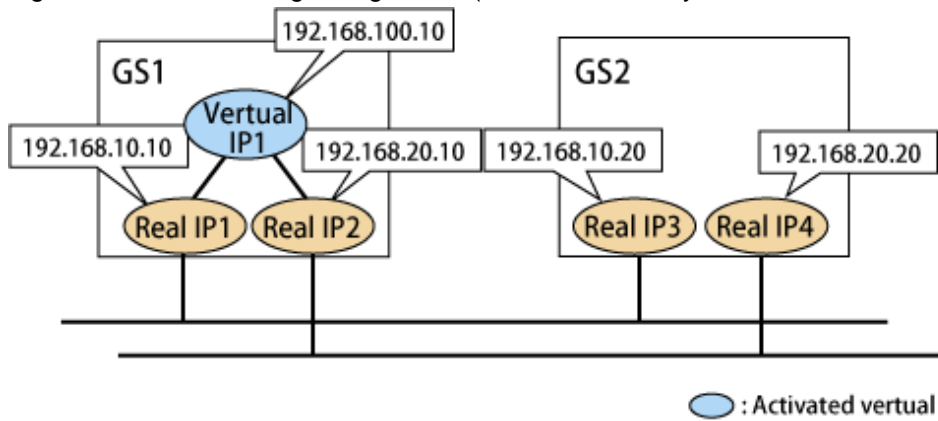
2. Check the settings.

```
# /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 3.22 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/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.100.10 -t
192.168.10.10,192.168.20.10
# /opt/FJSVhanet/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/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
+-----+-----+-----+-----+
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.

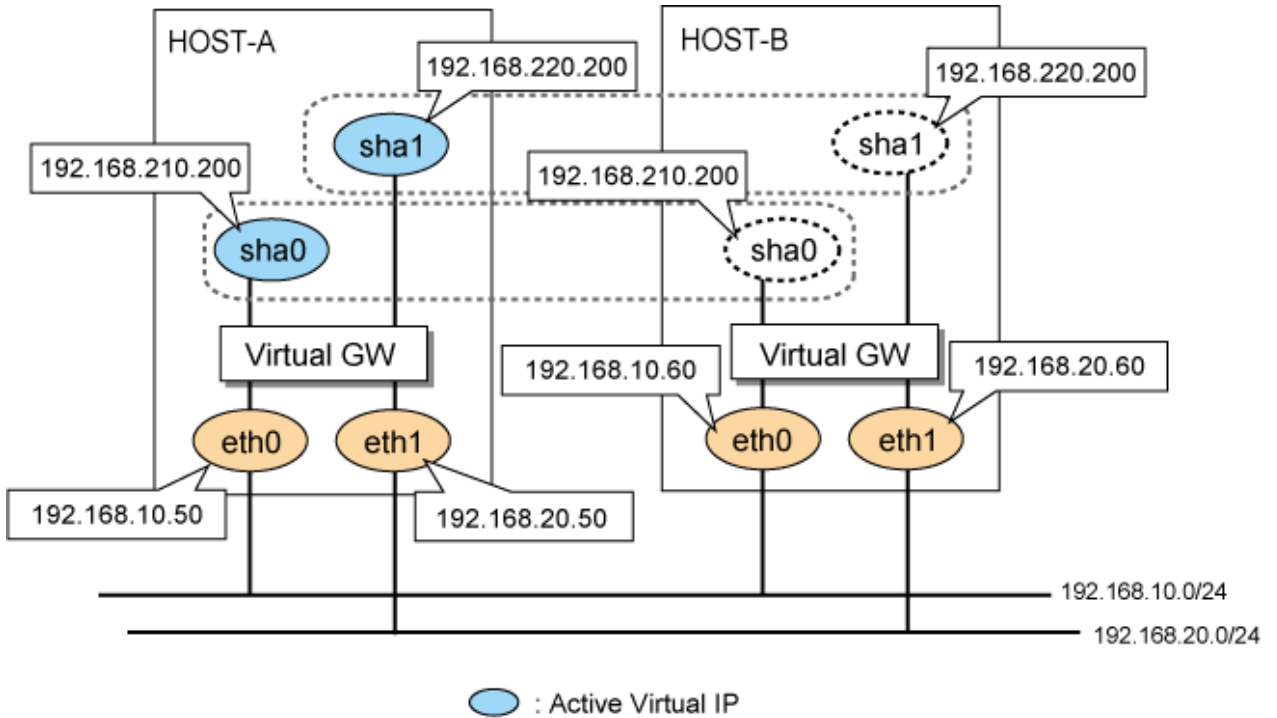


### Note

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 3.23 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))

```

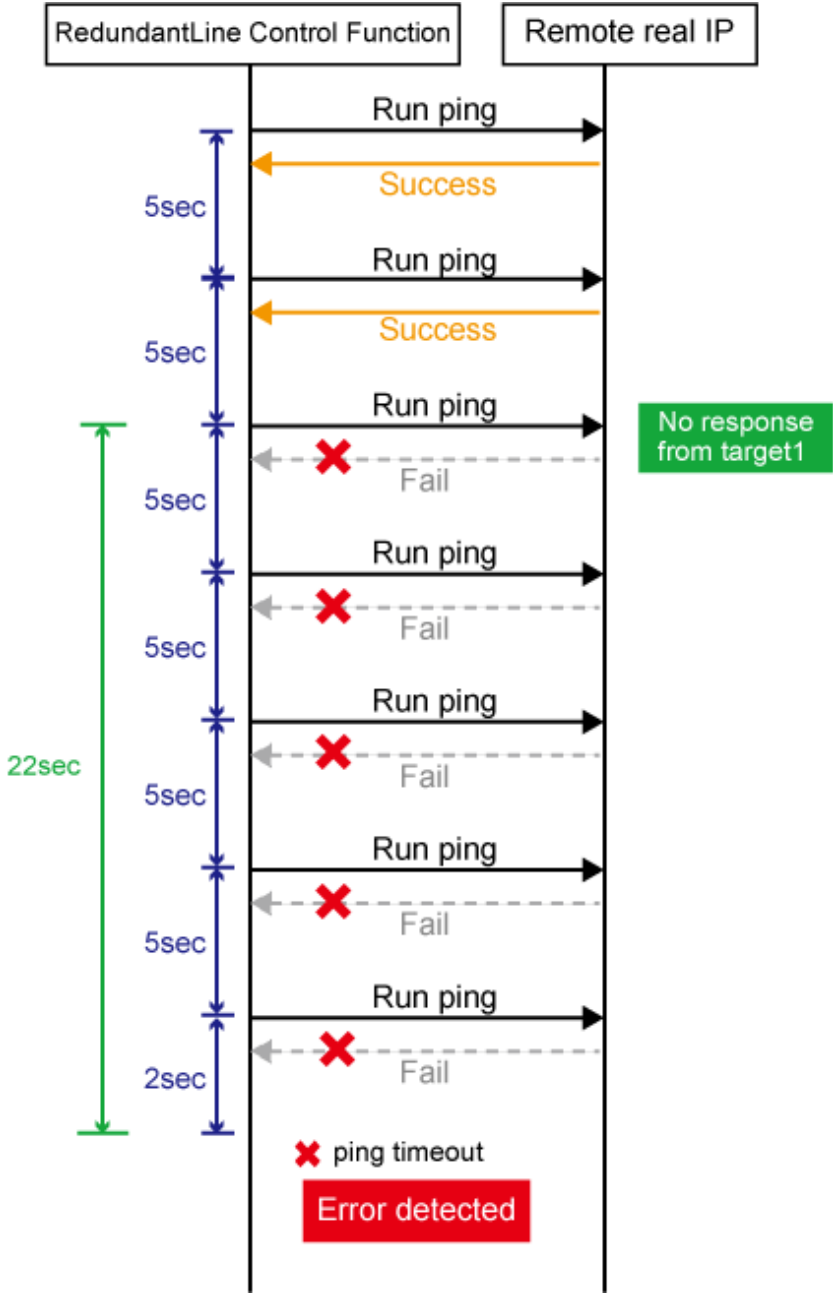
\*1: If the monitoring interval is 1 second, ping time out period would be 1 second, otherwise, ping time out period would be 2 seconds.

The default value is as follows.

5 sec x (5 time - 1) + 2 sec + 0 to 5 sec = 22 to 27 sec



Figure 3.24 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 pending until the waiting time for linkup elapses.



## Note

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

### 3.10.1.3 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) x retry count  
(count) + (0 to recovery monitoring interval (in seconds))
```

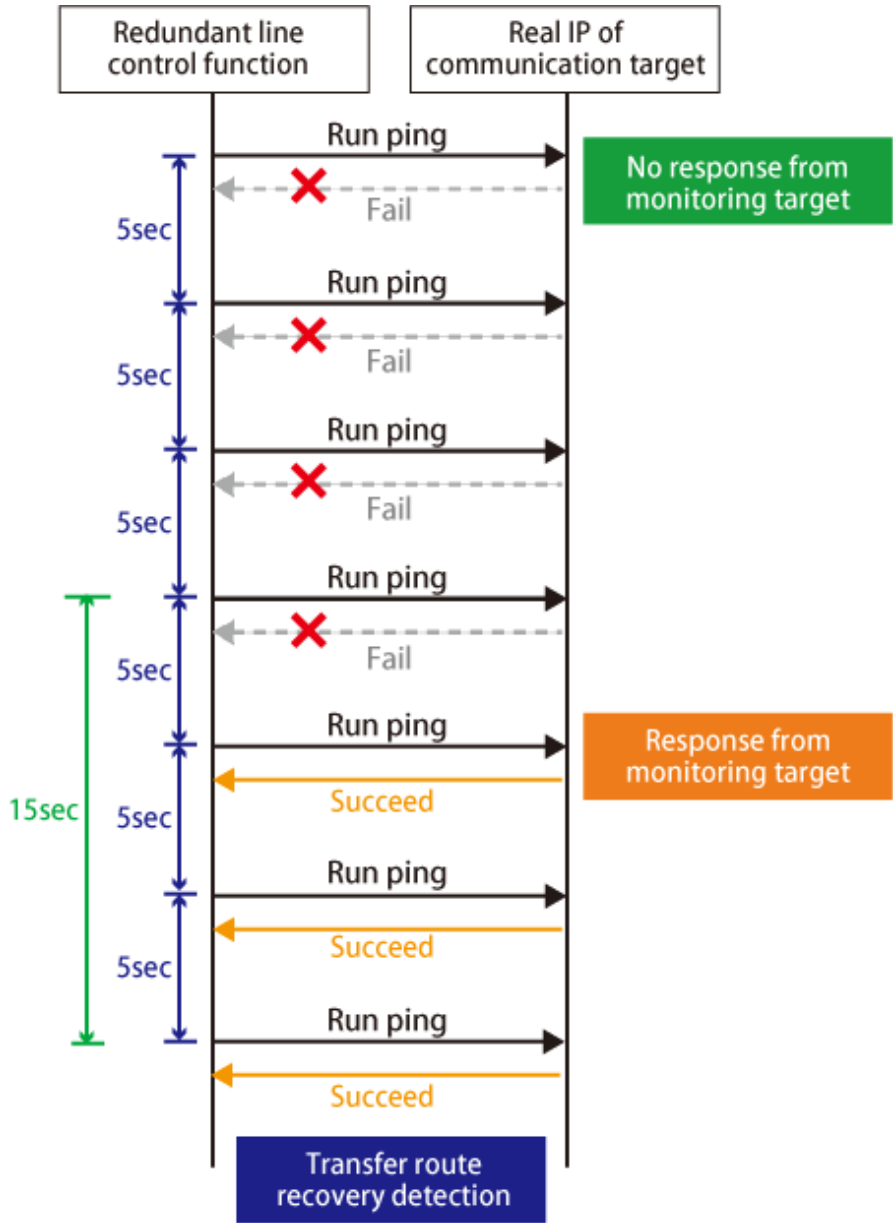
The default value is as follows.

5 sec x 0 time + 0 to 5 sec = 0 to 5 sec

When the retry count is 2 times, the value is as follows.

5 sec x 2 time + 0 to 5 sec = 10 to 15 sec

Figure 3.25 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)     :YES
  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 self-checking function.

```
# /opt/FJSVhanet/usr/sbin/hanetparam -e no
```

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

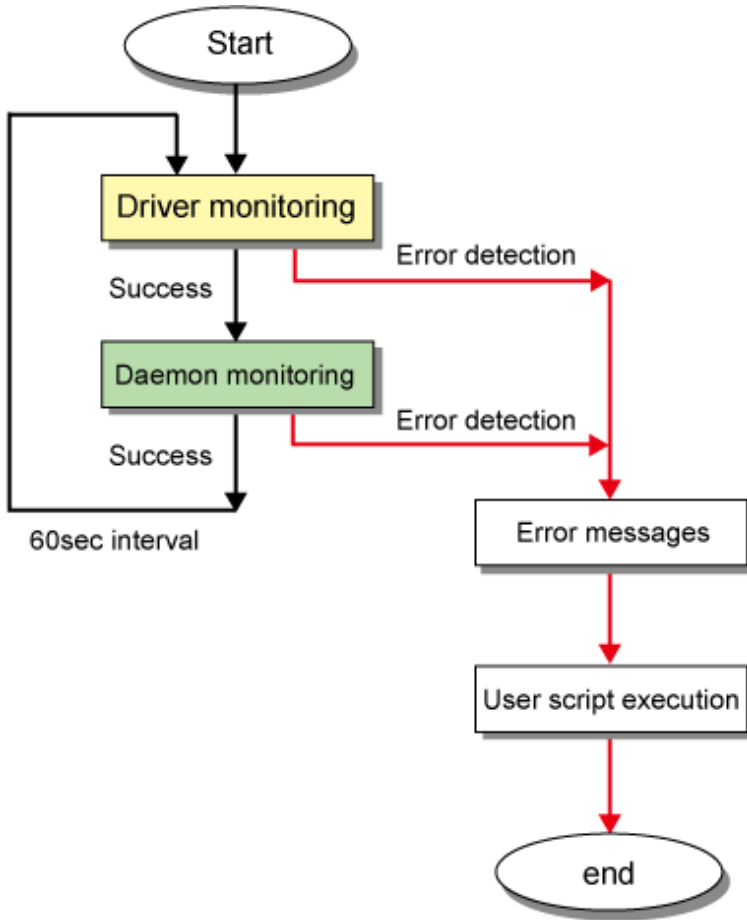
[Common Setting]
  Hostname resolution by file(h)     :YES
  Self-checking function(e)          :NO
```

3. 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 3.26 Error detection of the self-checking function



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

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

If an error has been detected, 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 whether or not to switch nodes when all the transfer paths have failed during cluster operation.

- 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/FJShanet/script/failover/sha.failover.sam (When detected an error in a transfer route)
- /etc/opt/FJShanet/script/patrol/sha.patrol.sam (When detected a standby patrol error or recovery)

Sample file for Virtual NIC mode

- /etc/opt/FJShanet/script/interface/sha-alive.sam (When detected an error or a recovery in the virtual interface)

Sample file for GS linkage mode

- /etc/opt/FJShanet/script/host/node\_event.sam

Sample file for all of Fast switching mode, Virtual NIC mode, and GS linkage mode

- /etc/opt/FJShanet/script/interface/sha-NN.takeover.interface.sam (When activating and deactivating the takeover virtual interface)

Sample file for Self-checking function

- /etc/opt/FJShanet/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/FJShanet/script/interface/shaX (When activating or deactivating an IP address)
- /etc/opt/FJShanet/script/failover/shaX (When detected an error in a transfer route)
- /etc/opt/FJShanet/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 Virtual NIC mode

- /etc/opt/FJShanet/script/alive/shaX (When detected an error or a recovery in the virtual interface)

\* shaX is the created virtual interface name for Virtual NIC mode.

Sample file for GS linkage mode

- /etc/opt/FJShanet/script/node\_event

Setup file for all of Fast switching mode, Virtual NIC mode, and GS linkage mode

- /etc/opt/FJShanet/script/interface/shaX-NN (When activating and deactivating the takeover virtual interface)

\* shaX-NN is the name that the colon (:) of the takeover virtual interface name is converted to the hyphen (-).

Setup file for Self-checking function

- /etc/opt/FJShanet/script/system/monitor

 Note

- Do not call the following commands for redundant line control function in the script file.
  - hanetconfig
  - strhanet
  - stphanet
  - hanetpoll
  - hanetnic
  - hanetpathmon
  - hanetobserv
  - dspobserv

- resethanet
- 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".

### Information

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

## 3.12.2.1 Settings for NIC switching mode

### Note

This version does not support IPv6 addresses for the NIC switching mode.

The following shows the samples of script file call formats and definition files.

#### (1) When activated or deactivated an IP address

[Script file call format]

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

param1

```
activate: Activated
inactivate: Inactivated
```

param2

```
before: Before activation or deactivation
after: After activation or deactivation
```

param3

```
ifname: Physical interface name
```

[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"

case $# 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
# 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 param2

param1

Primary: Error in a Primary interface

Secondary: Error in a Secondary interface

all: Error in both Primary/Secondary interfaces

param2

retryout: Retry out of the ping command

linkdown: Link-down of the interface

pinghang: Hang-up of the ping command

[Definition file sample]

```

#!/bin/sh
#
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2015
#
#ident "%W% %G% %U% - FUJITSU"

#
# Control interface for HA-Net
#
#
# Params
#
# $1 communication line state primary/secondary/all
# $2 event exit code retryout/linkdown/pinghang
#
#
# Set Params
#
#STATE=$1
#EXIT_CODE=$2
#PROC="process_name"

```

```

#kill -15 `/bin/ps -e | /bin/sed -n \
#       -e'/'$PROC'$/s/[^0-9 \t].*//p' \
#       ` > /dev/null 2>/dev/null

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

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

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

```

### (3) When detected a standby patrol error or recovery

[Script file call format]

/bin/sh shaX param1 param2

param1

establish: Standby patrol established

recover: Standby NIC monitoring recovered

fail: Standby NIC error

param2

Physical interface name of standby NIC: Physical interface name such as 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 of Virtual NIC mode

The following shows the script file call format and the definition file sample.

**(1) When detected an error or a recovery in the virtual interface**

[Script file call format]

/bin/sh shaX param1

param1

failed: Error in the virtual interface  
recover: Recover of the virtual interface

**[Definition file sample]**

```
#!/bin/sh
#
#       All Rights Reserved, Copyright (c) FUJITSU LIMITED 2016
#
#
#       Control interface for HA-Net
```

```

#
#
#      Param
#
#      $1      failed or recover
#
#
# Set Params
#
STATE=$1
VIF=`basename $0`

case "$STATE" in
'failed')

#
# script communication alive state transition to 'failed'
#

#echo "execute script communication alive state transition. if:$VIF
state:$STATE" > /dev/console

;;

'recover')

#
# script communication alive state transition to 'recover'
#

#echo "execute script communication alive state transition. if:$VIF
state:$STATE" > /dev/console

;;
*)
exit 1
;;
esac

exit 0

```

### 3.12.2.3 Settings for GS linkage mode

The following shows the script file call format and the definition file sample.

#### (1) When changing the remote hot-standby system, when an error is detected in remote host monitoring, and when changing nodes on the local system

[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 the route to all virtual IP addresses
# 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 ctdl.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.

3.12.2.4 Settings for all of Fast switching mode, Virtual NIC mode, and GS linkage mode

The following shows the script file call format and the definition file sample.

**(1) When activating and deactivating the takeover virtual interface**

[Script file call format]

/bin/sh shaX-NN param1 param2 param3

param1

active: Active  
inactive: Inactive

param2

before: Before activated/inactivated  
after: After activated/inactivated

param3

notice: Notice before activated/inactivated (only for "before")  
success: Successfully activated/inactivated (only for "after")  
failed: Failed to be activated/inactivated (only for "after")

[Definition file sample]

```
#!/bin/sh
#
#     All Rights Reserved, Copyright (c) FUJITSU LIMITED 2016
#
#
#     Control interface for HA-Net
#
```

```

#
# Params
#
# $1 active or inactive
# $2 before or after
# $3 notice or success or failed
#
#
# Set Params
#
EVENT=$1
TIMING=$2
RESULT=$3
VIF=`basename $0`

case "$EVENT" in
'active')
#
# Activate interface
#

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

#echo "execute script before activate interface on $VIF" > /dev/
console

;;

'after')
#
# script after activate interface
#

#if [ "$RESULT" = "success" ]; then
# echo "execute script after activate interface on $VIF result:
$RESULT" > /dev/console
#else
# echo "execute script after activate interface on $VIF result:
$RESULT" > /dev/console
#fi

;;
esac
;;

'inactive')
#
# Inactivate interface
#

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

#echo "execute script before inactivate interface on $VIF" > /dev/
console

```

```

;;

'after')
#
# script after inactivate interface
#

# if [ "$RESULT" = "success" ]; then
#   echo "execute script after inactivate interface on $VIF result:
$RESULT" > /dev/console
# else
#   echo "execute script after inactivate interface on $VIF result:
$RESULT" > /dev/console
# fi

;;
esac

;;
*)
  exit 1
;;
esac

exit 0

```

### 3.12.2.5 Settings for Self-checking function

The following shows the script file call format and the definition file sample.

#### (1) When an error and a recovery is detected in GLS

[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

```

### 3.12.3 Setting suppression of stopping userApplication when entire transfer routes fails

The function to suppress stopping userApplication when entire transfer routes fails can be used.

For details, refer to ["2.8.3 Suppression of stopping userApplication when entire transfer routes fails"](#)

The following settings must be made to suppress stopping userApplication.

A sample file (preStartGls.sh) is provided.

If the configuration described in ["2.8.3 Suppression of stopping userApplication when entire transfer routes fails"](#) is satisfied, it is not necessary to change the sample file.

Make sure that change the sample file as necessary, for example, to output a message to the system log.

1. Place the scripts on both the operation node and standby node.  
When placing a script, make sure that the directory and script name are the same on the operation node and standby node.  
The script name can be changed from the sample file name (preStartGrs.sh).  
Make sure that you have execute permission for the placed script.
2. Register the placed script with the userApplication PreOnline script.  
PreOnline scripts can be registered using RMS Wizard.  
For information about PreOnline scripts, refer to "PRIMECLUSTER Installation and Administration Guide"

#### [Sample file]

- preStartGls.sh

```

#!/bin/bash
#

```

```

# Copyright(c) 2022 FUJITSU LIMITED.
# All rights reserved.
#
LANG=C
#-----
# variables
#-----
STATE_STANDBY="Standby"
STATE_FAULTED="Faulted"
CFGLOG="/var/opt/FJSVhanet/log/config.log"
PROGRAMME="/bin/basename $0"
HANETPOLL="/opt/FJSVhanet/usr/sbin/hanetpoll"
HANETPOLL_OFF="{HANETPOLL} off"
HANETPOLL_ON_YES="{HANETPOLL} on -f yes"
HANETPOLL_ON_NO="{HANETPOLL} on -f no"
RCCMDDIR="/usr/opt/reliant/bin"
HVASSERT="{RCCMDDIR}/hvassert"
HANETSELECT="hanetselect"
MSG_OFFLINE="ERROR: Remote system is not online"
MSG_TIMEOUT="Command timed out!"
MSG_STANDBY="ERROR: Actual resource state is - Standby"
HVDISP="{RCCMDDIR}/hvdisp"
ECHO="echo" #bash built-in command
LOGGER="/usr/bin/logger"
GREP="/bin/grep"
AWK="/bin/awk"
SED="/bin/sed"
PGREP="/usr/bin/pgrep"
DATE="/bin/date"

# flag to output a message
SYSLOG_OUTPUT="off"

#-----
# functions
#-----
HANetLog(){
    if [ -f ${CFGLOG} ]; then
        DATETIME=`{DATE} +%Y/%m/%d %H:%M:%S.%3N`
        {ECHO} ["[${DATETIME}] - [${PROGRAMME}] [$$] $*" >> ${CFGLOG}
    fi
    return 0
}

HANetSysLog(){
    log_str=$*
    if [ ${SYSLOG_OUTPUT} != "off" ]; then
        {LOGGER} -t "hanet:${PROGRAMME}" -p user.err "${log_str}" >/dev/null 2>&1
    fi
    HANetLog ${log_str}
    return 0
}

PollExec(){
    # hanetpoll off
    poll_result=`{HANETPOLL_OFF} 2>&1`
    ret=$?
    if [ ${ret} -ne 0 ]; then
        # check hanetselect
        pgrep_result=`{PGREP} -x {HANETSELECT}`
        if [[ ${pgrep_result} != "" ]]; then
            # exist hanetselect

```

```

        if [ -z "${poll_result}" ]; then
            poll_result="ERROR:${HANETPOLL_OFF}"
        fi
        HAnetSysLog ${poll_result}
        exit 0
    else
        HAnetLog "Polling is already stopped.  ${poll_result}"
    fi
fi

# hanetpoll on
result=`$* 2>&1`
ret=$?
if [ ${ret} -ne 0 ]; then
    if [ -z "${result}" ]; then
        result="ERROR:$*"
    fi
    HAnetSysLog ${result}
    exit 0
fi
return 0
}

#-----
#   main
#-----
### In the case of Standby ( After transition )#####
if [[ ${HV_INTENDED_STATE} = ${STATE_STANDBY} ]];then
    # After state is Standby. Set no.
    PollExec ${HANETPOLL_ON_NO}
    exit 0
fi

### Get remote SysNode name #####
remote_node=`${HVDISP} ${HV_APPLICATION} | ${AWK} \
'$1="PriorityList" { gsub("PriorityList|'${RELIANT_HOSTNAME}'|:", ""); print $1}'`
if [[ ${remote_node} = "" ]]; then
    HAnetSysLog "Remote SysNode name is not set."
    exit 0
fi

### hvassert #####
# hvassert -h nodelRMS -s appl Faulted
result=`${HVASSERT} -h ${remote_node} -s ${HV_APPLICATION} ${STATE_FAULTED} 2>&1`
ret=$?
if [ ${ret} -eq 0 ]; then
    # Last Node: hanetpoll off -> hanetpoll on -f no
    PollExec ${HANETPOLL_ON_NO}
else
    case "${result}" in

        # Remote SysNode is OFFLINE.
        *${MSG_OFFLINE}* )
            HAnetLog ${result}
            # Offline: hanetpoll off -> hanetpoll on -f no
            PollExec ${HANETPOLL_ON_NO}
            ;;

        # Command is timeout.
        *${MSG_TIMEOUT}* )
            # Timeout: hanetpoll off -> hanetpoll on -f yes
            HAnetLog ${result}
    esac
fi

```

```

        PollExec ${HANETPOLL_ON_YES}
        ;;
    *${MSG_STANDBY}* )
        # other case Standby is normal case.: hanetpoll off -> hanetpoll on -f yes
        PollExec ${HANETPOLL_ON_YES}
        ;;
    * )
        # other case: hanetpoll off -> hanetpoll on -f yes
        HAnetLog ${result}
        PollExec ${HANETPOLL_ON_YES}
        ;;
esac
fi

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 Hot maintenance of NIC (PCI card)

---

The hot maintenance allows for replacing any malfunctioning NICs without disrupting ongoing operation. Making any settings for the hot maintenance before starting system operation is not required. For details on the hot maintenance procedure for NICs, see "6.3 NIC maintenance".

# 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/hanetnic	Dynamically adding/deleting/switching physical interface	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](#)".



- Be sure to use the strhanet command to activate a virtual interface. Do not use the ip command to perform the activation.
- Do not operate physical interfaces that the virtual interface bundles with a command such as the ip command while activating the 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](#)".



Be sure to use the stphanet command to deactivate a virtual interface. Do not use the ip command to perform the deactivation.

## 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.

## Point

When using the physical interfaces eth1 and eth2, the takeover virtual interfaces and the logical interfaces are displayed as the secondary addresses of eth1 and eth2 by the ip command.

## 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

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
Fast switching mode	Y	Y	Y	Y
NIC switching mode	Y	Y	Y	Y
Virtual NIC mode	Y	Y	Y	Y
GS linkage mode	Y	Y	N	N

[Meaning of the symbols] Y: Supported N: 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	Y	N	N	N	N
Mutual standby	Y	N	N	N	N
Cascade	Y	N	N	N	N
Priority transfer	Y	N	N	N	N

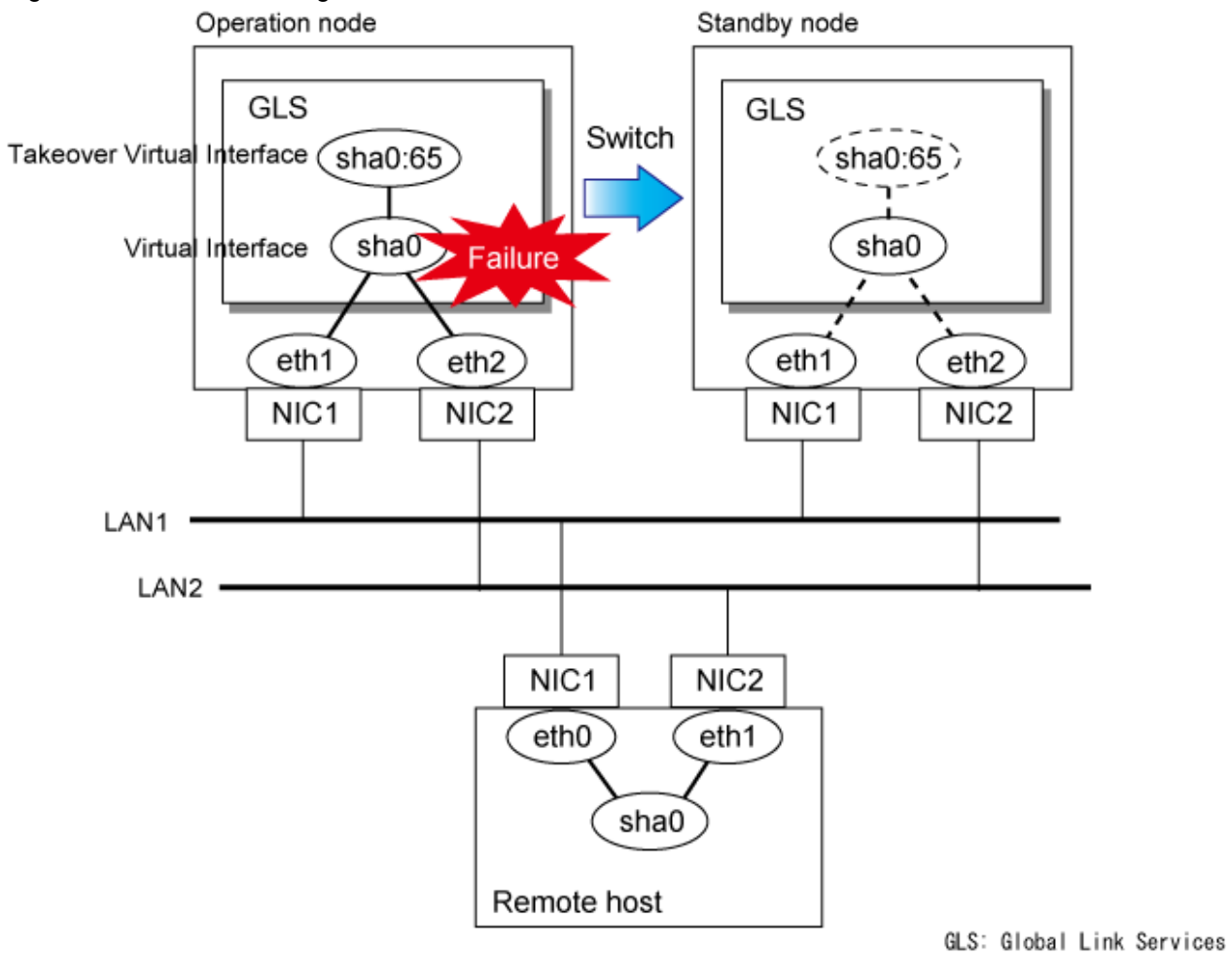
[Meaning of the symbols] Y: Supported N: Not supported

## 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

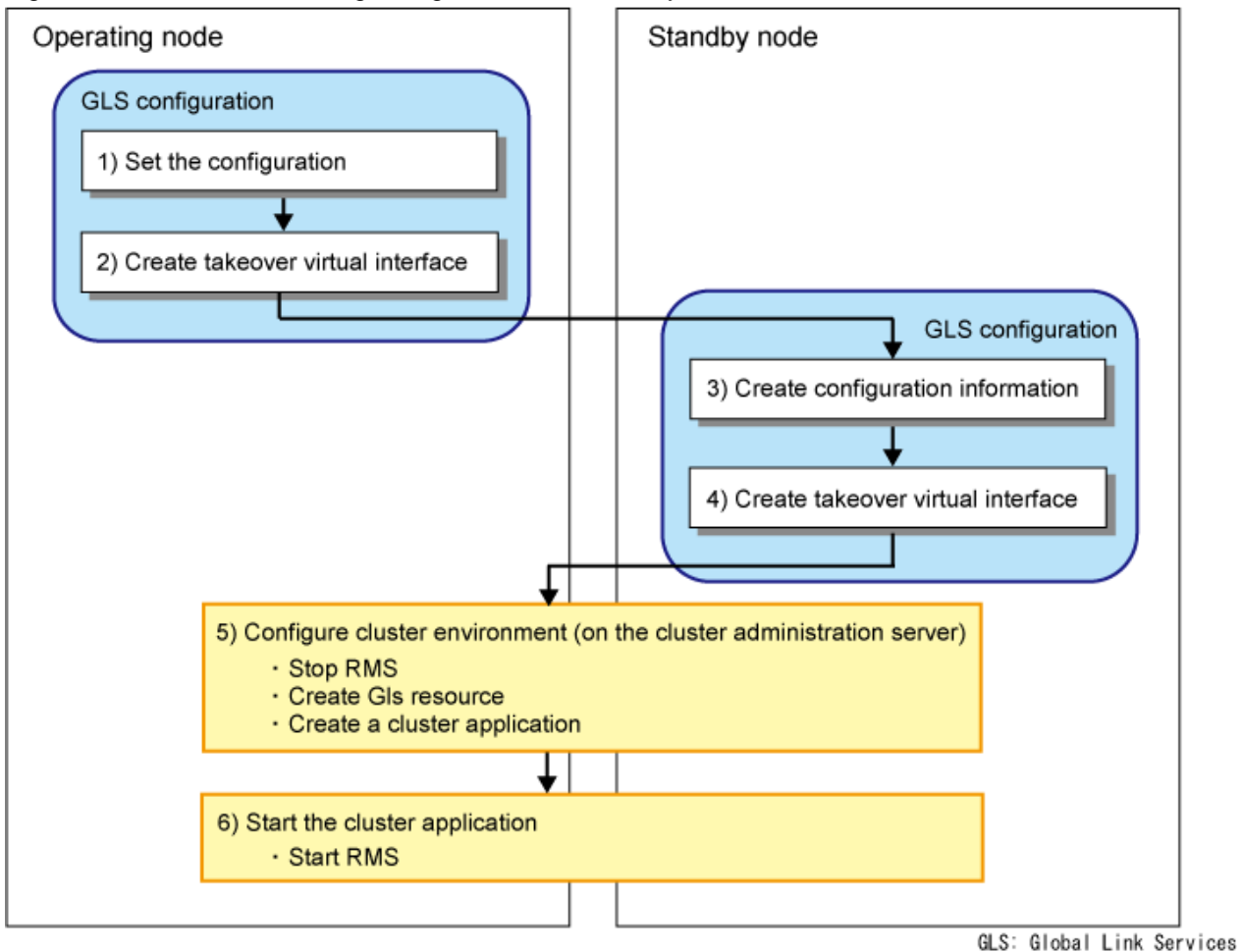
If you modified the configuration information for the cluster operation and the takeover virtual interface information, enable the modified settings by rebooting the system or by executing the `resethanet -s` option before operating GLS.

## 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.	<code>/opt/FJSVhanet/usr/sbin/hanethvrsc</code>	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 hanethvrsc Command](#)" for the detail of the command.

[Configuring a takeover virtual interface]

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc 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 GIs resource, and create a userApplication. Cluster system can be configured using RMS Wizard. Refer to "PRIMECLUSTER Installation and Administration Guide" for details.



See

.....  
The function to suppress stopping userApplication when entire transfer routes fails can be used.

For details, refer to "[2.8.3 Suppression of stopping userApplication when entire transfer routes fails](#)".  
.....

## 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

---

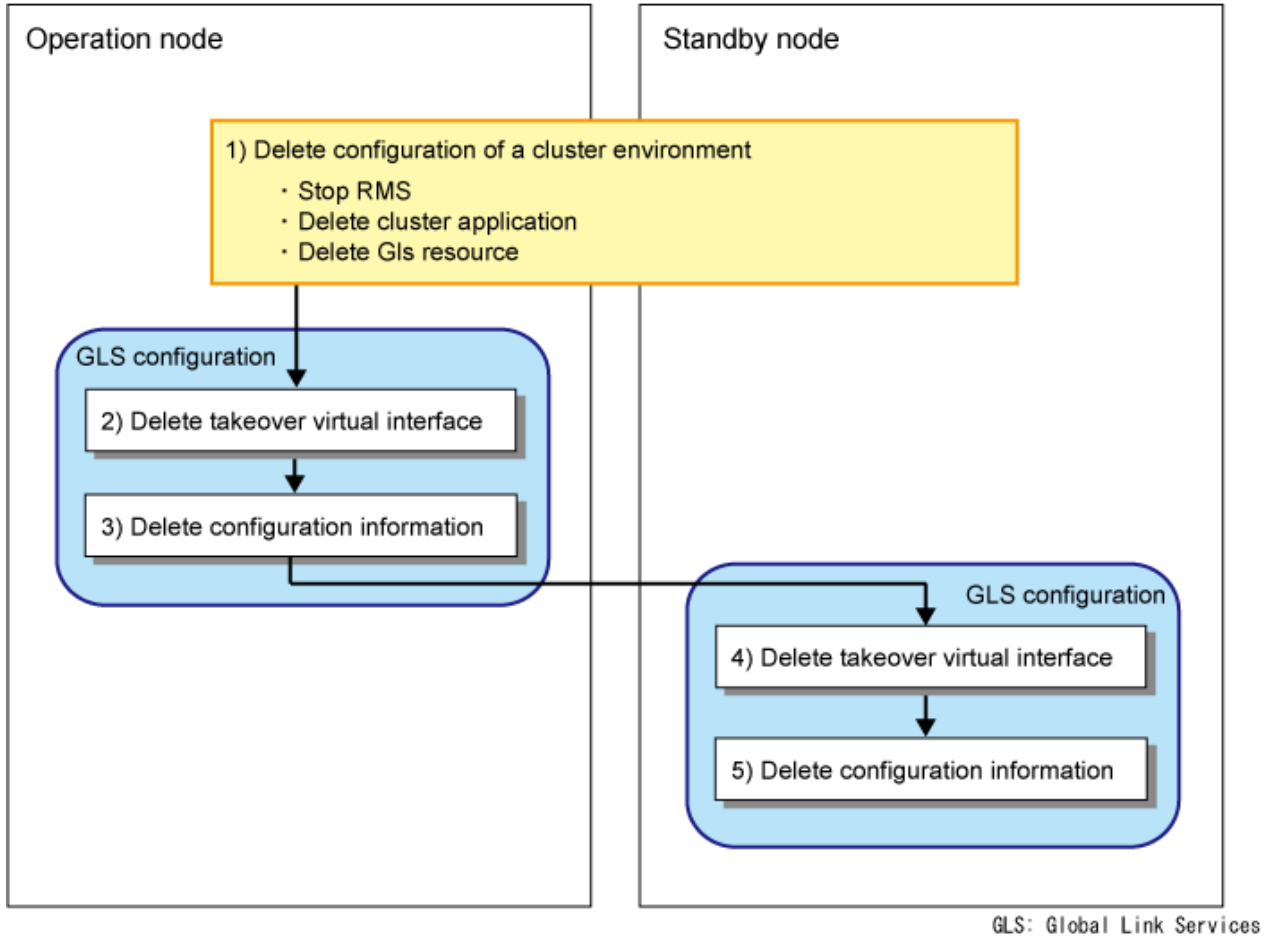
Configuration information and takeover resource information operated by the cluster system cannot be changed directly. Delete the takeover resource information first, and after changing corresponding configuration information, register the takeover resources information again.

## 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.

GLS: Global Link Services

### 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.

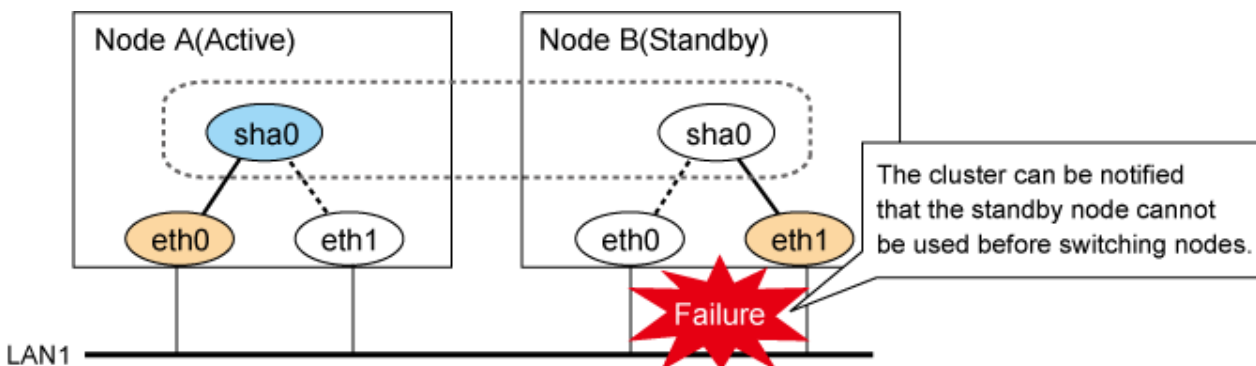
The following describes about monitoring GLS resource status of standby node.

#### 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 from a GLs resource failure following a transfer path failure on the standby node.

##### 1) Recovering the transfer path where a failure has occurred

Restore the failed transfer path to the normal status (perform necessary work such as reconnecting the cable, powering on the switch/HUB again, and replacing the failed switch/HUB).

## 2) Clearing the GIs resource failure status

Clear the GIs resource failure status back to the original status by using "Cluster Admin" in Web-Based Admin View. From this operation, the GIs resource for the standby node is reconfigured in a userApplication as the 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.

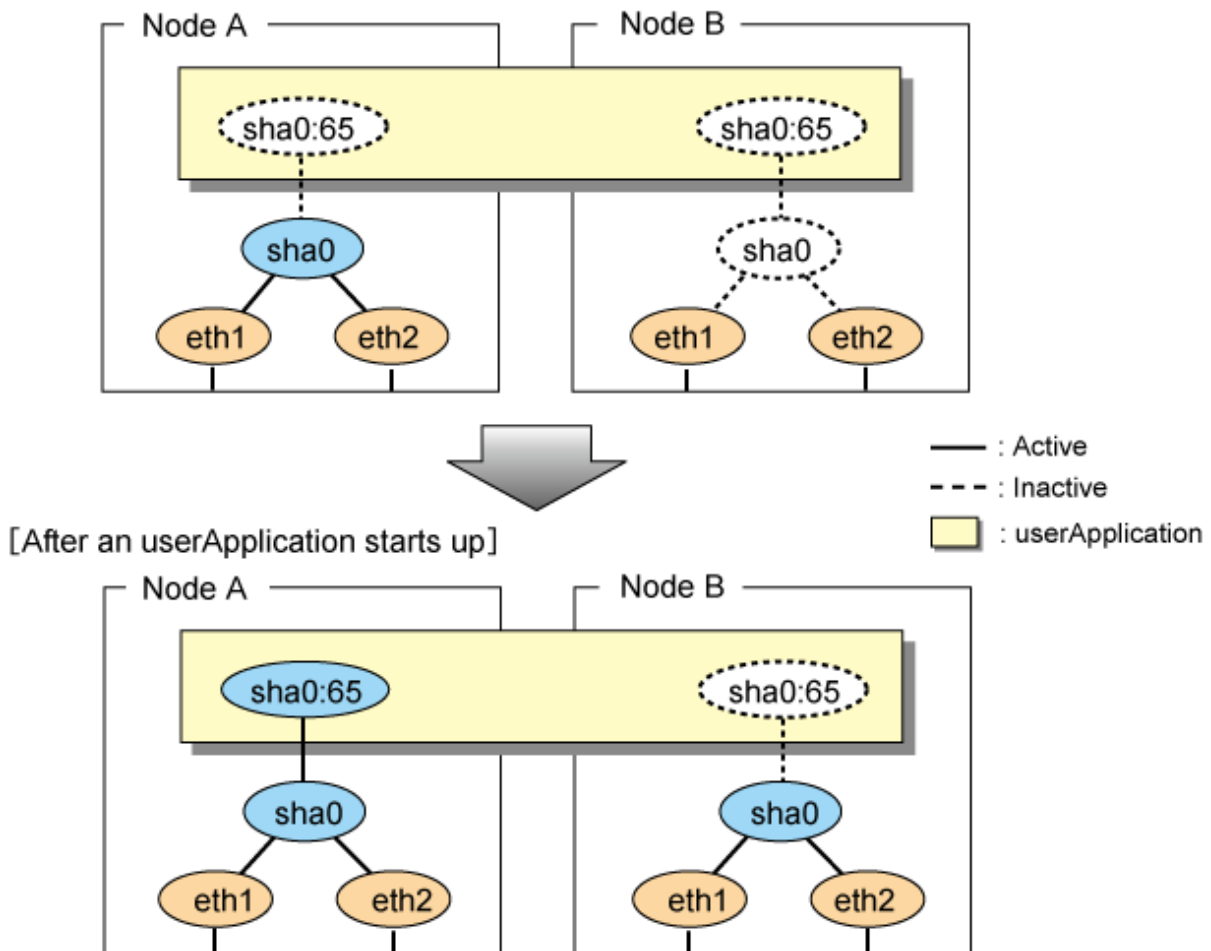
When operating, Fast switching mode uses the redundant line control function to communicate with the remote system.

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

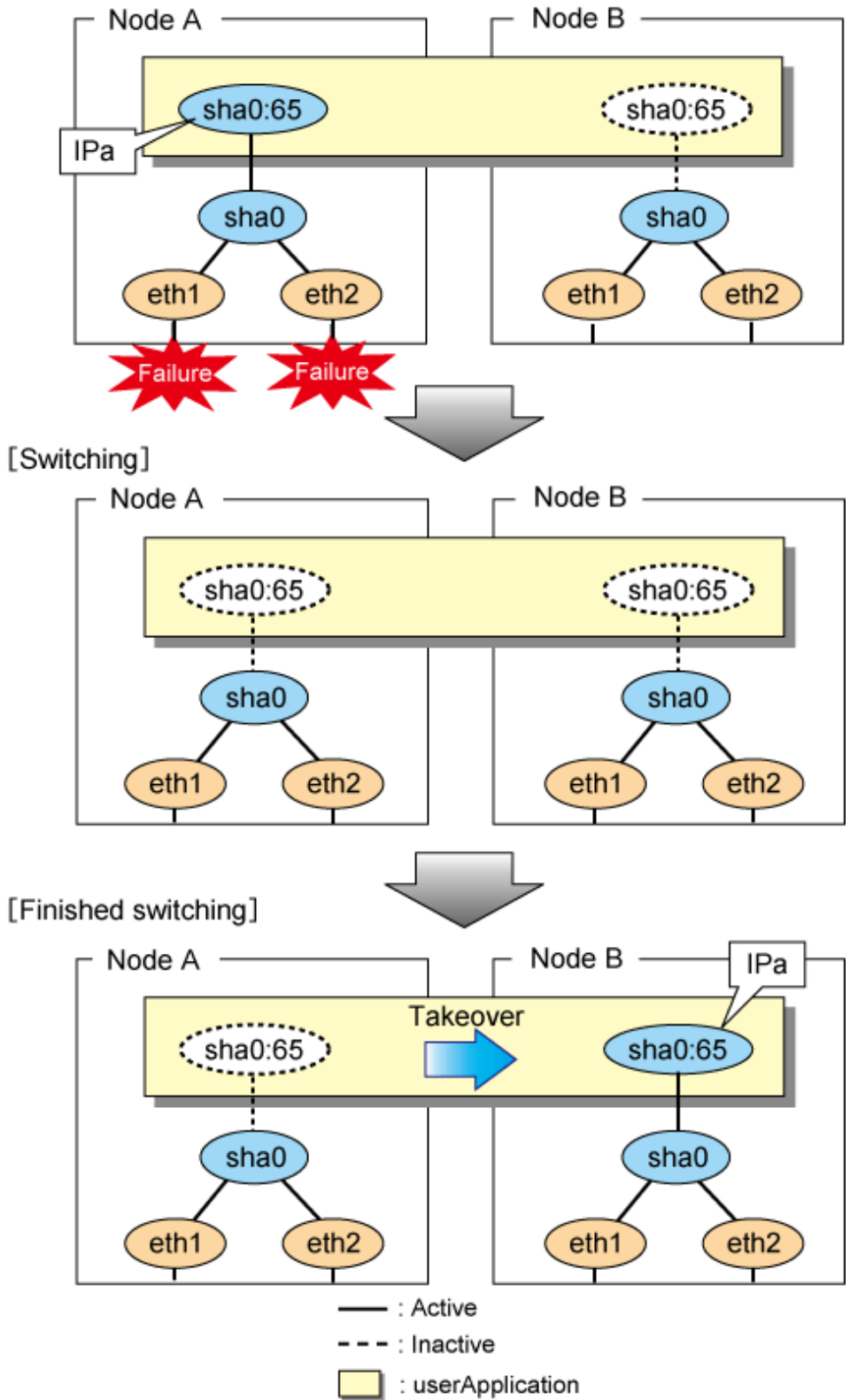
During normal operation, the system communicates with the remote system using Redundant Line Control Function on the operating node.

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 hung 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.

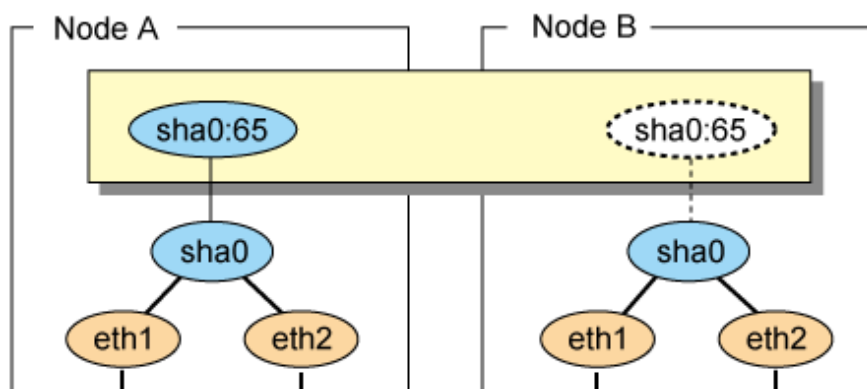
Restore the original operation status by performing fail-back operation for userApplication from "Cluster Admin" in Web-Based Admin View.

## 5.4.1.4 Stopping

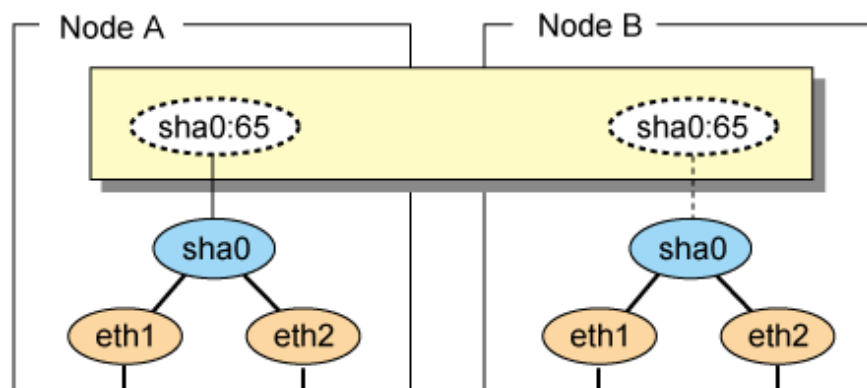
Figure 5.6 Stopping behavior of Fast switching mode illustrates stopping process of userApplication.

Figure 5.6 Stopping behavior of Fast switching mode

[Before an userApplication stops]



[After an userApplication stops]



— : Active  
- - - : Inactive  
■ : userApplication

## 5.4.2 Active Standby (NIC switching mode)

### 5.4.2.1 Starting

Since the following three types of IP takeover function can be used when using the NIC switching mode with IPv4, 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.

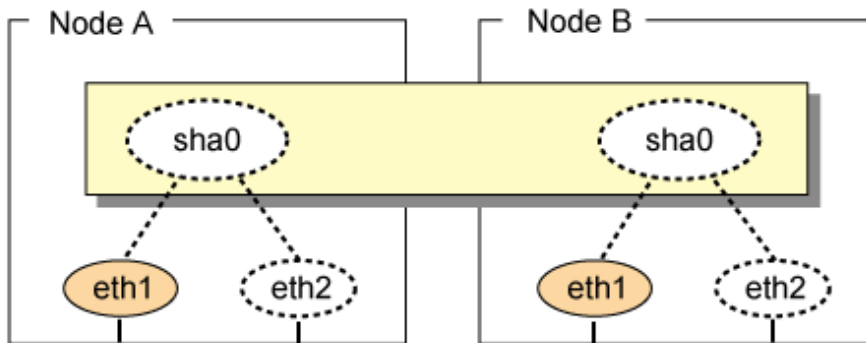
- Physical IP address takeover II

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.

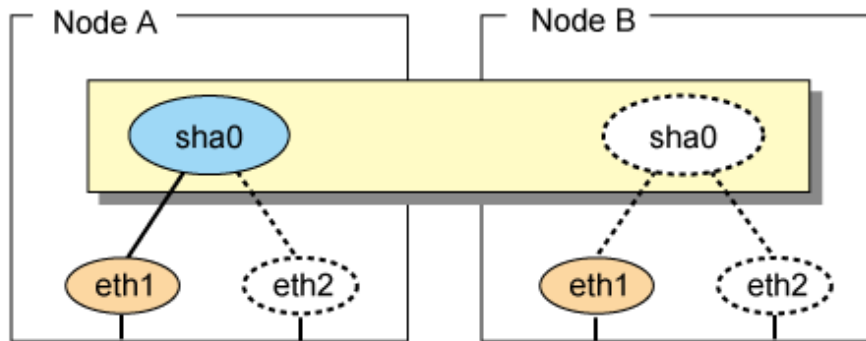
For logical IP takeover, the physical interface (eth1) for both operating node and standby node is activated when the redundant line control function starts up. Once the userApplication starts up, the takeover virtual interface is activated on the operating node.

[Figure 5.7 Startup behavior of NIC switching mode \(logical IP takeover\)](#) shows startup behavior for logical IP takeover.

Figure 5.7 Startup behavior of NIC switching mode (logical IP takeover)  
 [Before an userApplication starts up]



[After an userApplication starts up]

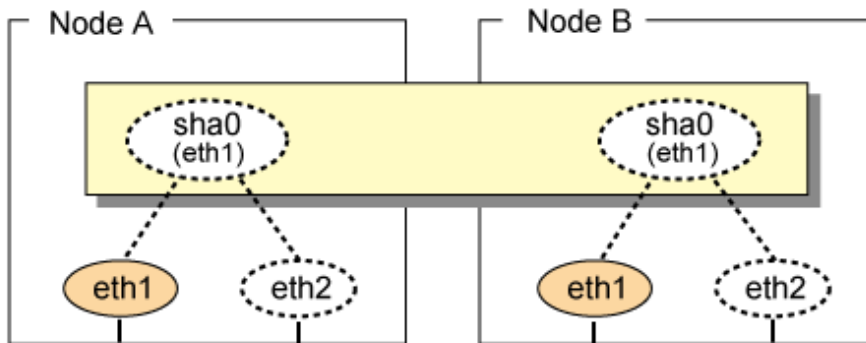


- : Active
- - - : Inactive
- : userApplication

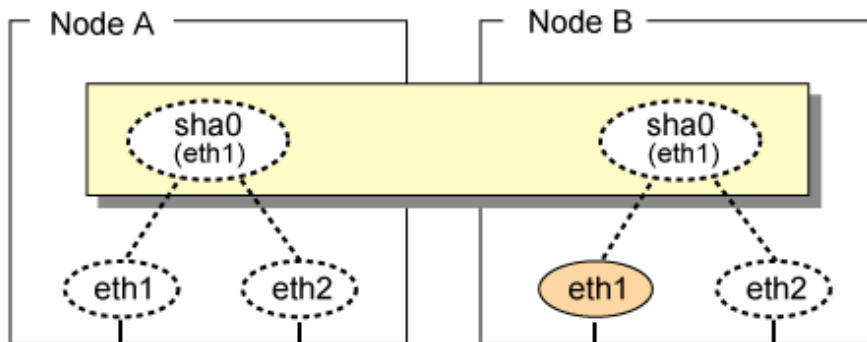
For taking over physical IP address I, activate the physical interface (eth1) for operating node and standby node when the redundant line control function starts up. After the userApplication starts, it will activate the physical interface by allocating a takeover IP address to the physical interface 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

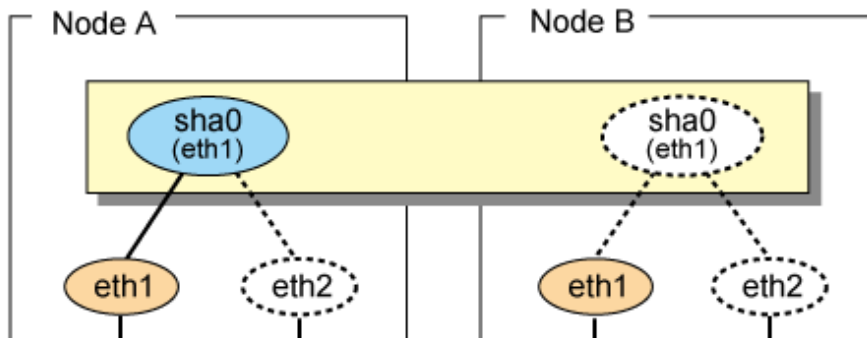
Figure 5.8 Startup behavior of NIC switching mode (takeover physical IP address I)  
 [Before an userApplication starts up]



[Starting an userApplication]



[After an userApplication starts up]



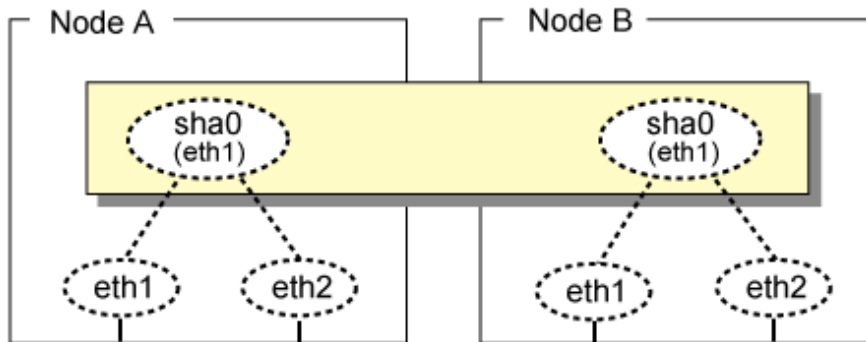
— : Active  
 - - - : Inactive  
 □ : userApplication

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.

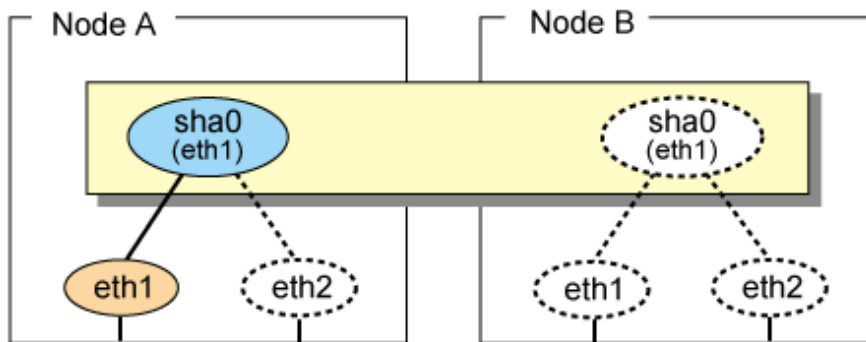
Figure 5.9 Startup behavior of NIC switching mode (takeover physical IP address II) shows a startup behavior of the takeover physical IP address II



Figure 5.9 Startup behavior of NIC switching mode (takeover physical IP address II)  
 [Before an userApplication starts up]



[After an userApplication starts up]



— : Active  
 - - - : Inactive  
 □ : userApplication

### 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 (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) is allocated to the logical interface for the secondary interface (eth2) on the operating node A. Once IPa is allocated, the logical interface for the secondary interface turns into the activated state.

When switching the node due to a failure in the transfer routes, the NIC switching mode inactivates the takeover virtual interface to which the takeover IP address (IPa) has been allocated on the operating node A. Then it allocates the takeover IP address (IPa) to the primary interface (eth1) which has already been activated on the standby node B and finally activates the logical interface.

Figure 5.10 Switching behavior of NIC switching mode (logical IP takeover)  
 [Operating (Failure occurred in node A)]

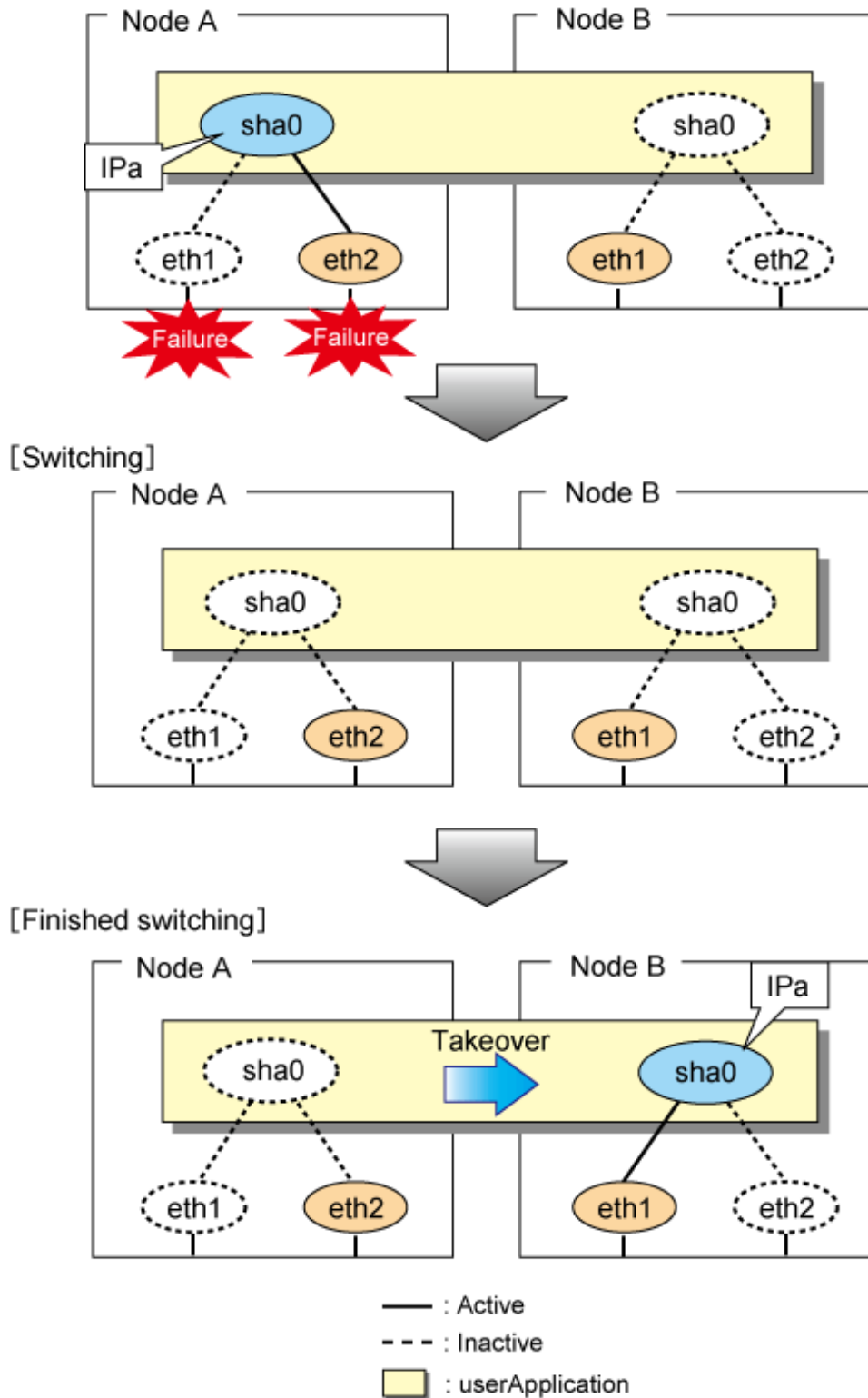


Figure 5.11 Switching behavior of NIC switching mode (takeover physical IP I) (continued) and Figure 5.12 Switching behavior of NIC switching mode (takeover physical IP I) (end) illustrate switching behavior of NIC switching mode (takeover physical IP address I).

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)]

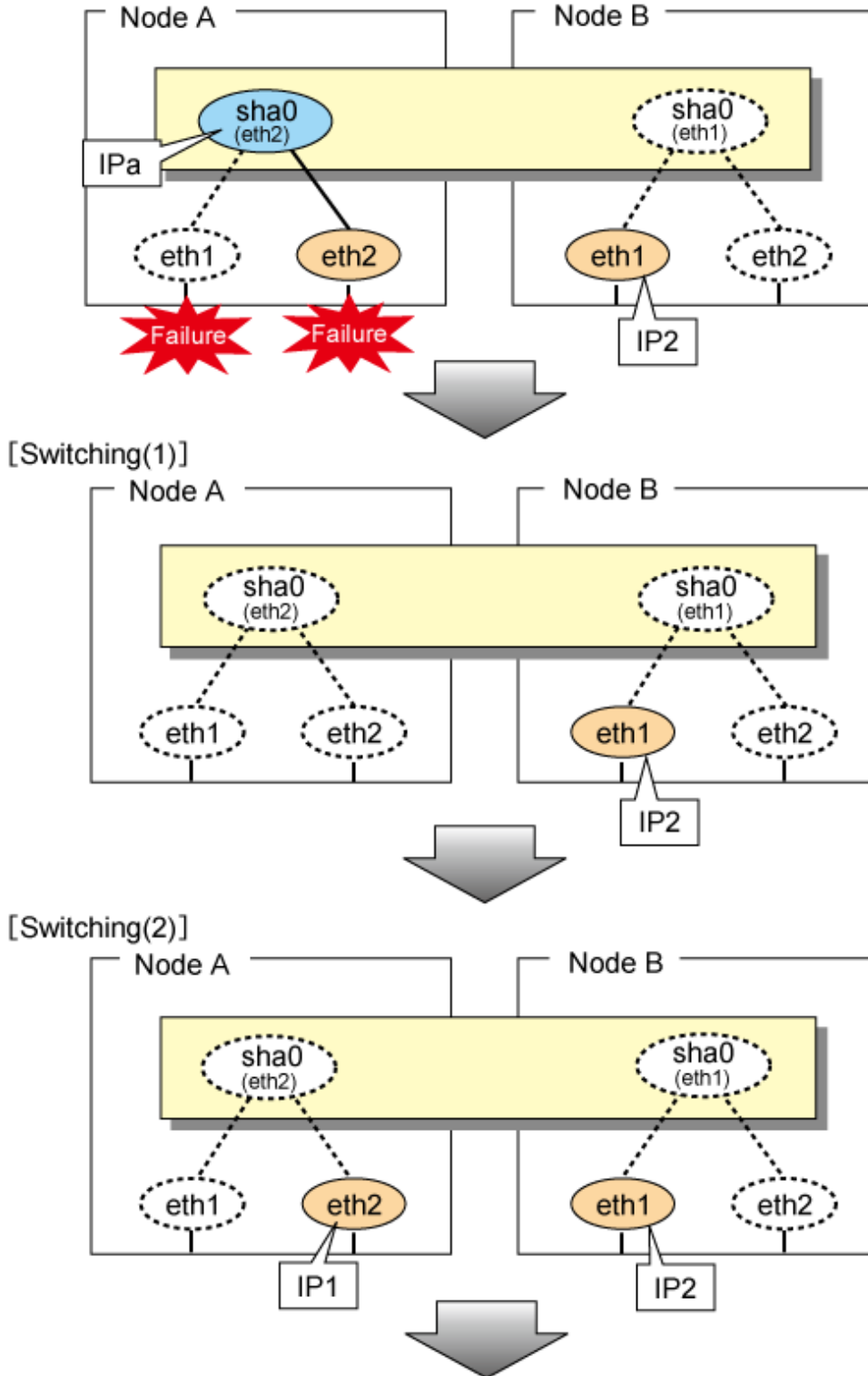


Figure 5.12 Switching behavior of NIC switching mode (takeover physical IP I) (end)  
 [Switching(3)]

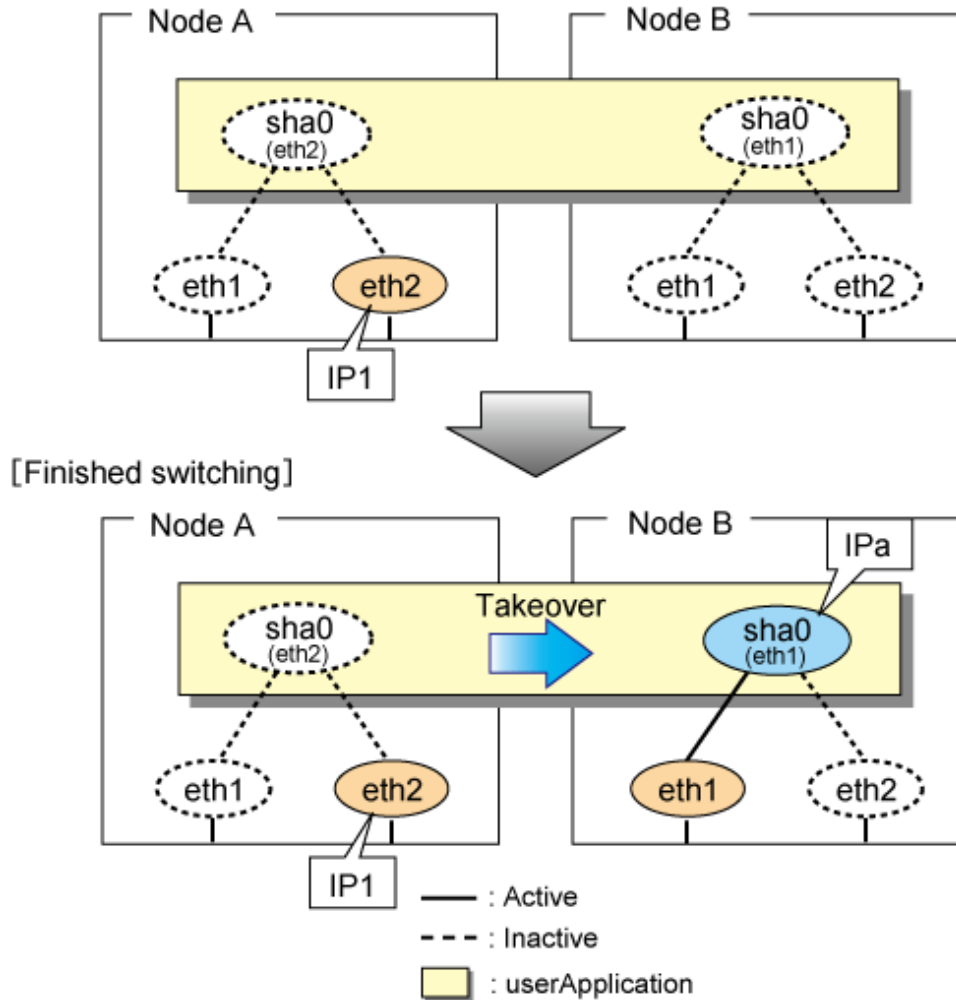
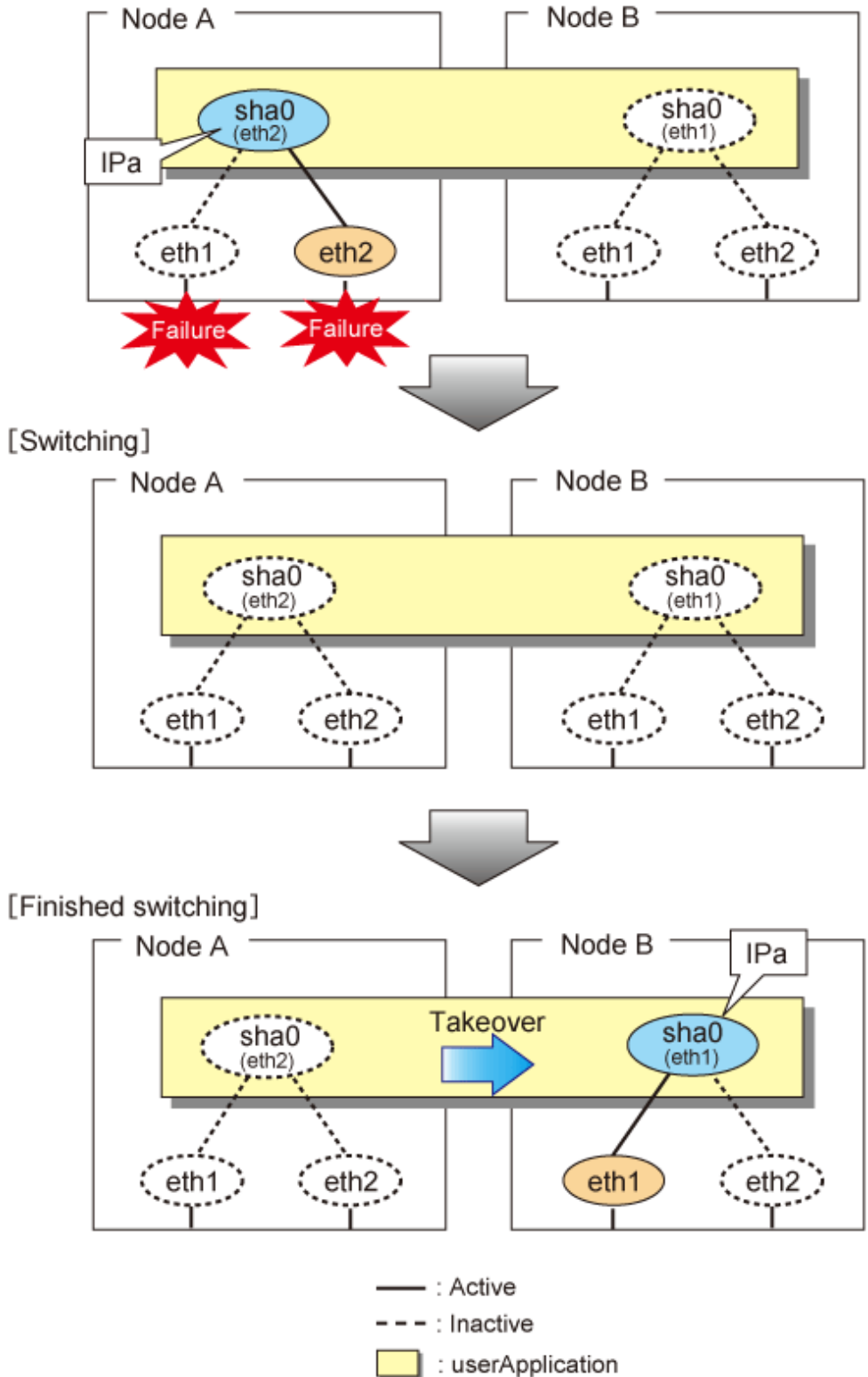


Figure 5.13 Switching behavior of NIC switching mode (takeover physical IP address II) illustrates switching behavior of NIC switching mode (takeover physical IP address II).

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]

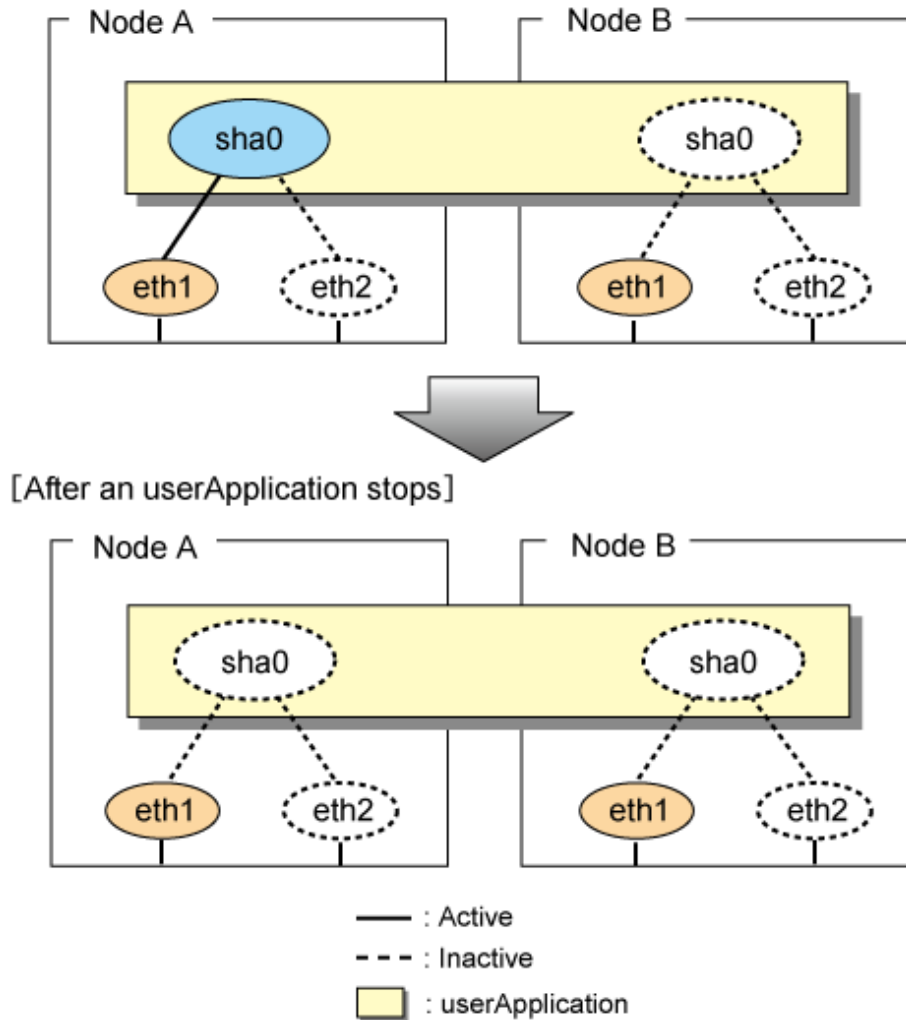


Figure 5.15 Stopping process of NIC switching mode (physical IP takeover I) illustrates stopping behavior of userApplication for the physical IP takeover I.

Figure 5.15 Stopping process of NIC switching mode (physical IP takeover I)  
 [Before an userApplication stops]

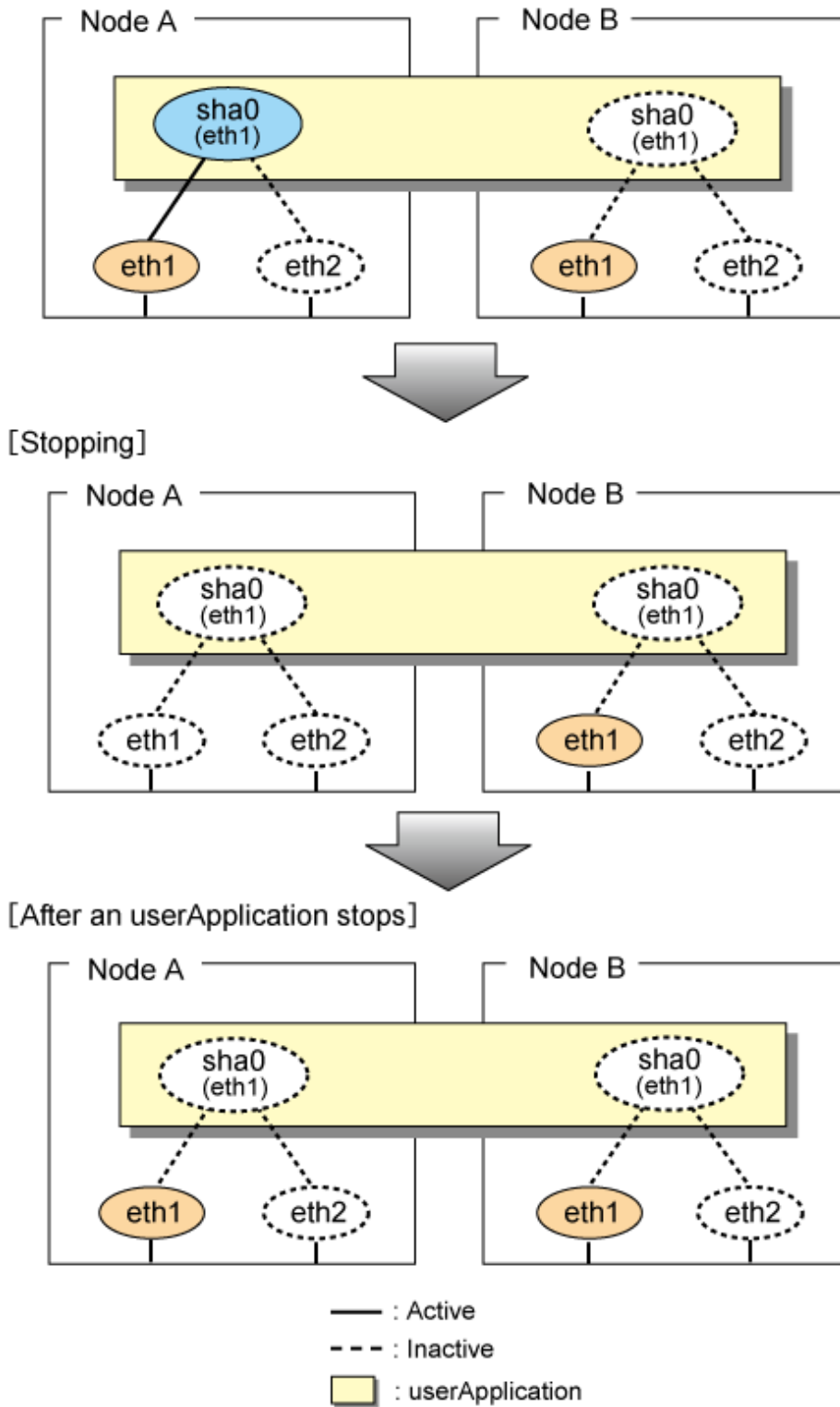
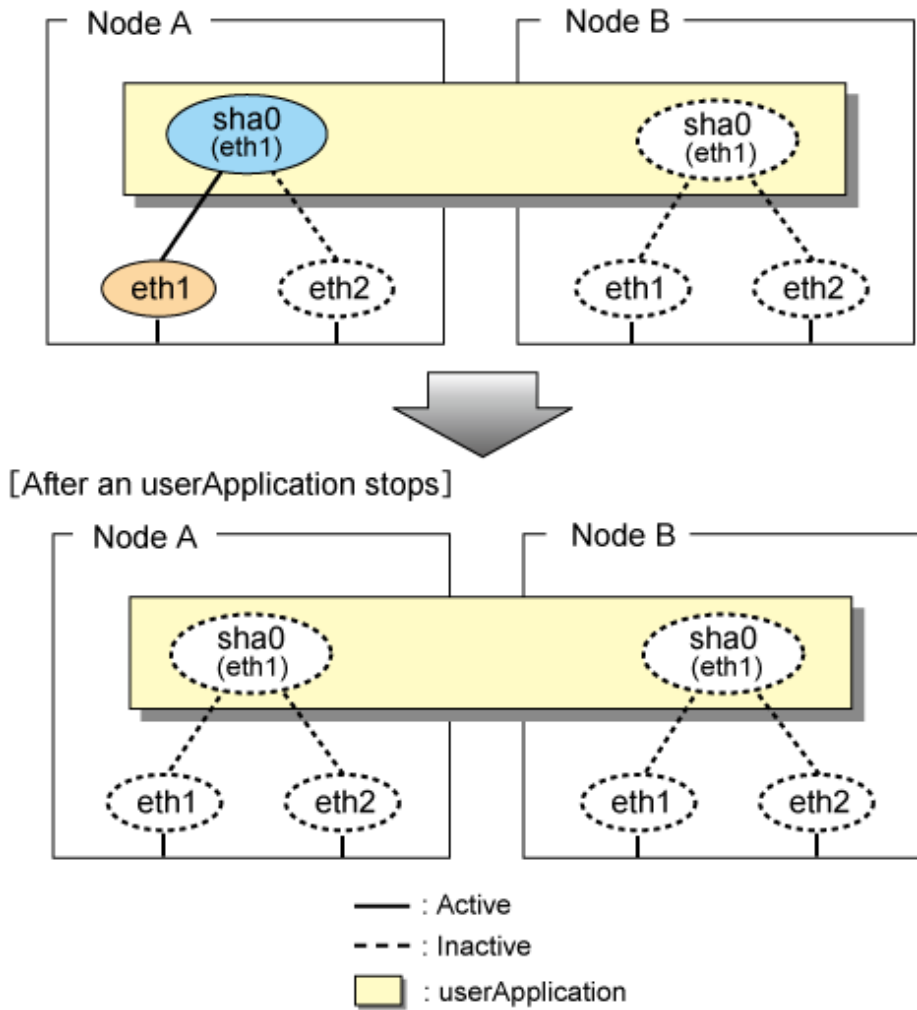


Figure 5.16 Stopping process of NIC switching mode (physical IP takeover II) illustrates stopping behavior of userApplication for the physical IP takeover II.

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.

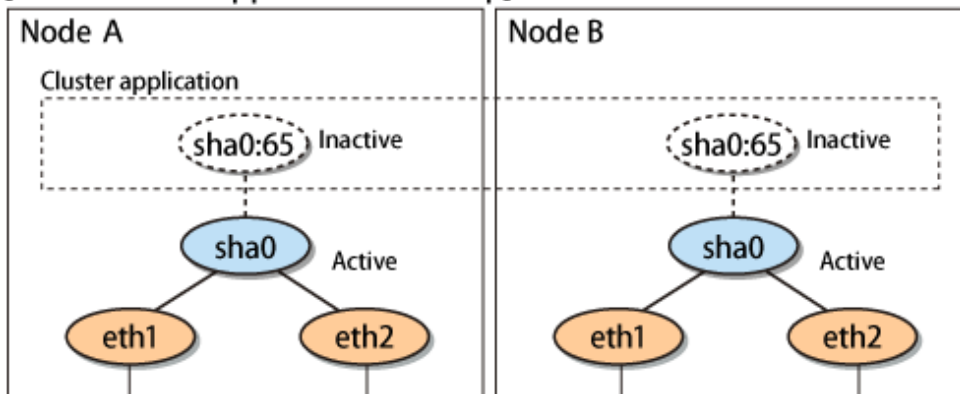
Once it becomes active, regardless of stopping or restarting userApplication, it remains to be active until the system stops.

Figure 5.17 Startup behavior of Virtual NIC mode shows behavior of Virtual NIC mode after starting up

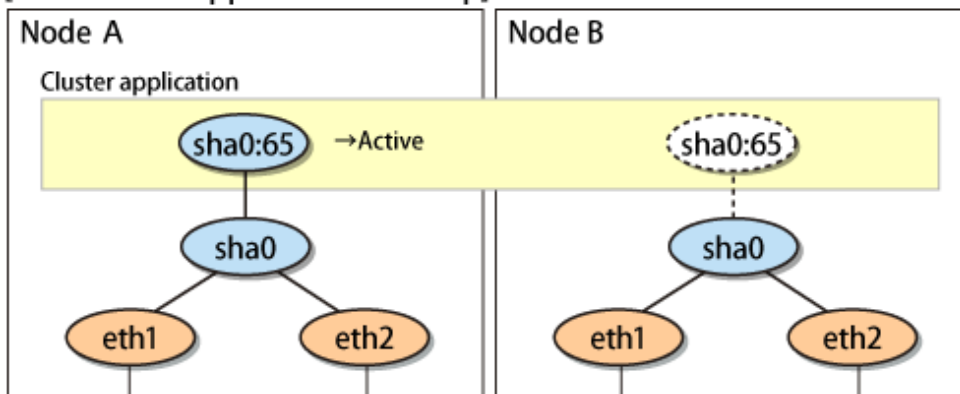


Figure 5.17 Startup behavior of Virtual NIC mode

[Before cluster application starts up]



[After 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.

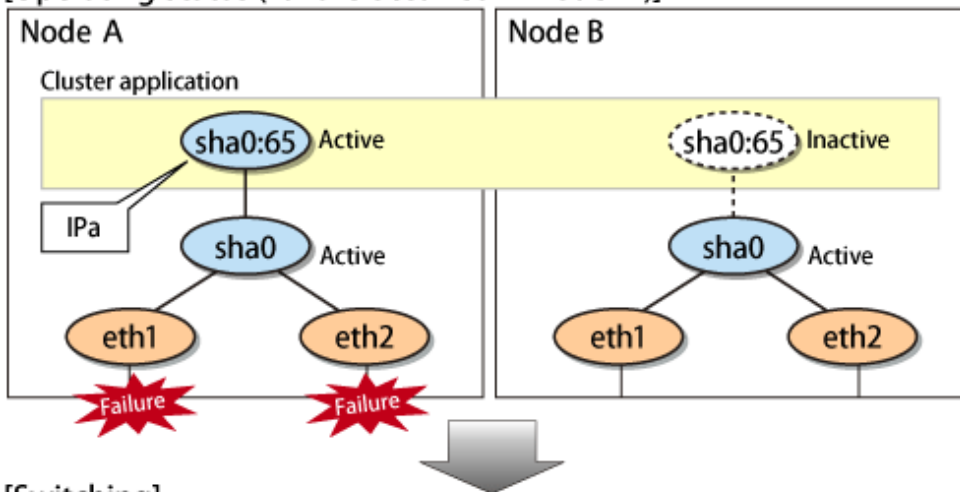
If a failure (panic, hang-up, or line failure) occurs on the operating node, Redundant Line Control Function switches the resources to the standby node. Then, applications make reconnection to take over the communication from the operating node.

Figure 5.18 Switching behavior of Virtual NIC mode indicates switching behavior of Virtual NIC mode.

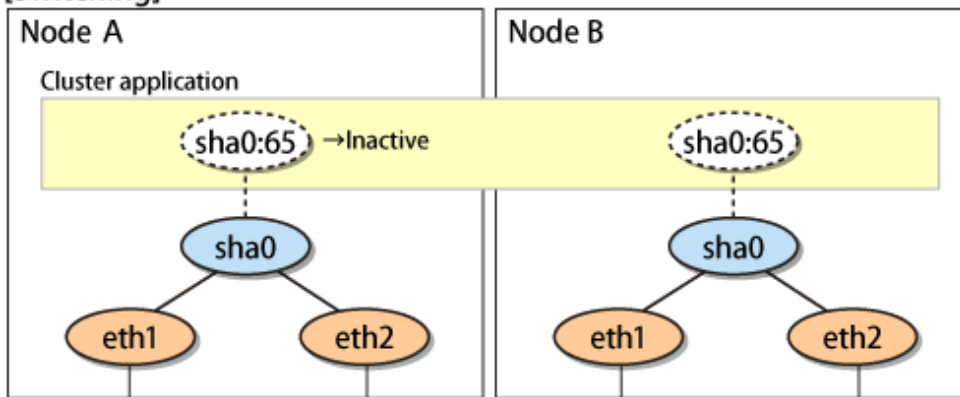
In the following figure, the takeover IP address (IPa) is allocated to the takeover virtual interface (sha0:65) for operating node A. Then it activates the takeover virtual interface. When switching the interface due to failures in the transfer path, the takeover virtual interface (sha0:65) for operating 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

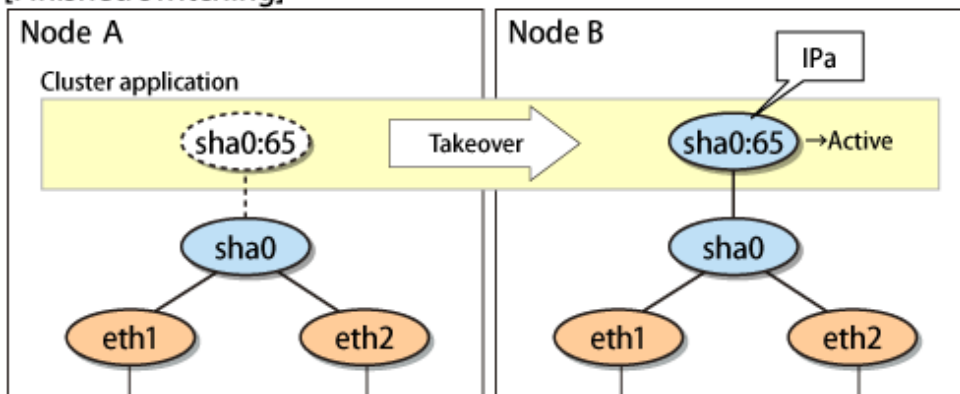
**[Operating Status (Failure occurred in node A)]**



**[Switching]**



**[Finished switching]**



**P 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.

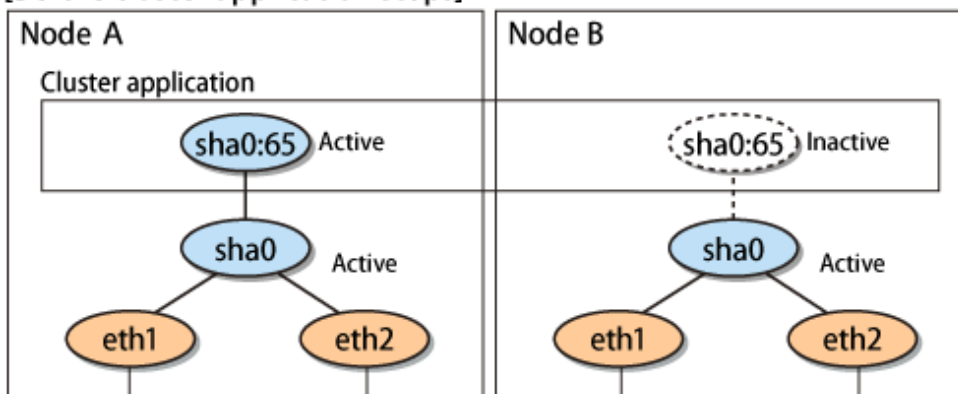
Restore the original operation status by performing fail-back operation for userApplication from "Cluster Admin" in Web-Based Admin View.

## 5.4.3.4 Stopping

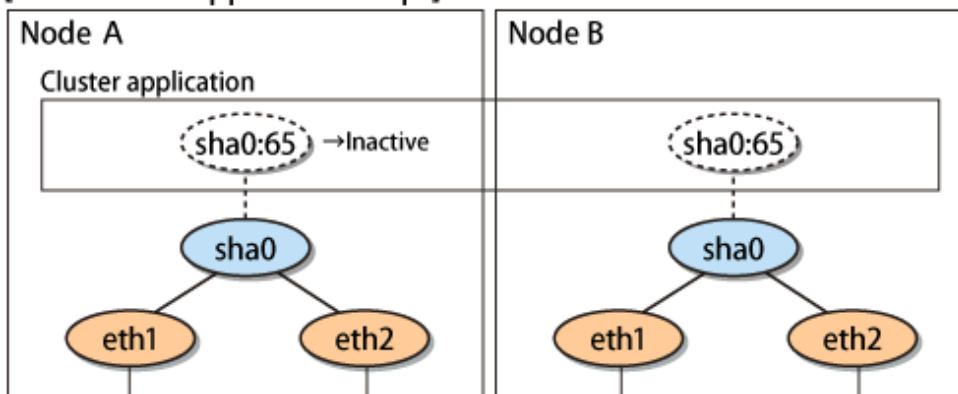
Figure 5.19 Stopping behavior of Virtual NIC mode illustrates stopping process of userApplication.

Figure 5.19 Stopping behavior of Virtual NIC mode

[Before cluster application stops]



[After cluster application stops]



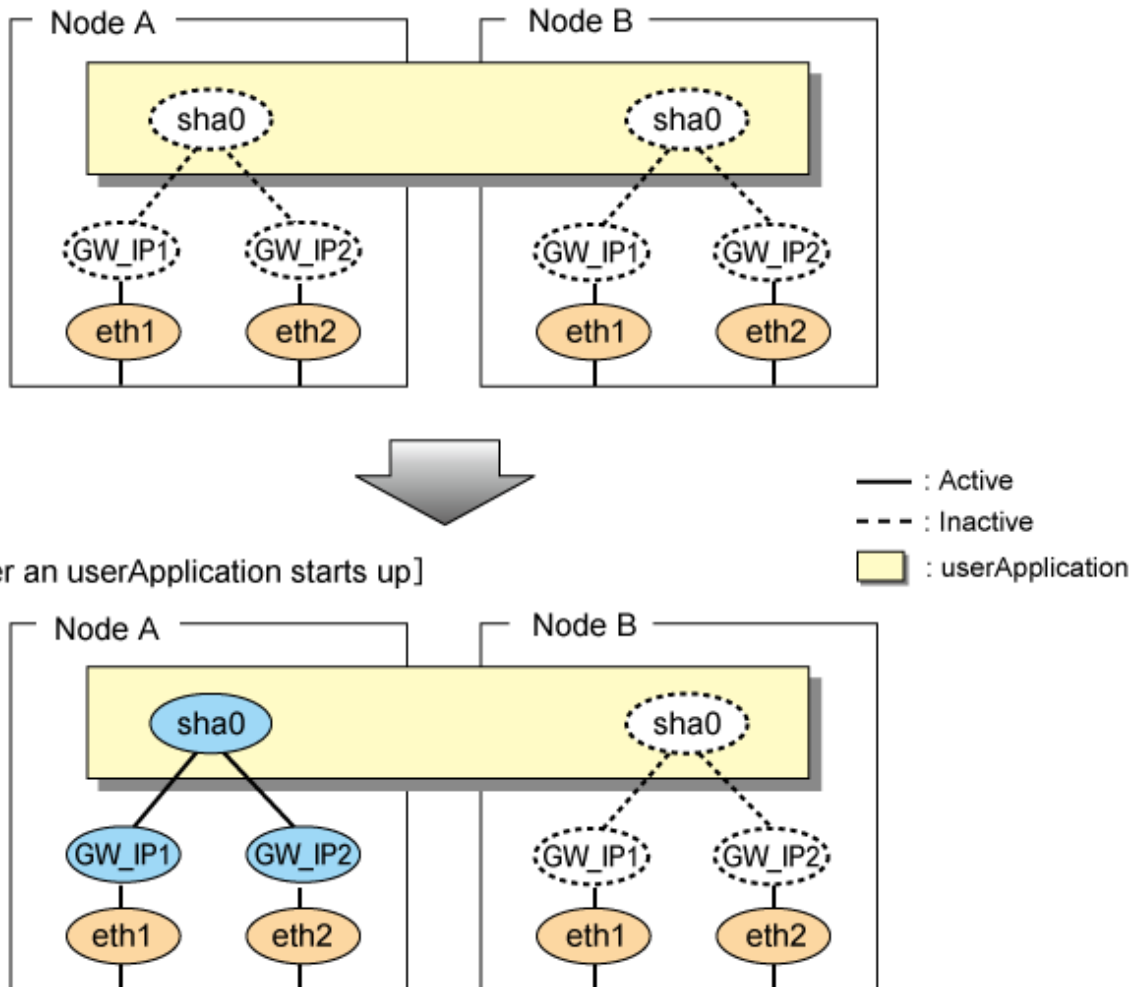
## 5.4.4 Active Standby (GS linkage mode)

### 5.4.4.1 Starting

By starting userApplication, the takeover virtual interface (sha0) and the gateway addresses (GW\_IP1, GW\_IP2) on the operating node become active allowing communication using the takeover virtual IP address. During normal operation, the GS linkage mode uses the takeover virtual interface on the operating node to communicate with the remote system.

Figure 5.20 Startup behavior of GS linkage mode shows startup behavior of the GS linkage mode.

Figure 5.20 Startup behavior of GS linkage mode  
 [Before an userApplication starts up]



Note

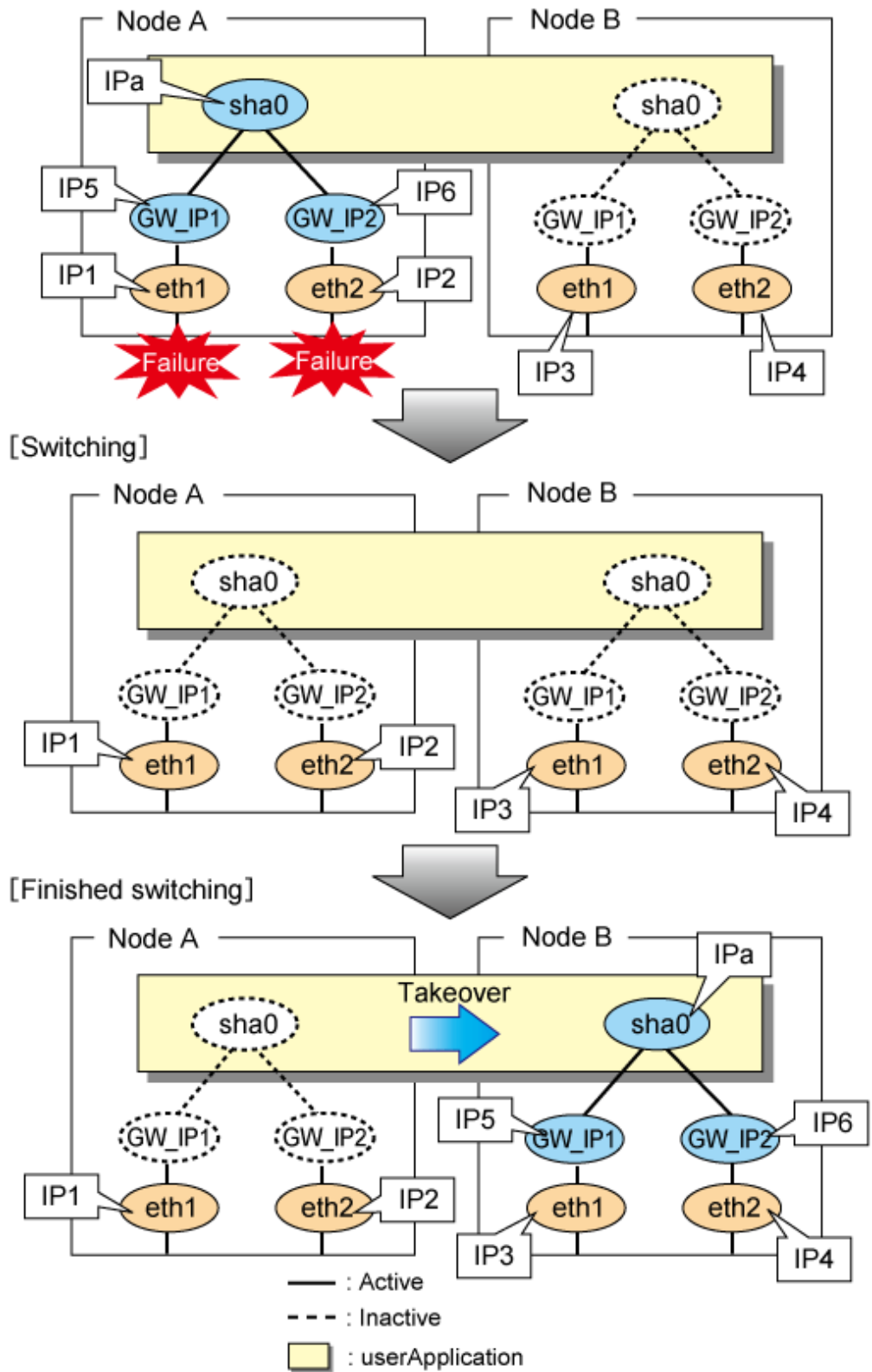
Activate the gateway addresses (GW\_IP1, GW\_IP2) only when they are connected to GS via a router.

### 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 the gateway addresses (GW\_IP1, GW\_IP2) only when they are connected to GS via a router.

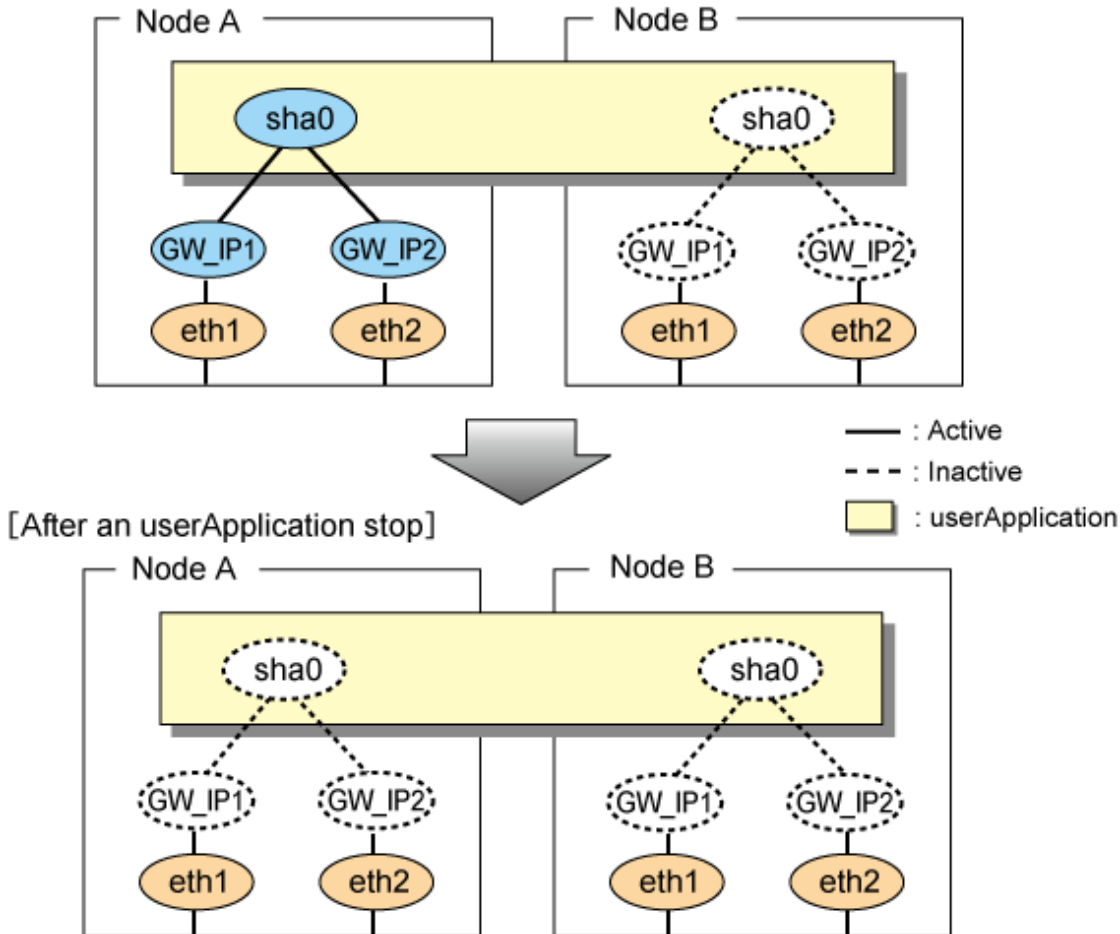
### 5.4.4.3 Fail-back

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 the gateway addresses (GW\_IP1, GW\_IP2) only when they are connected to GS via a 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

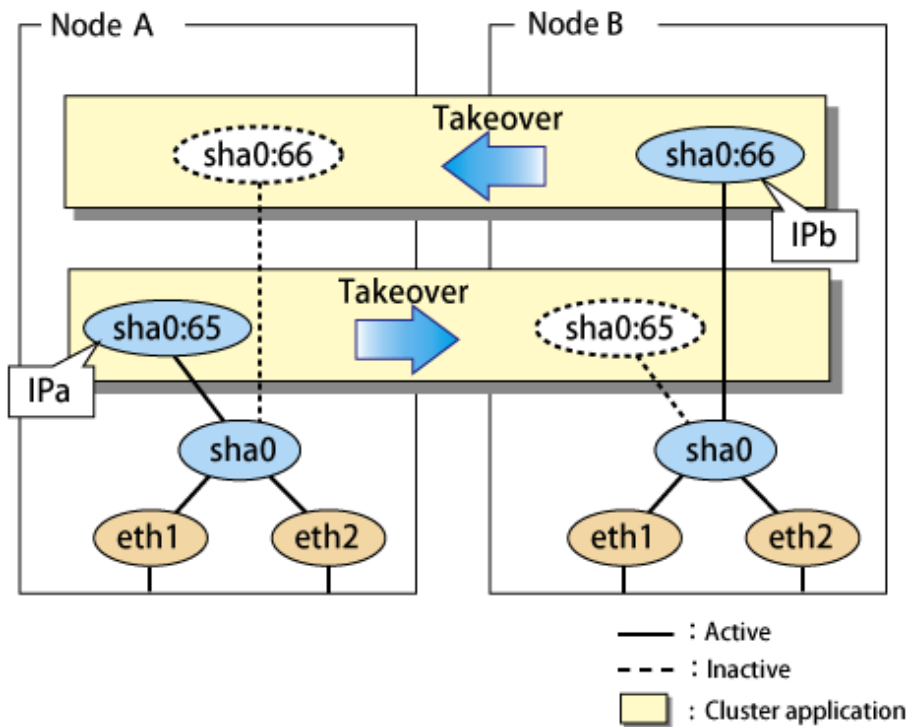
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "5.4.1.1 Starting".

## 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)

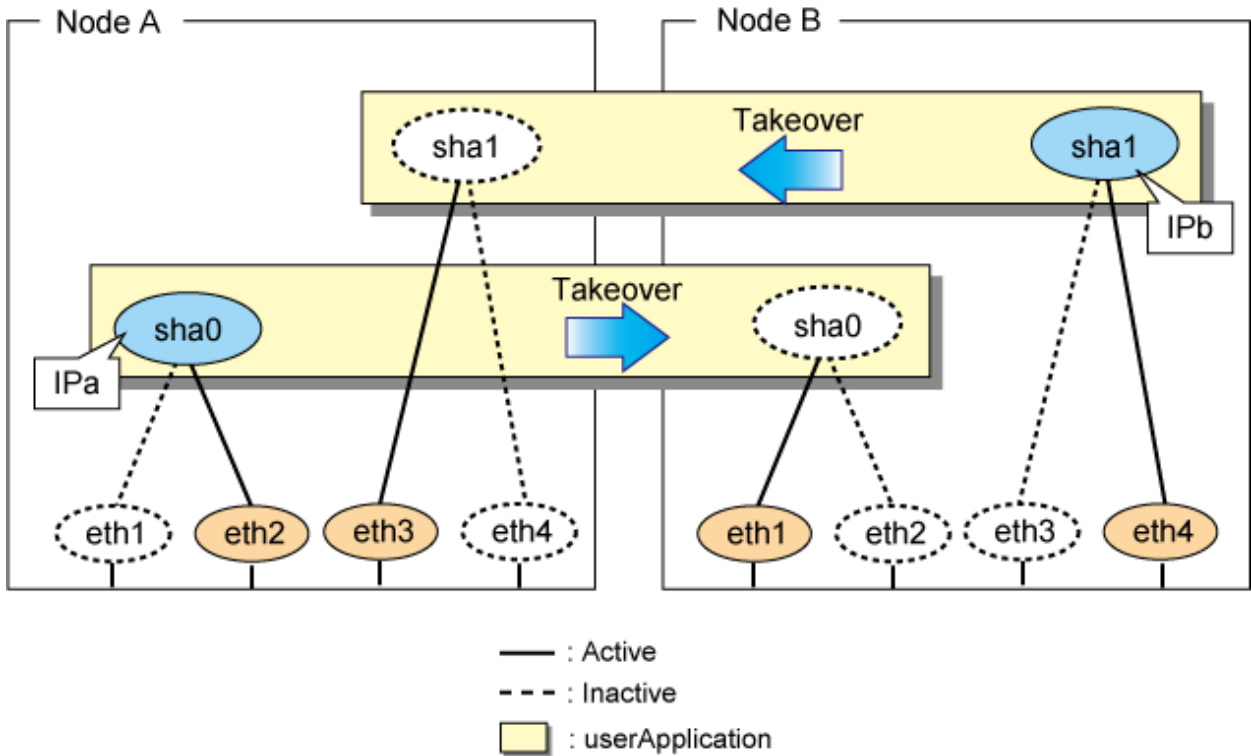
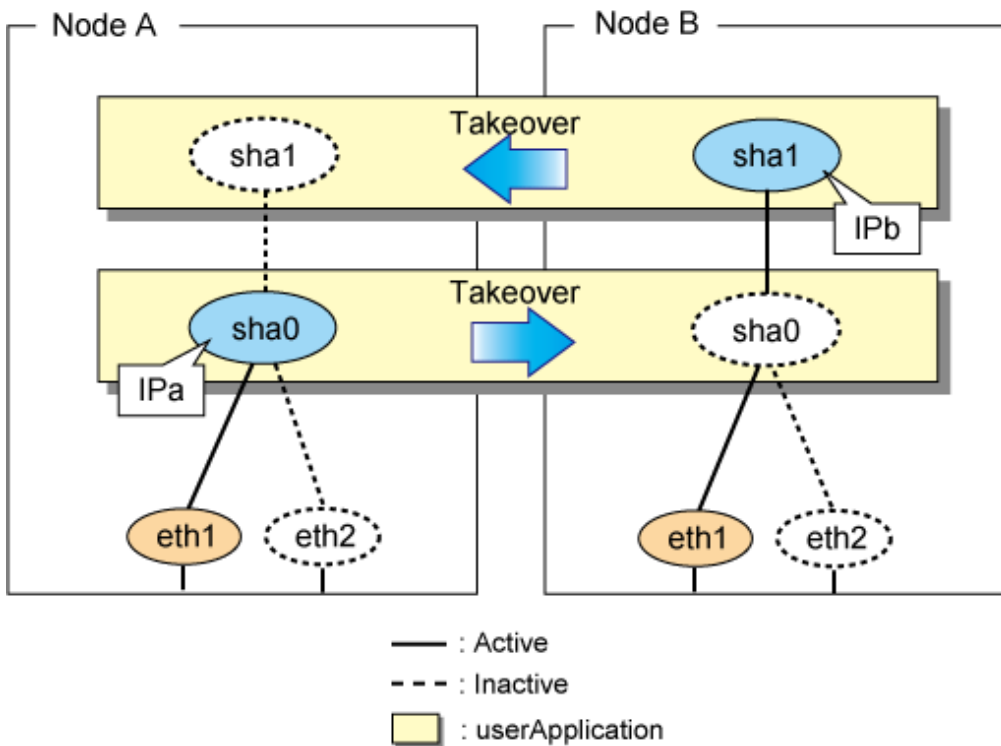


Figure 5.25 Mutual standby configuration diagram in NIC switching mode (NIC sharing) shows the mutual standby configuration diagram in NIC switching mode (NIC sharing). The takeover of an address, etc. is performed in the same way as for the active standby configuration. For more information, see "5.4.2.2 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

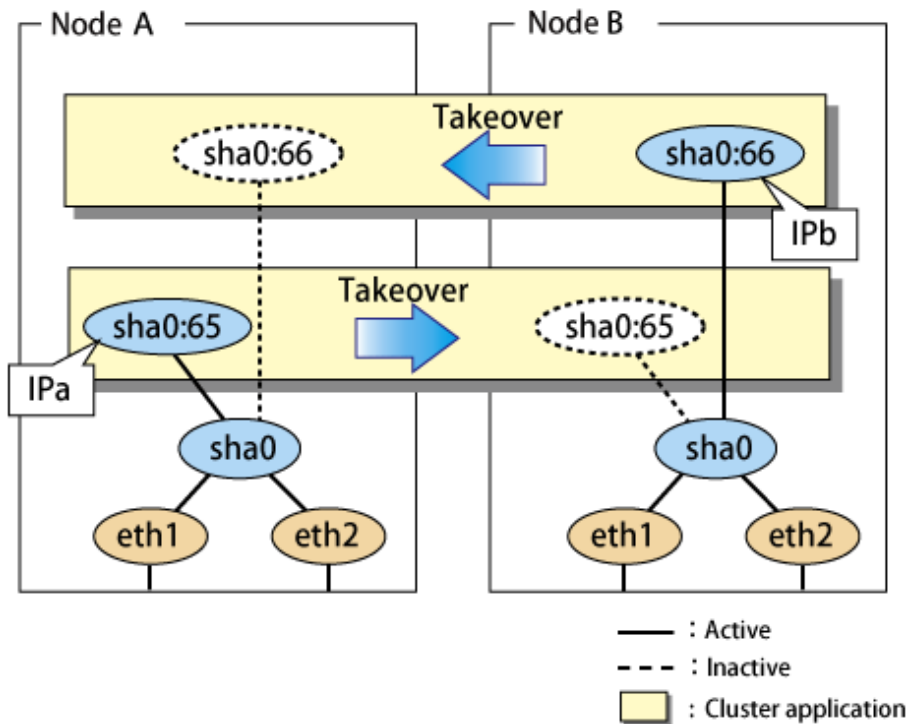
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "5.4.3.1 Starting".

### 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

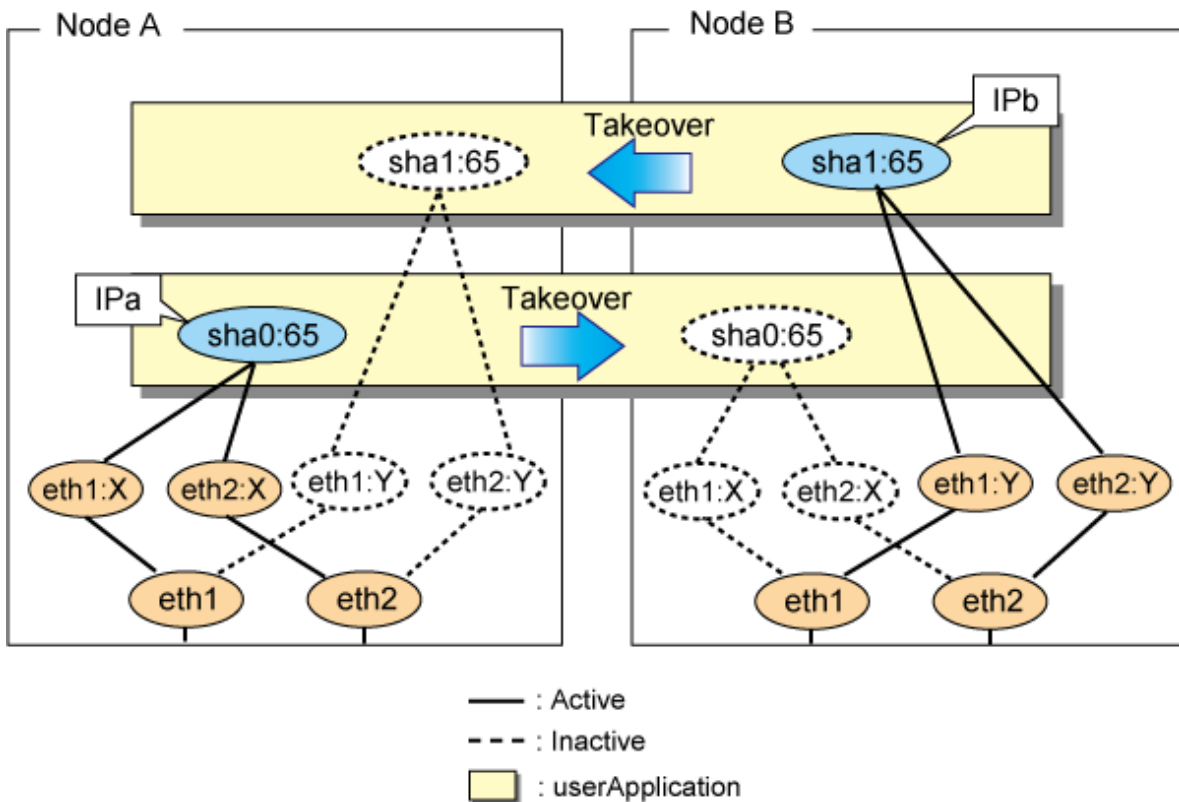
Starting process is equivalent to the active standby operation, except that the mutual standby operation contains various userApplications. For more information, see "5.4.4.1 Starting".

### 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

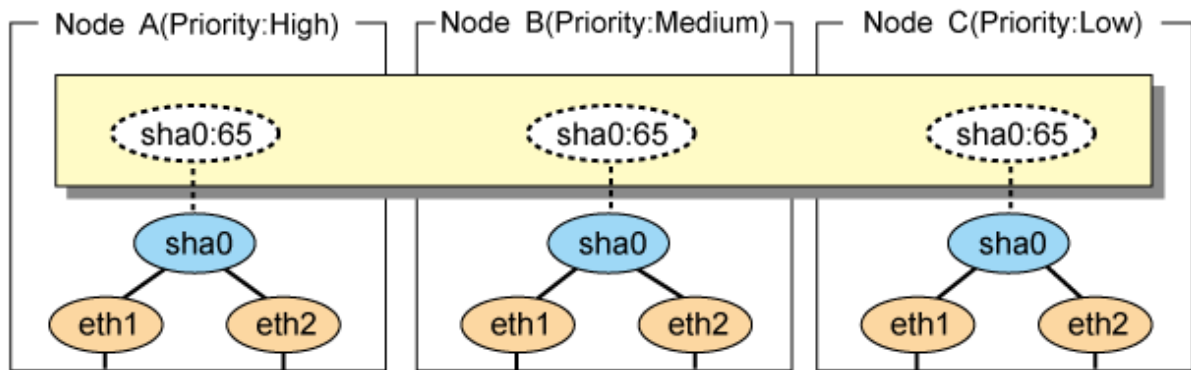
When the userApplication starts up, the takeover virtual interface (sha0:65) becomes active on the operating node, allows to hold communication using the takeover virtual IP address.

During normal operation, userApplication communicates with the remote system using the virtual interface on the operating node.

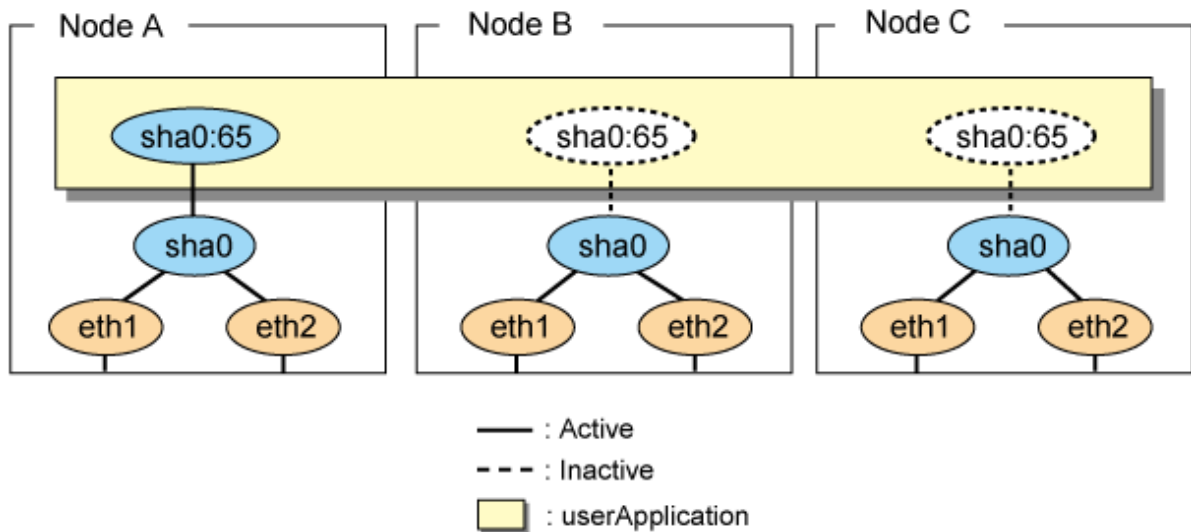
After the redundant control function start-up, the virtual interface is activated. Once it has been activated, regardless of the cluster system shutdown or restart, it stays to be active until the system shuts down.

[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]



[After an userApplication starts up]



### 5.4.9.2 Switching

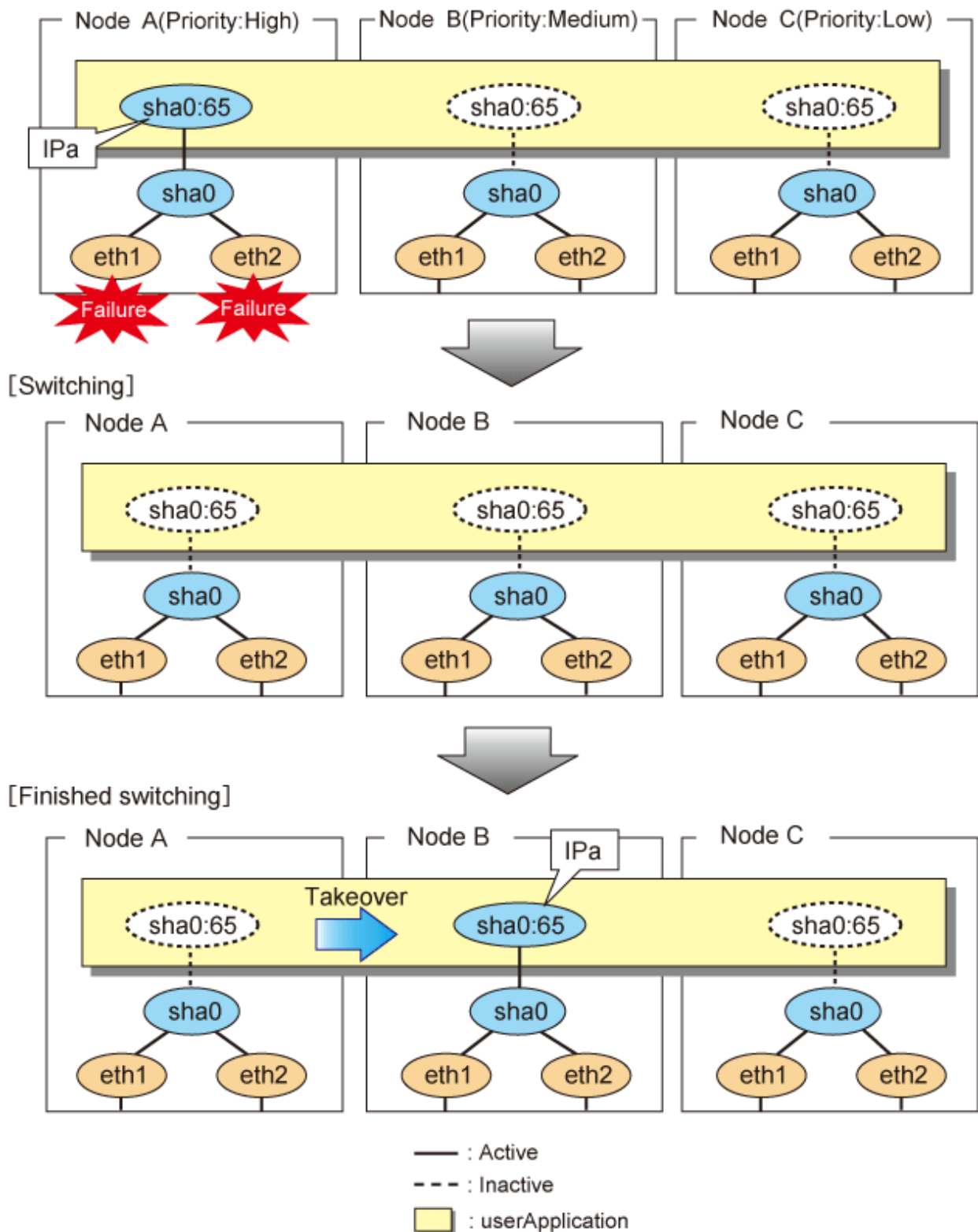
During normal operation, userApplication communicates with the remote system using the takeover virtual interface on the operating node.

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

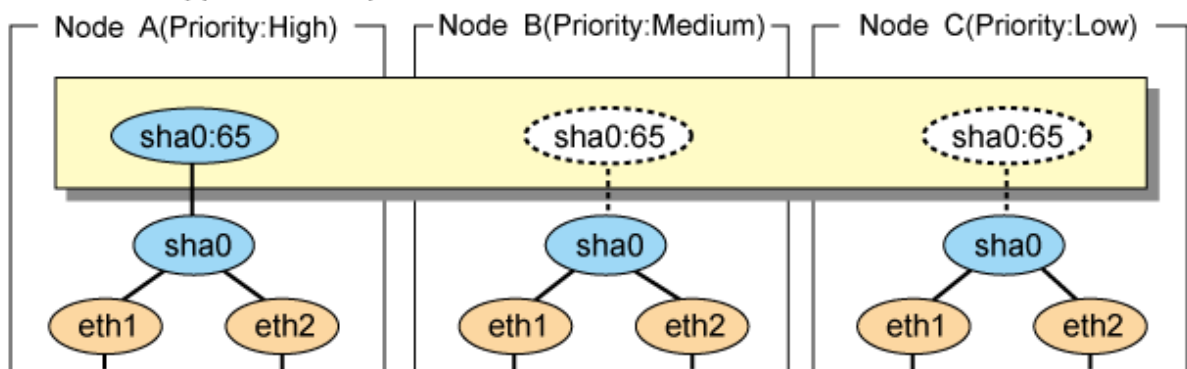
Fail-back the userApplication to an arbitrary node on standby using "Cluster Admin" of Web-Based Admin View.

## 5.4.9.4 Stopping

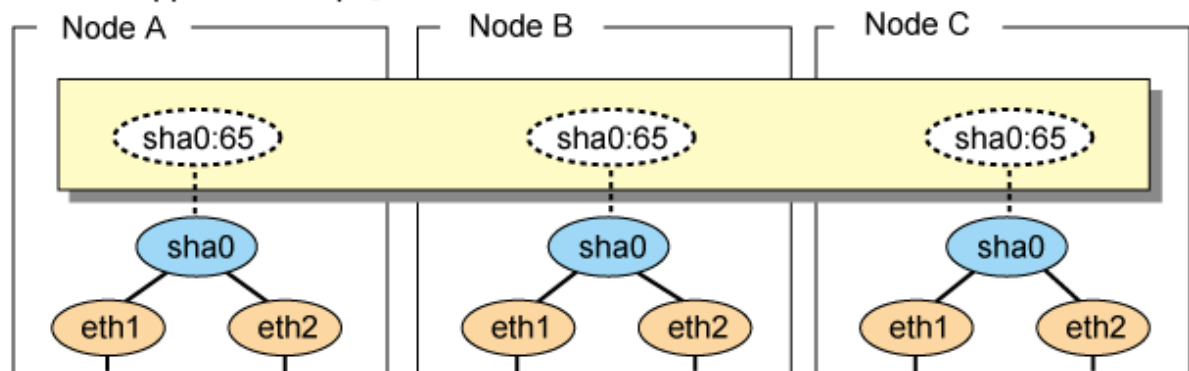
Figure 5.30 Stopping operation of Fast switching mode illustrates stopping operation of a userApplication

Figure 5.30 Stopping operation of Fast switching mode

[Before an userApplication stops]



[After an userApplication stops]



— : Active  
- - - : Inactive  
■ : userApplication

## 5.4.10 Cascade (NIC switching mode)

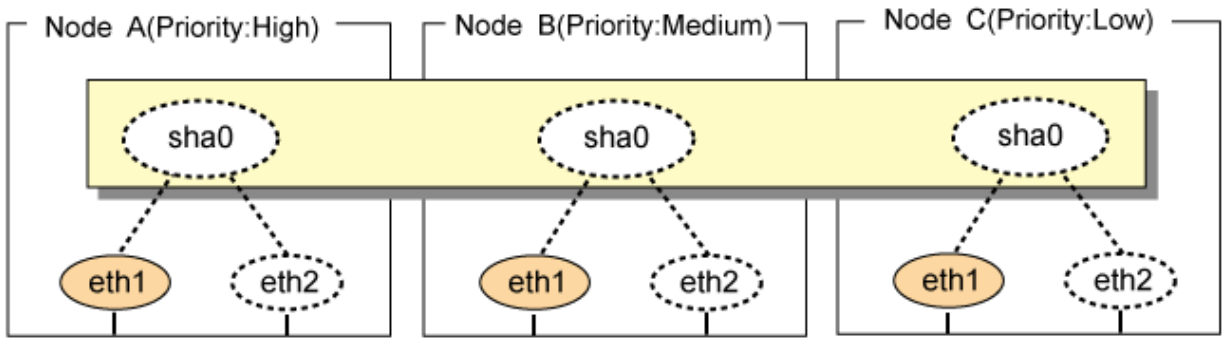
### 5.4.10.1 Starting

There are three types of IP takeover feature in NIC switching mode. For detail, refer to "5.4.2.1 Starting".

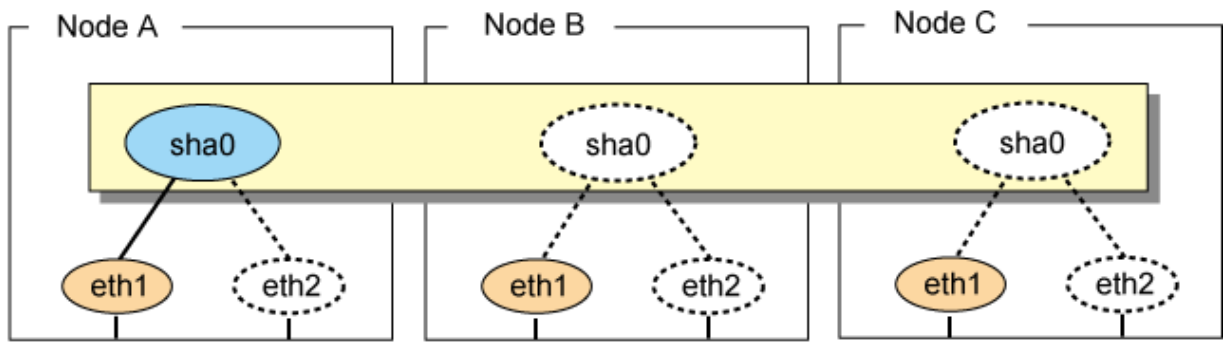
The physical interface (eth1) for each node becomes active when the redundant line control function starts up for logical IP takeover. Once the userApplication starts up, the takeover virtual interface then becomes active on the operating node which has higher priority.

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]



[After an userApplication starts up]

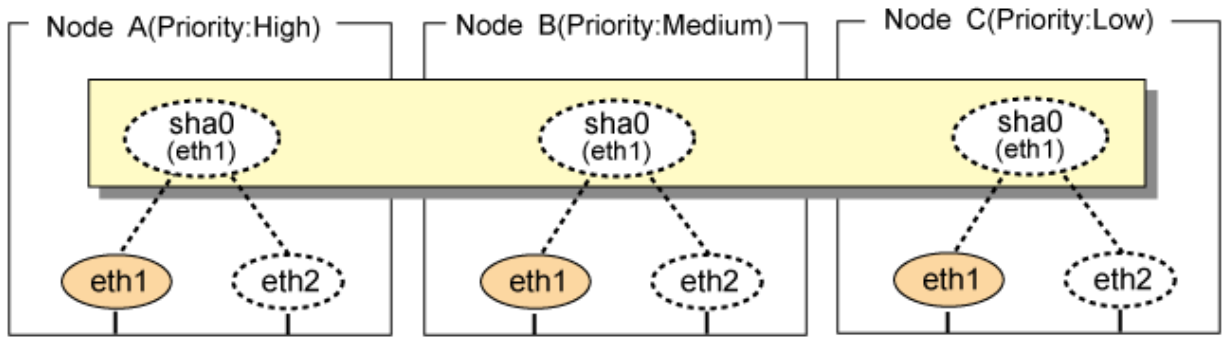


- : Active
- - - : Inactive
- : userApplication

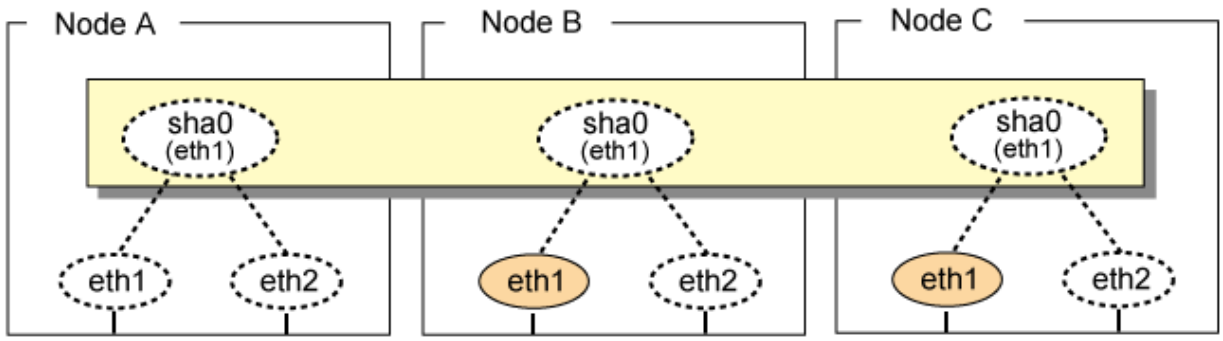
The physical interface (eth1) for each node becomes active when the redundant control function starts up for the physical IP takeover I. Once the userApplication starts up, it activates the physical interface (eth1) by allocating the takeover IP address to the physical interface (eth1) on the operating 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.

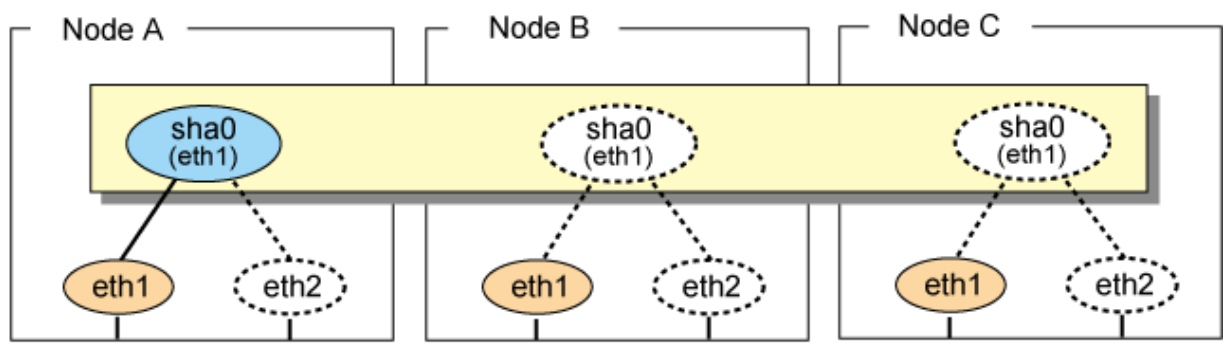
Figure 5.32 Start-up behavior of NIC switching mode (physical IP takeover I)  
 [Before an userApplication starts up]



[Starting an userApplication]



[After an userApplication starts up]



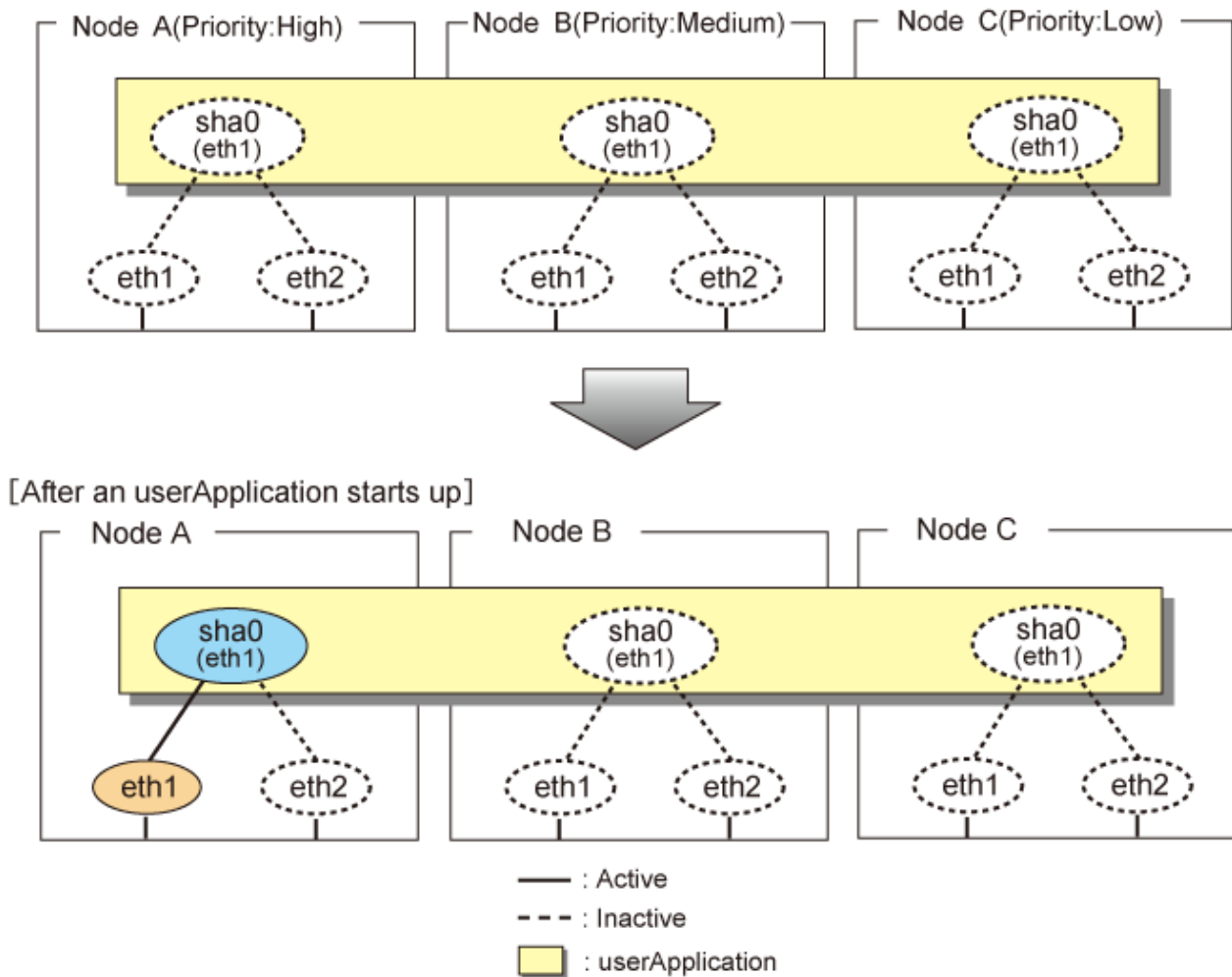
- : Active
- - - : Inactive
- : userApplication

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) is allocated to the logical interface for the secondary interface (eth2) on the operating node A. Once IPa is allocated, the logical interface for the secondary interface turns into the activated state.

When switching the node due to a failure in the transfer routes, the NIC switching mode inactivates the takeover virtual interface to which the takeover IP address (IPa) has been allocated on the operating node A. Then it allocates the takeover IP address (IPa) to the primary interface (eth1) which has already been activated on the standby node B and finally activates the logical interface.

Figure 5.34 Switching operation of NIC switching mode (logical IP takeover)  
 [Operating Status(Failure occurred in node A)]

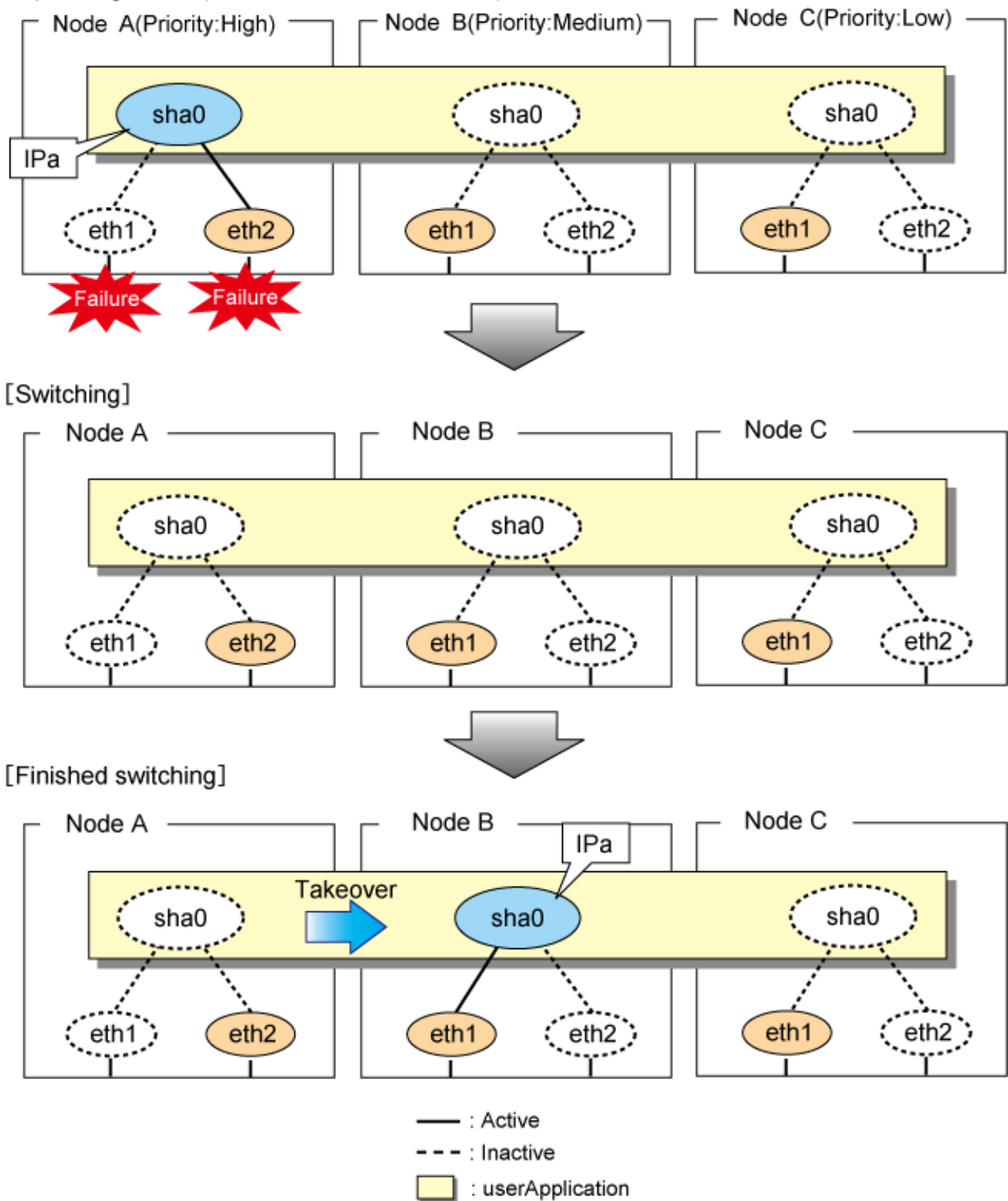


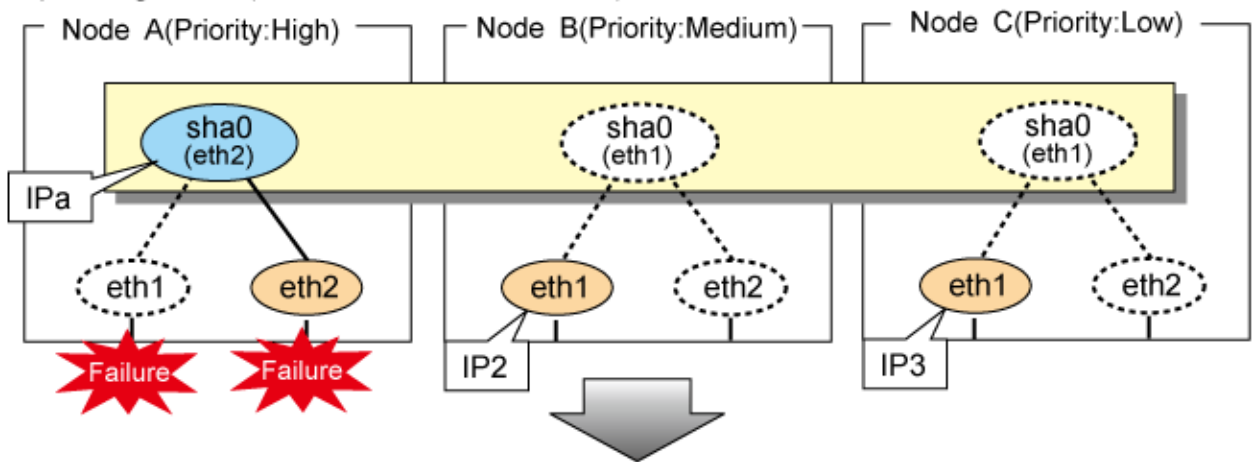
Figure 5.35 Switching operation of NIC switching mode (physical IP takeover I) (continues) and Figure 5.36 Switching operation of NIC switching mode (physical IP takeover I) (end) illustrate switching behavior of NIC switching mode (takeover physical IP address I).

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.

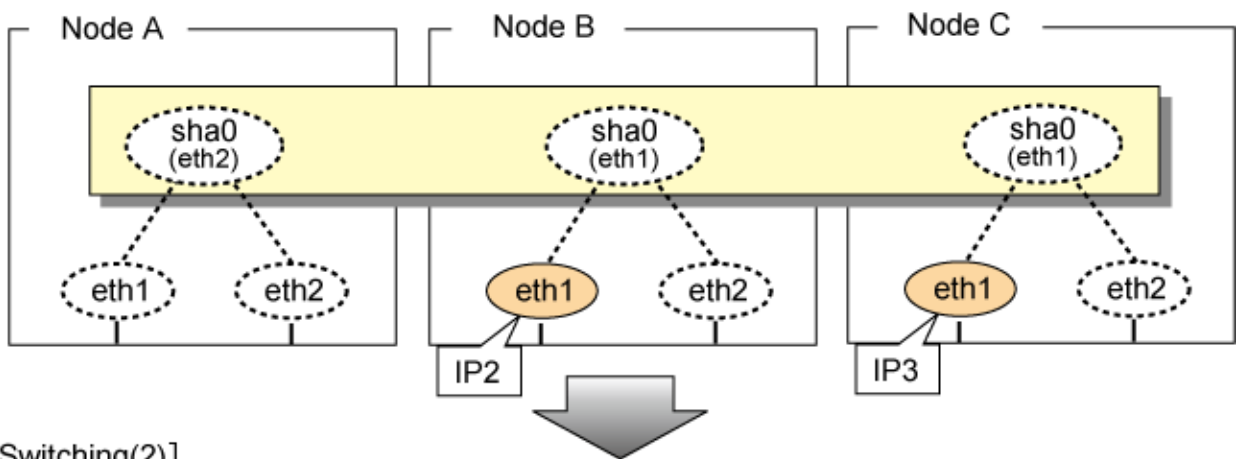
When switching the node due to a failure in the transfer routes, temporally inactivate the primary interface (eth1), which has been active in the standby node B. Then it allocates the takeover IP address (IPa) to activate the primary interface (eth1). Once the primary interface activates, different IP 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)]

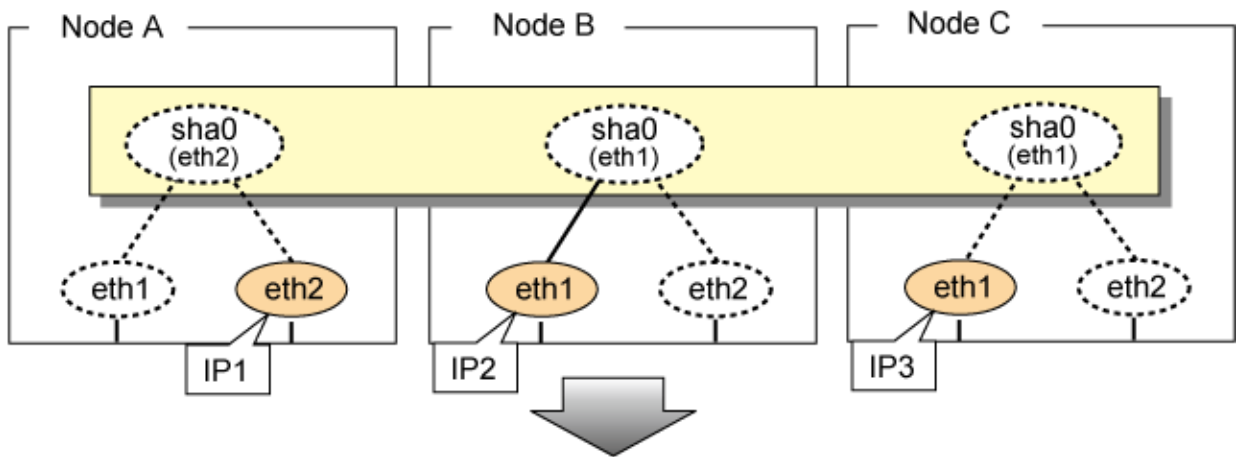


Figure 5.36 Switching operation of NIC switching mode (physical IP takeover I) (end)  
 [Switching(3)]

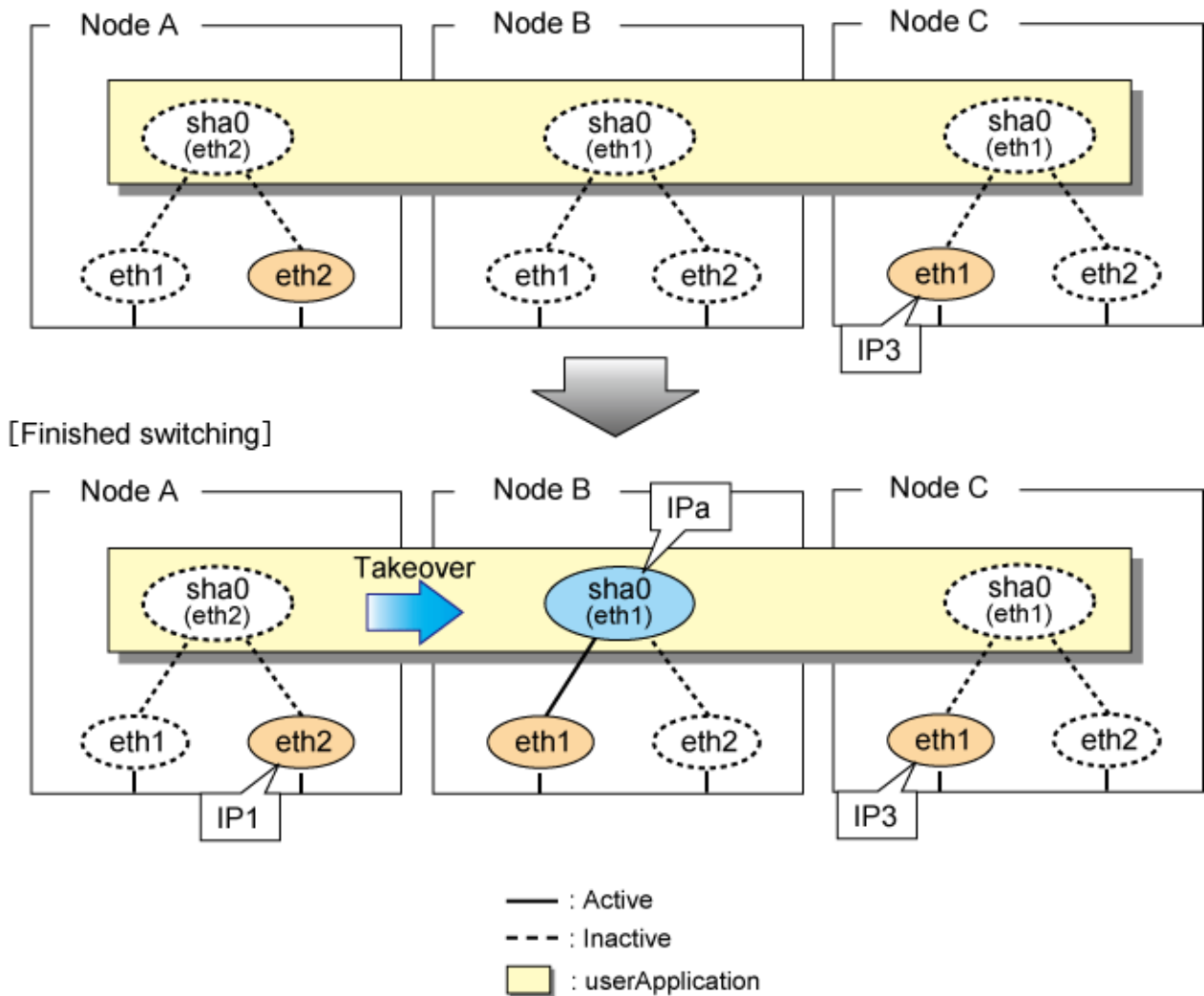


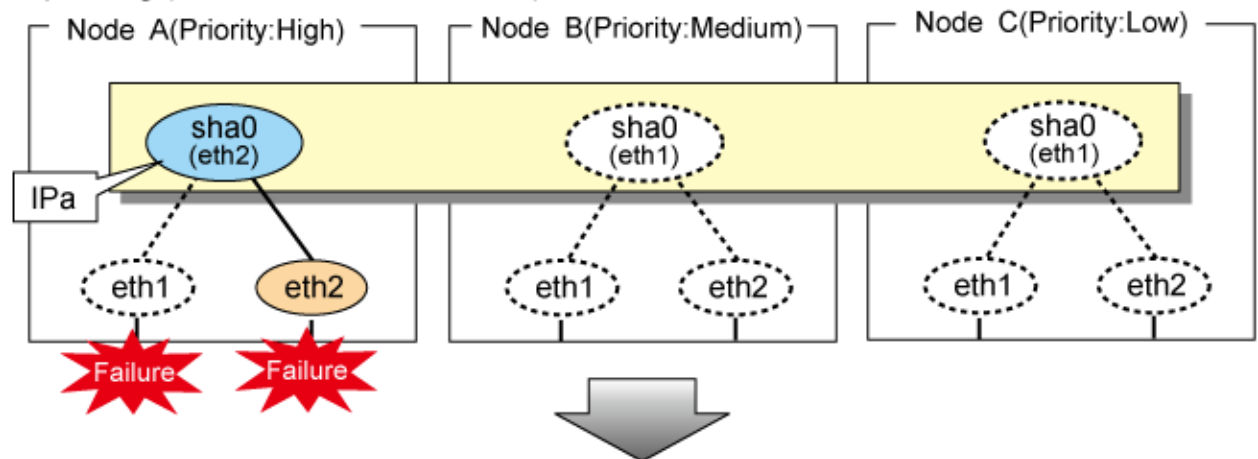
Figure 5.37 Switching operation of NIC switching mode (physical IP takeover II) illustrates switching behavior of NIC switching mode (takeover physical IP address I).

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.

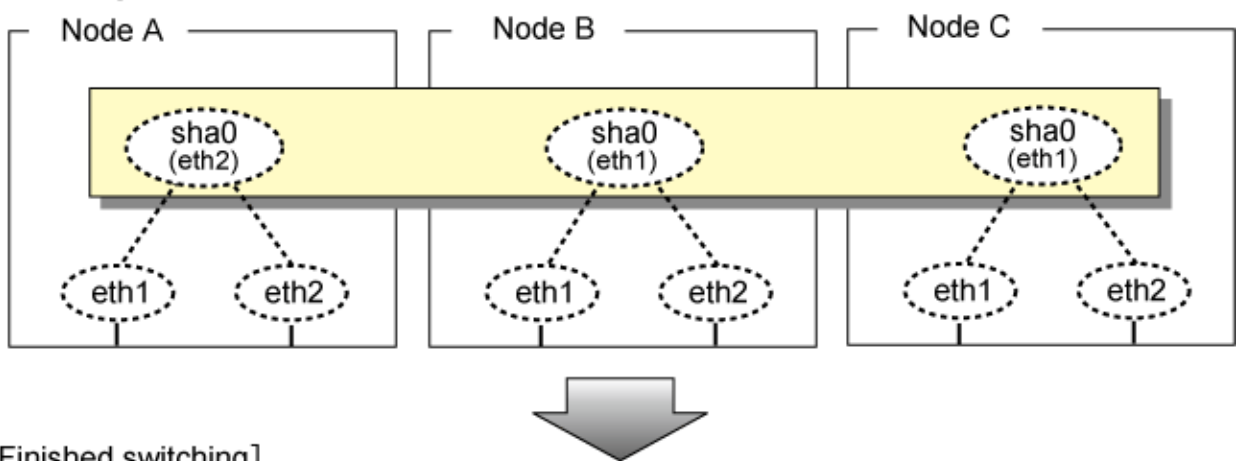
When switching the node because of a failure in the transfer path, activate the standby node B turns to be active by allocating the takeover IP address (IPa) to the primary interface (eth1). After the IP address is successfully passed over to the standby node B, becomes inactive the secondary interface (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)

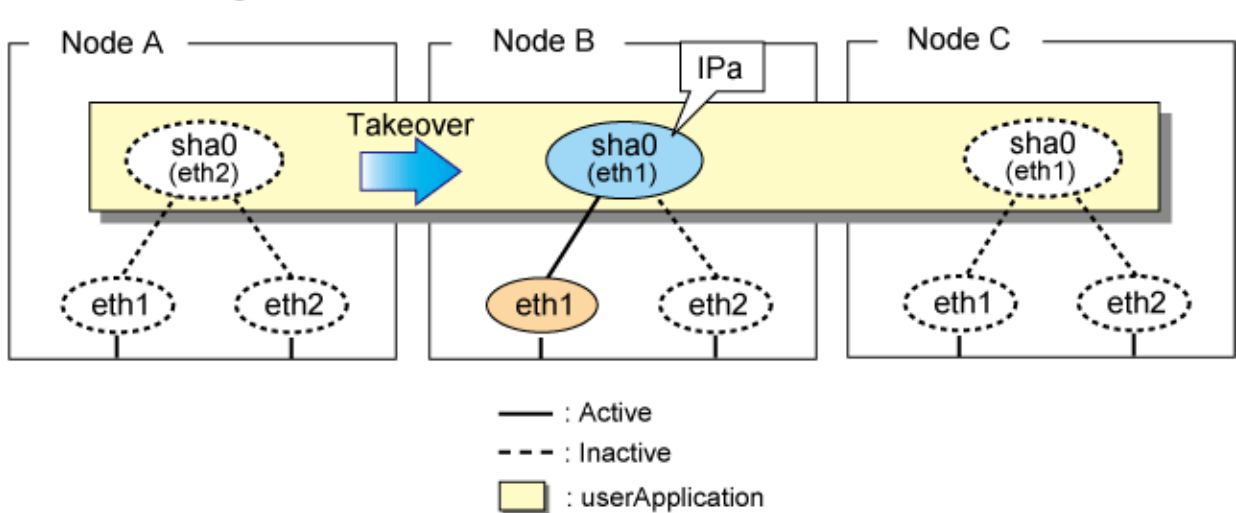
[Operating (Failure occurred in node A)]



[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]

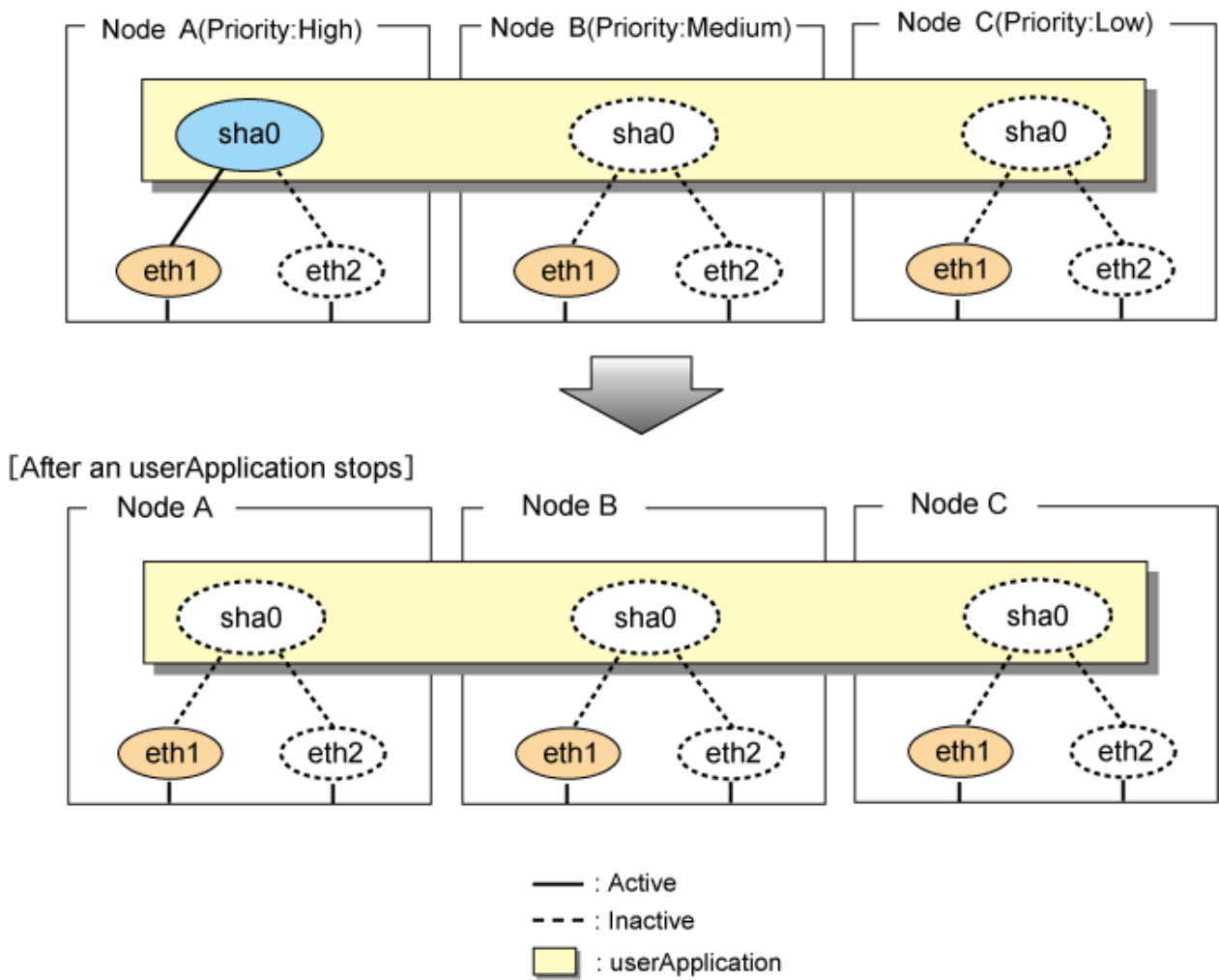
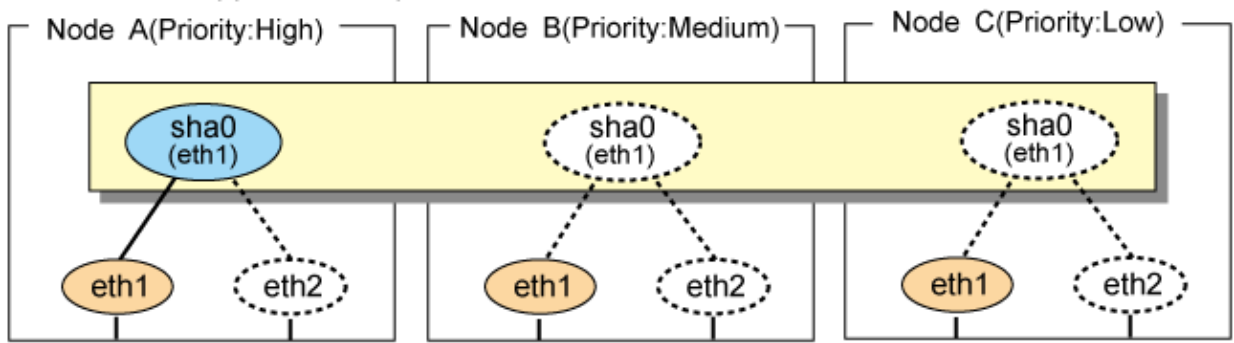
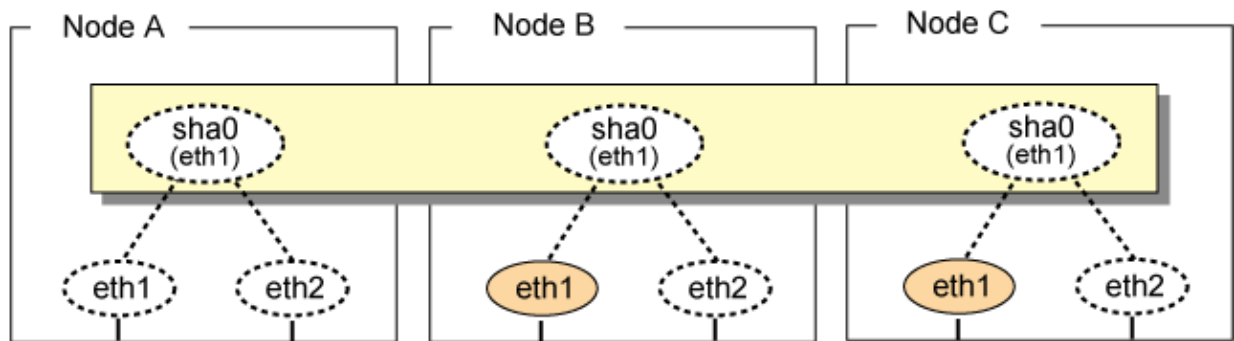


Figure 5.39 Stopping operation of NIC switching mode (physical IP takeover I) illustrates stopping operation of a userApplication for physical IP takeover I.

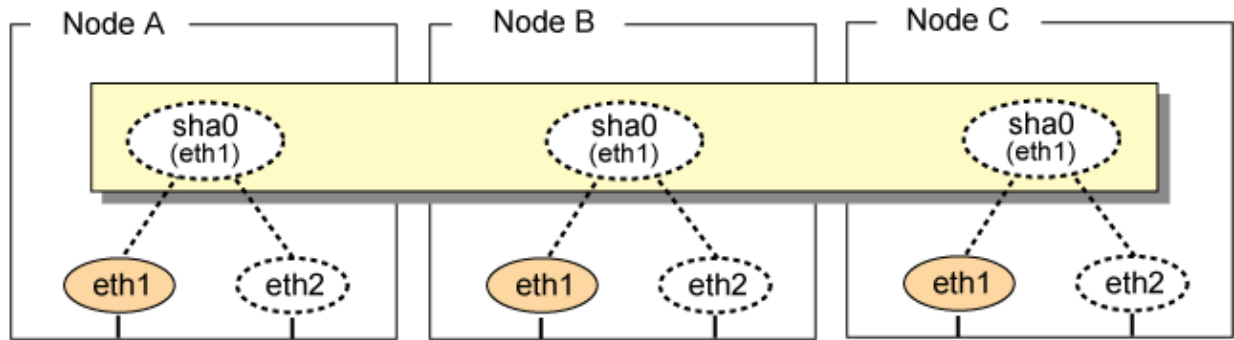
Figure 5.39 Stopping operation of NIC switching mode (physical IP takeover I)  
 [Before an userApplication stops]



[Stopping]



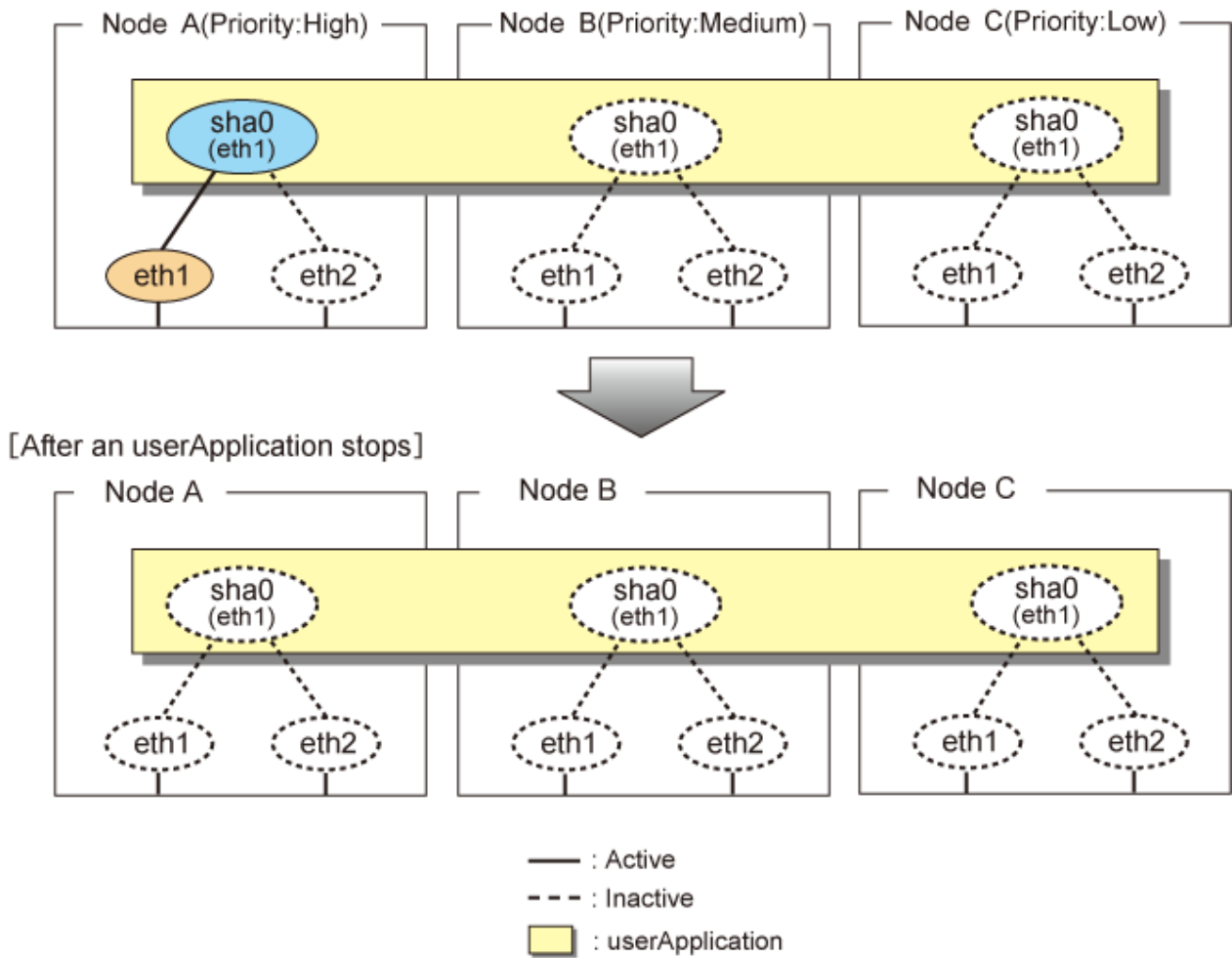
[After an userApplication stops]



- : Active
- - - : Inactive
- : userApplication

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.

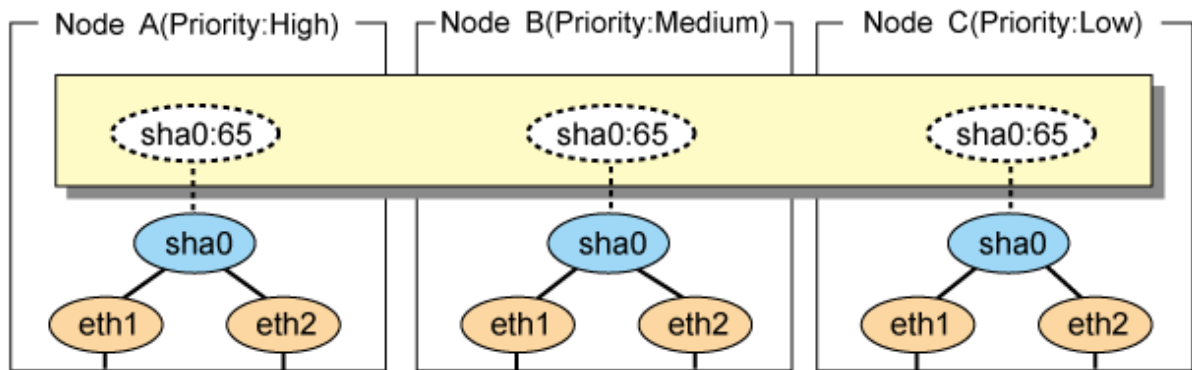
During normal operation, userApplication communicates with the remote system using the virtual interface on the operating node.

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.

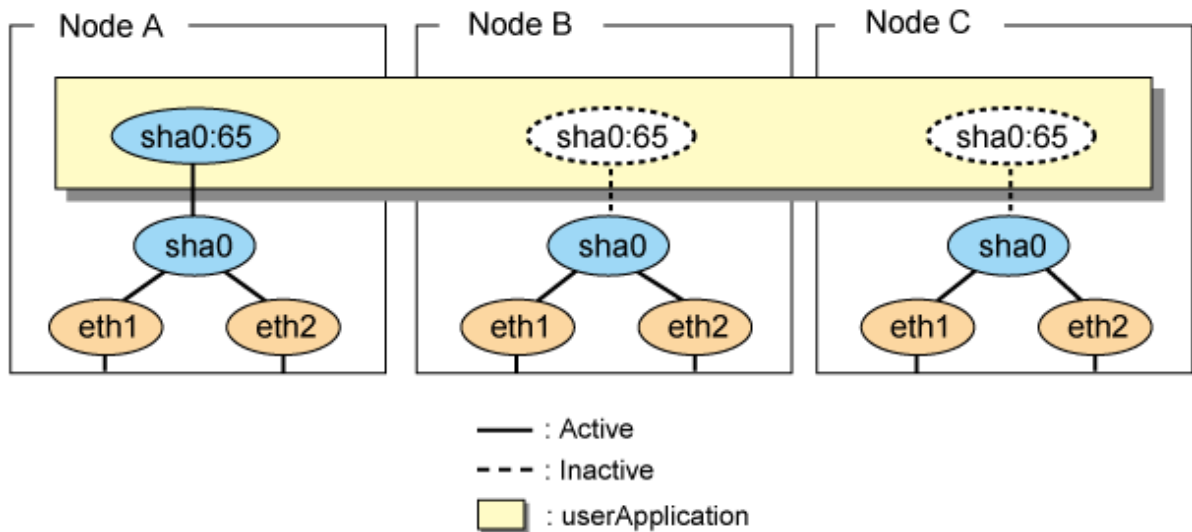
Figure 5.41 Startup behavior of Virtual NIC mode illustrates start-up behavior of Virtual NIC mode.



Figure 5.41 Startup behavior of Virtual NIC mode  
 [Before an userApplication starts up]



[After an userApplication starts up]



### 5.4.11.2 Switching

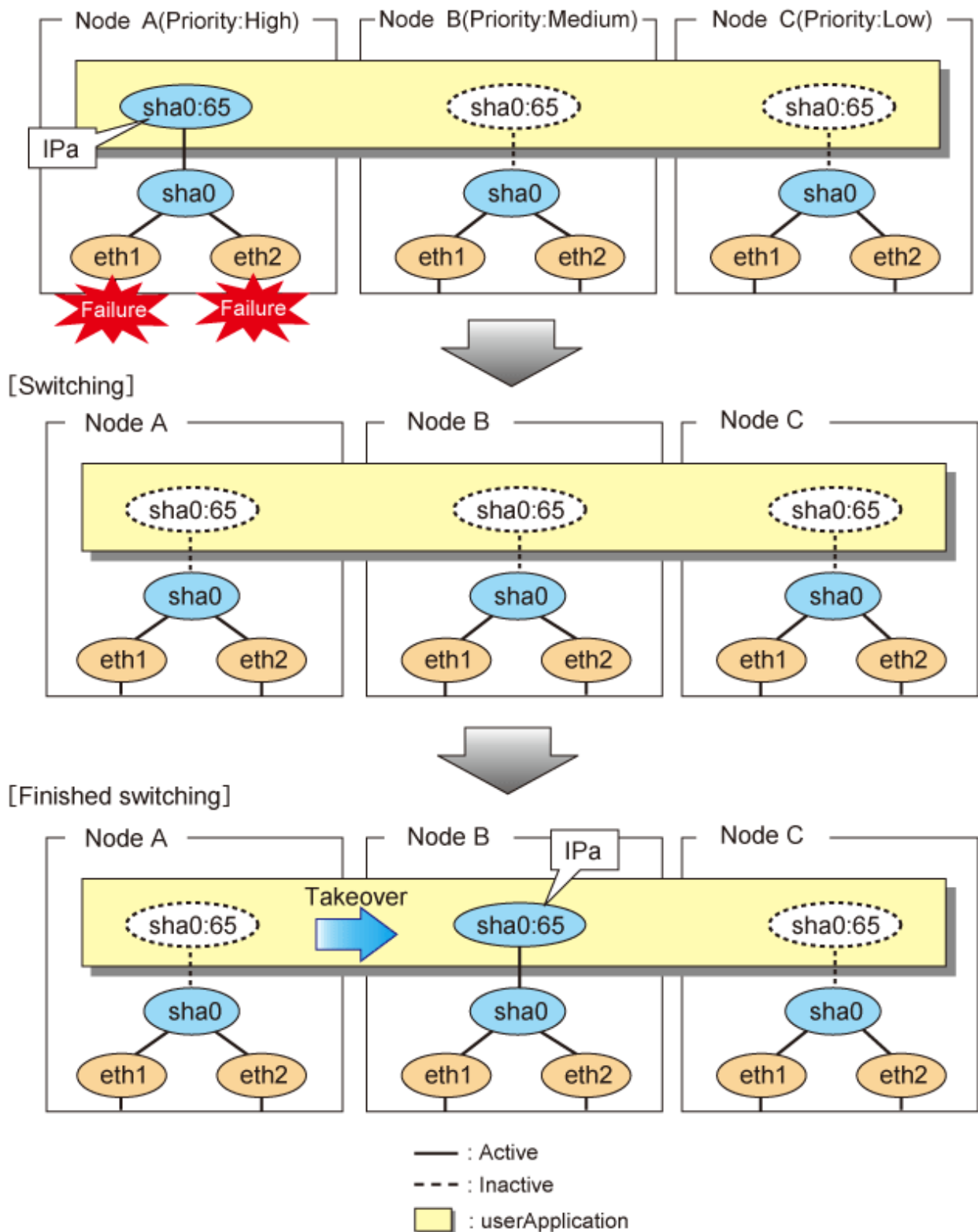
During normal operation, userApplication communicates with the remote system using the takeover virtual interface on the operating node.

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

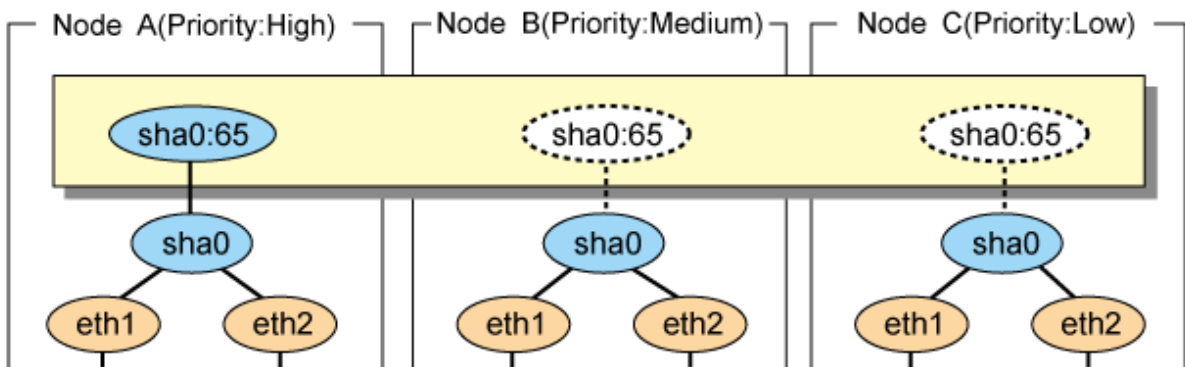
Fail-back the userApplication to an arbitrary node on standby using "Cluster Admin" of Web-Based Admin View.

## 5.4.11.4 Stopping

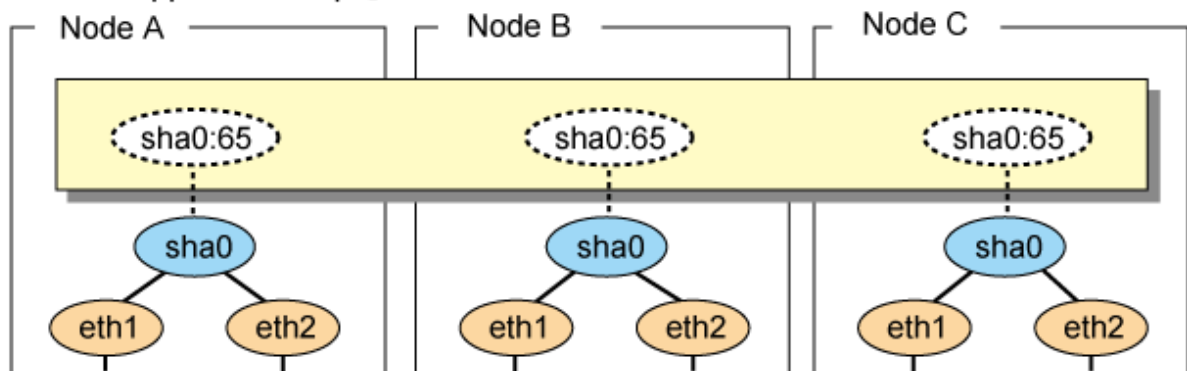
Figure 5.43 Stopping behavior of Virtual NIC mode illustrates stopping operation of a userApplication

Figure 5.43 Stopping behavior of Virtual NIC mode

[Before an userApplication stops]



[After an userApplication stops]



— : Active  
 - - - : Inactive  
 [Yellow Box] : userApplication

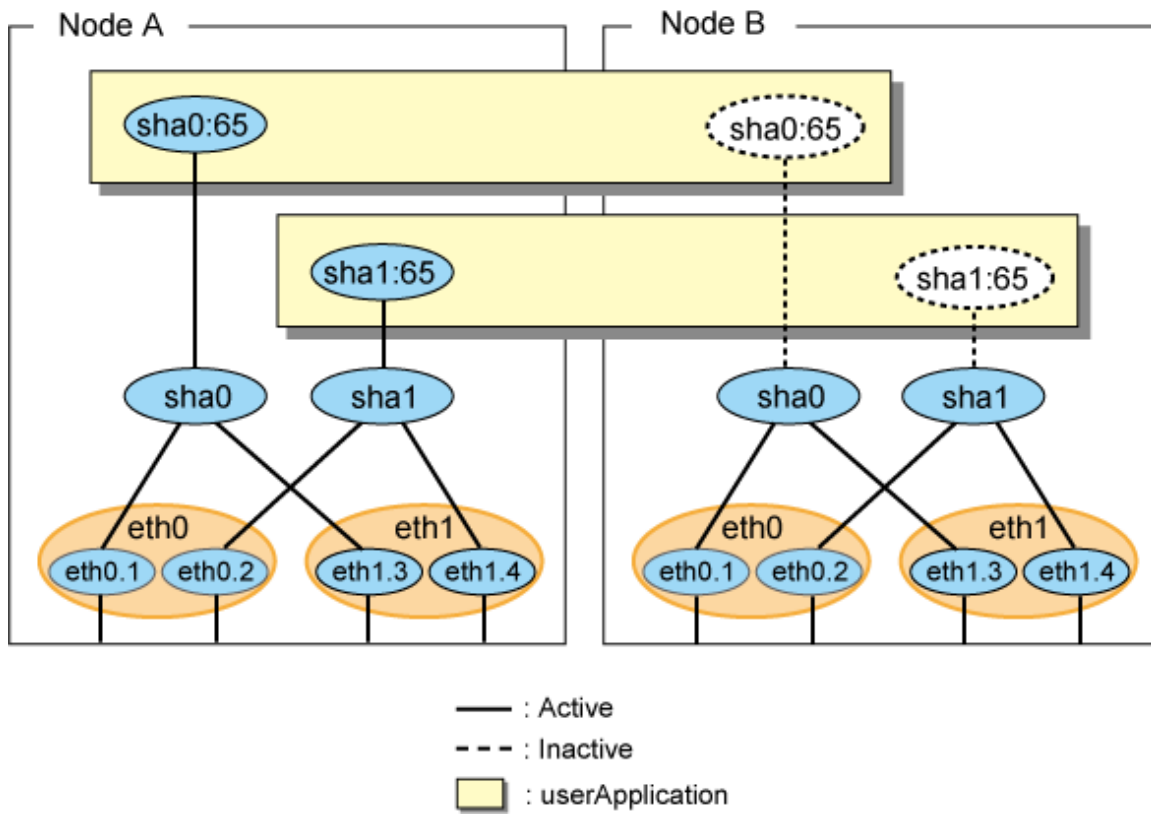
## 5.5 Tagged VLAN interface multiplexing on cluster system

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).

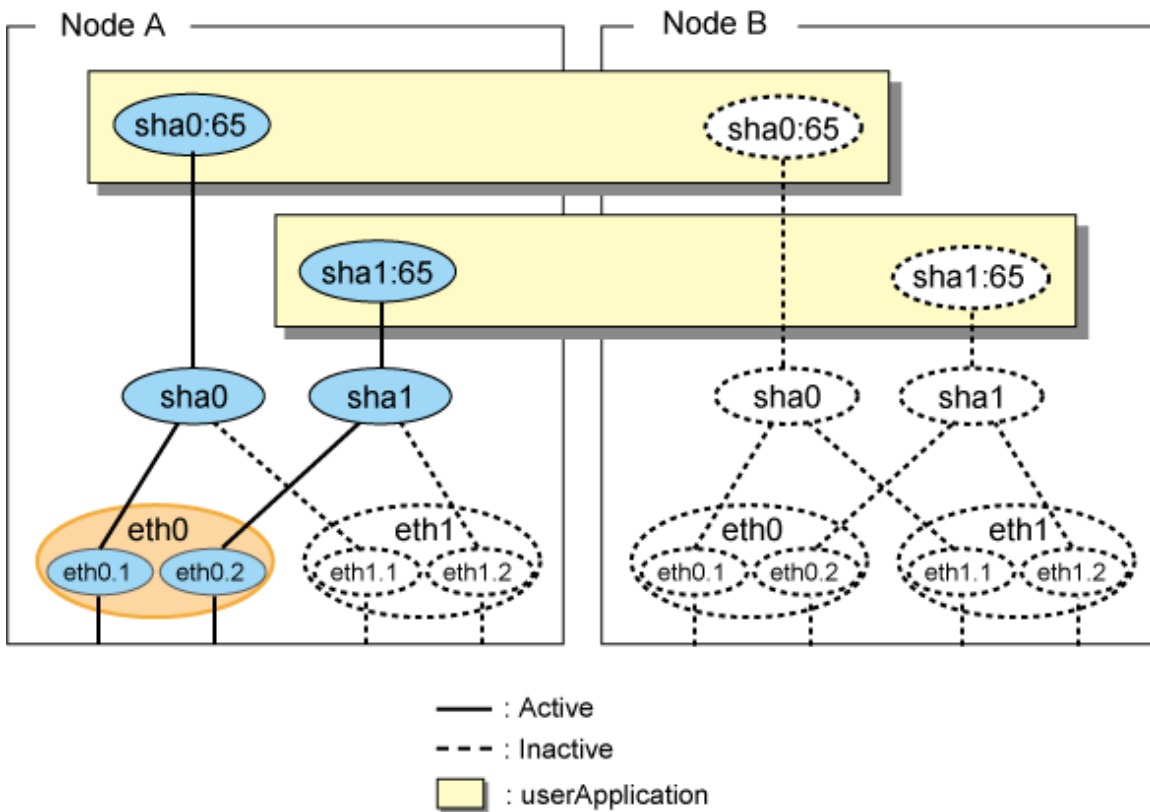
Figure 5.44 Tagged VLAN interface multiplexing on Fast switching mode (Active standby)



### 5.5.2 Active standby (NIC switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Active standby).

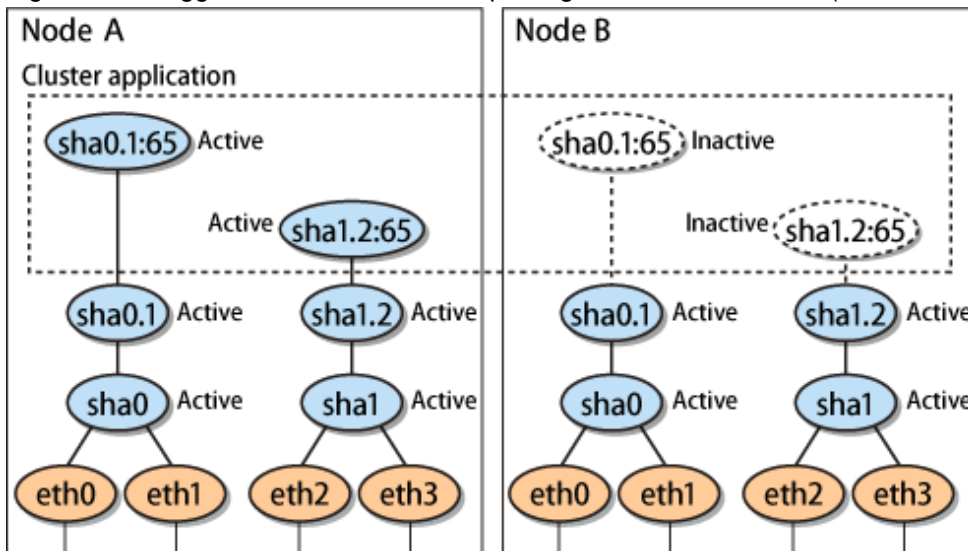
Figure 5.45 Tagged VLAN interface multiplexing on NIC switching mode (Active standby)



### 5.5.3 Active Standby (Virtual NIC mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Active standby).

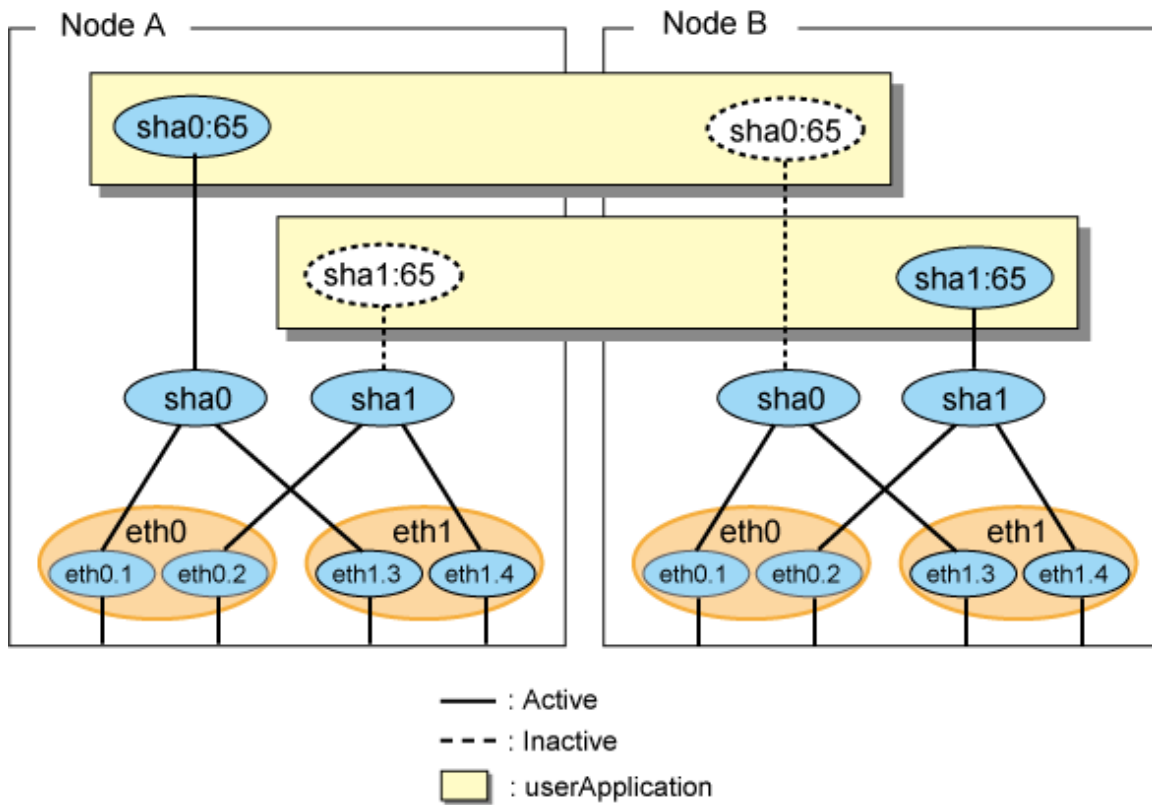
Figure 5.46 Tagged VLAN interface multiplexing on Virtual NIC mode (Active standby)



### 5.5.4 Mutual Standby (Fast switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

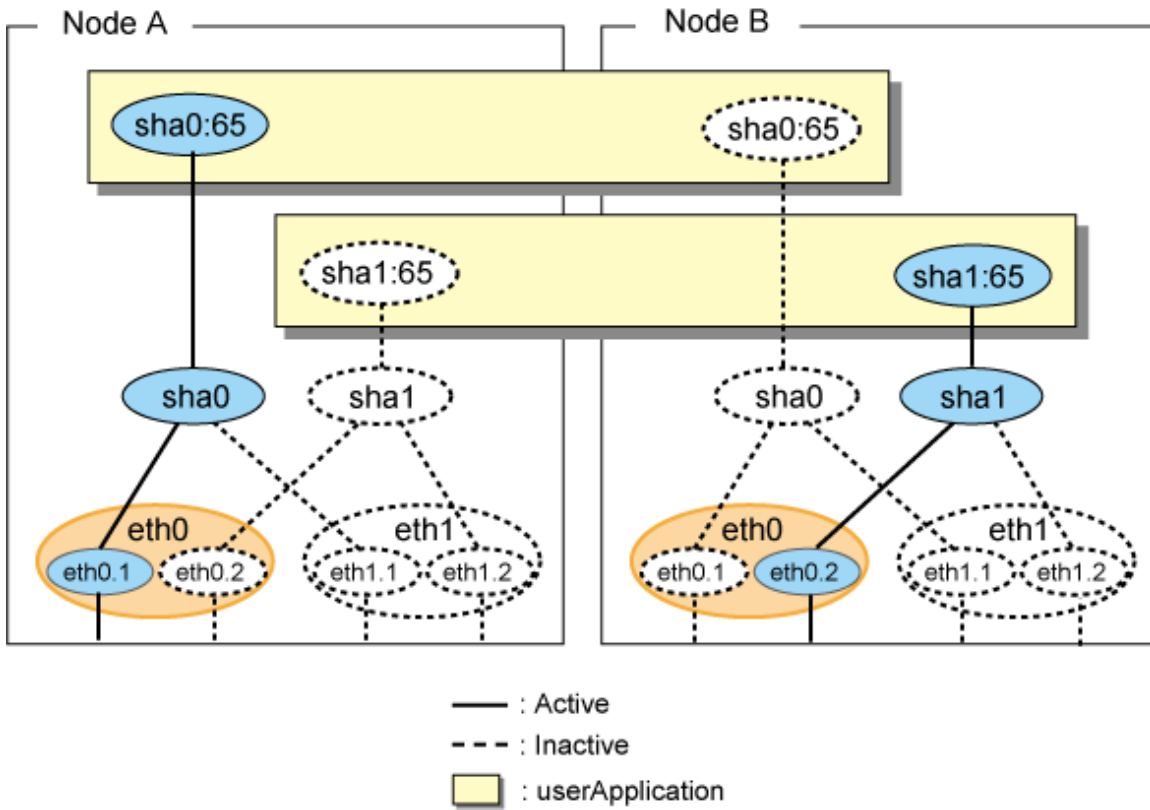
Figure 5.47 Tagged VLAN interface multiplexing on Fast switching mode (Mutual Standby)



### 5.5.5 Mutual Standby (NIC switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

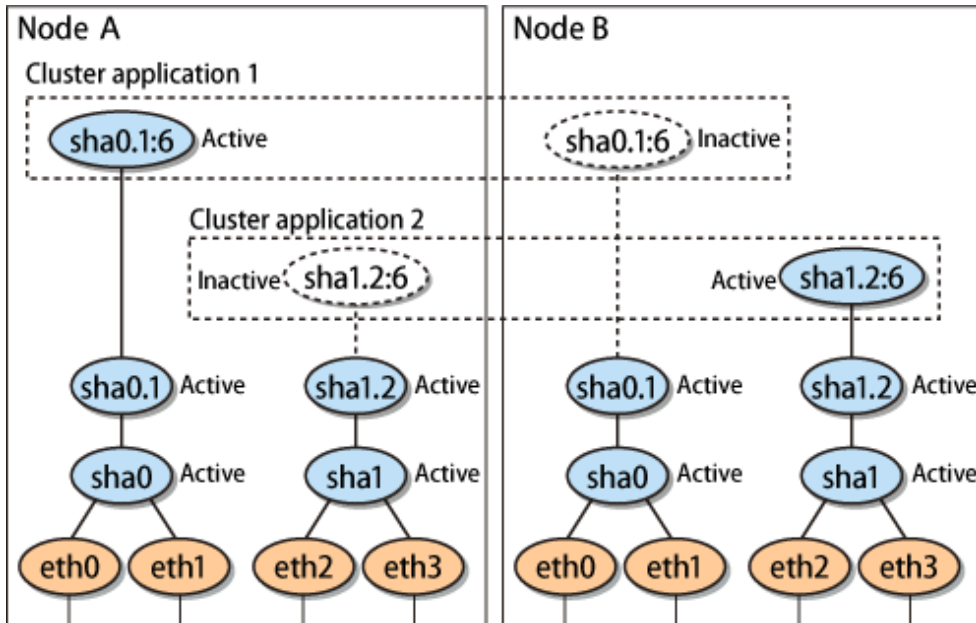
Figure 5.48 Tagged VLAN interface multiplexing on NIC switching mode (Mutual Standby)



### 5.5.6 Mutual Standby (Virtual NIC mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Mutual standby).

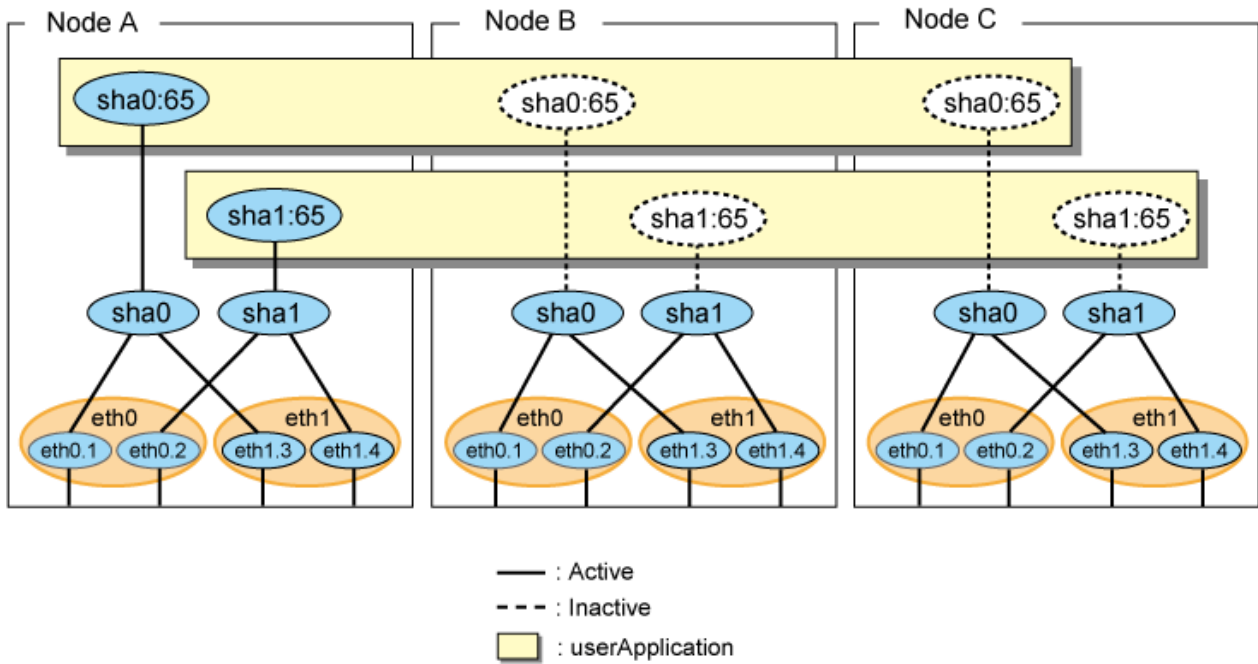
Figure 5.49 Tagged VLAN interface multiplexing on Virtual NIC mode (Mutual Standby)



### 5.5.7 Cascade (Fast switching mode)

The figure below illustrates tagged VLAN interface multiplexing on a cluster system (Cascade).

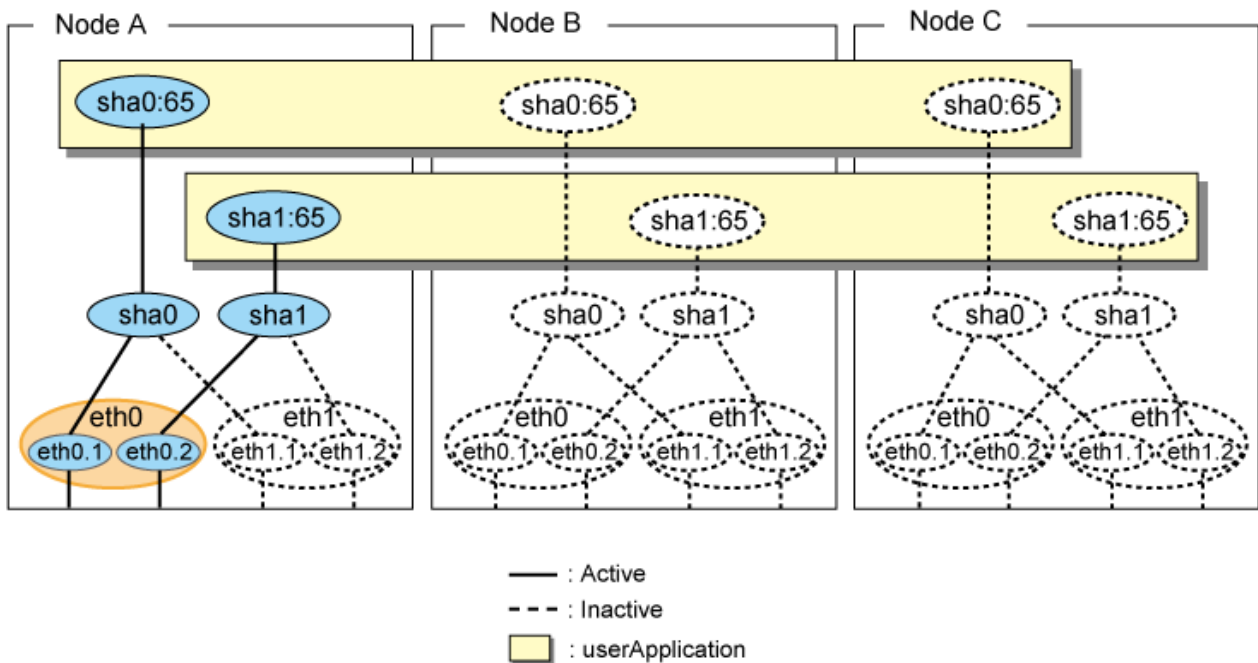
Figure 5.50 Tagged VLAN interface multiplexing on Fast switching mode (Cascade)



### 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)

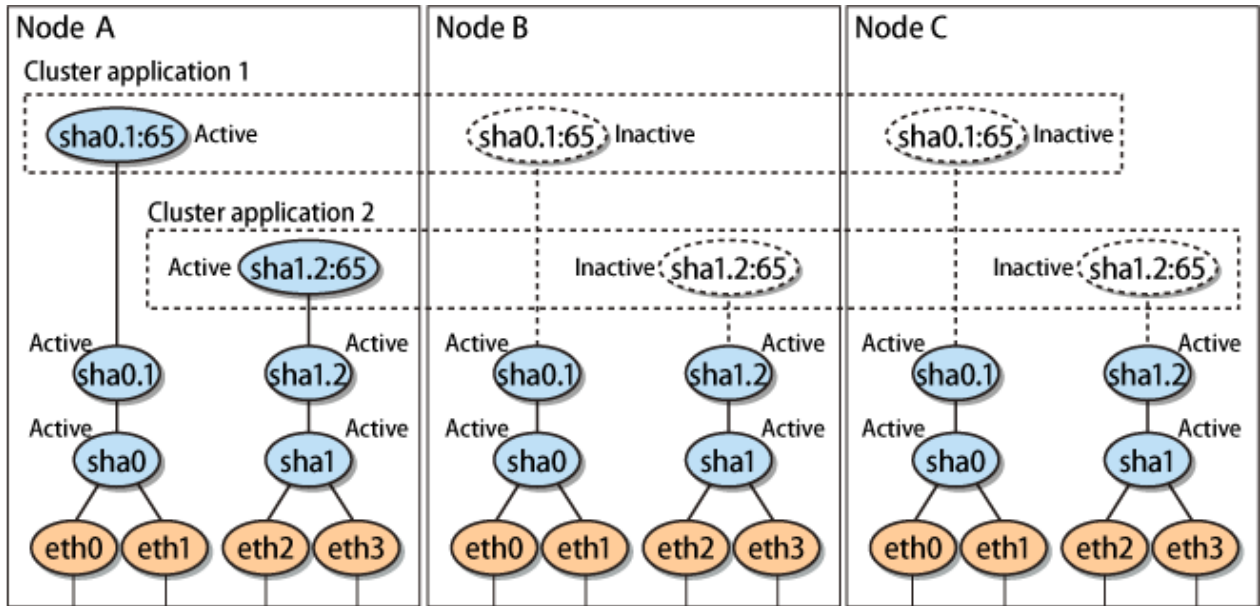


### 5.5.9 Cascade (Virtual NIC mode)

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 the investigation material of a Redundant Line Control Function all together, see "[6.1.1 Command to collect materials](#)" or "[6.1.2 Collecting Information by FJQSS \(Information Collection Tool\)](#)."

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)
- The investigation material 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 command) for the NIC that the Redundant Line Control function uses, which should be collected when a failure occurs.

In addition, confirm that GLS and network devices are set correctly, referencing "[Appendix H Troubleshooting](#)".

### 6.1.1 Command to collect materials

#### [Form]

```
/opt/FJSVhanet/usr/sbin/hanet_snap [-s] [save-directory]
```

#### [Detail of the function]

This command collects the investigation material 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 investigation material.

When omitted this option, all the investigation material is 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. If the target command or the file does not exist in the system, the execution result of the command or the file is not collected.

[Meaning] Y: Collected N: Not collected

Type	File name when collected	Collected information	Minimum investigation on material
System information: OSInfo/	arp_n	arp -n	Y
	arpables_list	arpables --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/arpables /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/bridge_info	bridge fdb show bridge link show bridge mdb show bridge vlan show ip -d link show master <bridge_name> * <bridge_name>: bridge name	Y
	etc/class_net	ls -l /sys/class/net	Y
etc/class_net_dev	/sys/class/net/*/carrier /sys/class/net/*/features	Y	

Type	File name when collected	Collected information	Minimum investigation on material
		/sys/class/net/*/flags /sys/class/net/*/iflink /sys/class/net/*/type	
	etc/firewalld/firewall_cmd_info	firewall-cmd --state firewall-cmd --list-all-zones firewall-cmd --list-lockdown-whitelist-commands firewall-cmd --list-lockdown-whitelist-contexts firewall-cmd --list-lockdown-whitelist-uids firewall-cmd --list-lockdown-whitelist-users	Y
	etc/firewalld/firewalld.conf	/etc/firewalld/firewalld.conf	Y
	etc/firewalld/icmptypes/	/etc/firewalld/icmptypes/*.xml	Y
	etc/firewalld/services/	/etc/firewalld/services/*.xml	Y
	etc/firewalld/zones/	/etc/firewalld/zones/*.xml	Y
	etc/frr	/etc/frr/*	Y
	etc/fstab	/etc/fstab	Y
	etc/rc_list	ls /etc/rc.d/*	Y
	etc/routel	routel	Y
	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	N
	etc/sysctl.d/	/etc/sysctl.d/*	Y
	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
	etc/NetworkManager/nmcli_info	/usr/bin/nmcli c /usr/bin/nmcli d /usr/bin/nmcli g /usr/bin/nmcli n	Y
	etc/NetworkManager/nmcli_devices_details	nmcli d show	Y
	etc/NetworkManager/nmcli_connections_details/<connection_name>	nmcli c show <connection_name> * <connection_name>: connection profile name	Y
	ethdev_info	ethtool ethX	Y

Type	File name when collected	Collected information	Minimum investigation on material
	free	free -bt	Y
	iANS/	/etc/ians ianscfg -s	Y
	ifconfig_a	ifconfig -a	Y
	ifstat_ae	ifstat -ae	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 ip mrule ip netns list ip tcp_metrics ip tuntap ip -f inet6 route ip -s link	Y
	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
	log/journal_log	journalctl --all --full	N
	lsmod	lsmod	Y
	lspci	lspci	Y
	netstat	netstat -na netstat -ni netstat -np netstat -nr	Y

Type	File name when collected	Collected information	Minimum investigation on material
		netstat -na -A inet6 netstat -nr -A inet6 netstat -ng netstat -ns	
	nft_list_ruleset	nft list ruleset	Y
	nftables.conf	/etc/sysconfig/nftables.conf	Y
	nstat_az	nstat -az	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
	ss	ss -f inet6 -na ss -na ss -np	Y
	sysconfig/	/etc/sysconfig/hwconf /etc/sysconfig/network /etc/sysconfig/netdump /etc/sysconfig/ntpd /etc/sysconfig/static-routes /etc/sysconfig/network-scripts/	Y
	sysconfig/chronyd	/etc/sysconfig/chronyd	Y
	sysctl_a	sysctl -a	N
	systemd/systemctl_list	systemctl list-dependencies --full systemctl list-units --all --full systemctl list-unit-files --all --full	N
	systemd/systemctl_fjsvhanet_info	systemctl show fjsvhanet.service --all --full systemctl status fjsvhanet.service --full	Y
	systemd/systemd_analyze_plot.svg	systemd-analyze plot	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
	usr/lib/sysctl.d/	/usr/lib/sysctl.d/*	Y

Type	File name when collected	Collected information	Minimum investigation on material
GLS information: hanetInfo/	config/	/etc/opt/FJSVhanet/config/	Y
	dev_sha	ls -l /dev/sha	Y
	dsp_conf	dsphanet dsphanet -o dsphanet -v dspathmon dspobserv dspobserv -ddd dspoll	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-drv rpm -qi kmod-FJSVhanet-drv-xen rpm -qi kmod-FJSVhanet-drv-PAE	Y
script/	/etc/opt/FJSVhanet/script/	Y	
Cluster system information: RCInfo/	hvdisp_a	hvdisp -a	N
	log/	/var/opt/reliant/log/	N

[Meaning of the symbols] Y: It extracts. N: It does not extract.

(\*) /proc/net/rpc cannot be obtained.

### [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 the investigation material under /tmp.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap
```

- When collecting the minimum investigation material under /tmp.

```
# /opt/FJSVhanet/usr/sbin/hanet_snap -s
```

- When collecting the minimum investigation material under /home/user1.

```
# /opt/FJSSVhanet/usr/sbin/hanet_snap -s /home/user1
```

## 6.1.2 Collecting Information by FJQSS (Information Collection Tool)

[Detail of the function]

By using FJQSS (Information Collection Tool), collect the investigation material required to maintain the Redundant Line Control Function.

The collected material includes all the investigation materials in the list of the collected information in "6.1.1 Command to collect materials."

[Using example]

1. Execute the following command.

```
# /opt/FJSSVqstl/fjqss_collect
```

2. The product selection menu appears. Input the number of the product of which you want to collect the investigation material ("PRIMECLUSTER GL"), then input "[Enter]".  
For the cluster system, if the number of the cluster product (PRIMECLUSTER HA Server, for example) is specified, the investigation material of PRIMECLUSTER including GLS can be collected at once.
3. Press the [Y] key according to the instruction in the prompt.
4. After the FJQSS has completed the collection, the name of the output directory of the collected investigation material appears. Verify that the investigation material has been collected in the directory.
5. Send the created file to field engineers.

[Output form]

The following file is created in the output directory of the collected material.

resultYYYYMMDDHHMMSS.tar.gz

(YYYYMMDDHHMMSS: time (year, month, day, hour, minute, and second) that the collection started)



### Information

About FJQSS (Information Collection Tool) and its usage

You can collect the information necessary for the trouble investigation with FJQSS (Information Collection Tool). See the FJQSS User's Guide bundled to the installation medium of the product.

When you see the FJQSS User's Guide, open the following file in the installation medium of the product by the browser.

documents/fjqss-manual\_sollnx/index\_en.html

## 6.1.3 Collecting 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    192.168.10.10 eth2,eth3
sha12     -             p           sha1
sha2      192.168.100.110 c           eth4,eth5
```



2. Execute the tcpdump command to collect packet traces.

If a virtual interface bundles several physical interfaces, execute the tcpdump command for all physical interfaces in the bundle.

Execution examples are shown below:

- For Fast switching mode (sha0)

```
# tcpdump -p -i eth0 -w /tmp/packet_trace.eth0
# tcpdump -p -i eth1 -w /tmp/packet_trace.eth1
# tcpdump -p -i sha0 -w /tmp/packet_trace.sha0
```

- For NIC switching mode (sha1 and sha12)

```
# tcpdump -p -i eth2 -w /tmp/packet_trace.eth2
# tcpdump -p -i eth3 -w /tmp/packet_trace.eth3
```

- For GS linkage mode (sha2)

```
# tcpdump -p -i eth4 -w /tmp/packet_trace.eth4
# tcpdump -p -i eth5 -w /tmp/packet_trace.eth5
# tcpdump -p -i sha2 -w /tmp/packet_trace.sha2
```

- For Virtual NIC mode (sha3)

```
# tcpdump -p -i eth6 -w /tmp/packet_trace.eth6
# tcpdump -p -i eth7 -w /tmp/packet_trace.eth7
# tcpdump -p -i sha3 -w /tmp/packet_trace.sha3
```

### Information

For the tcpdump command, refer to the Linux manual.

### Note

When executing the tcpdump command, specify the -p option to collect packet traces in non-promiscuous mode.

## 6.2 HUB maintenance

This section describes the procedures for swapping or restarting HUBs of the monitoring destination of GLS in the following four patterns.

- When HUBs are swapped or restarted in the Fast switching mode/the GS linkage mode
- When the monitoring destination IP address is changed by swapping HUBs in the NIC switching mode/the Virtual NIC mode
- When the monitoring destination IP address is not changed by swapping HUBs in the NIC switching mode/the Virtual NIC mode
- When HUBs are restarted in the NIC switching mode/the Virtual NIC mode

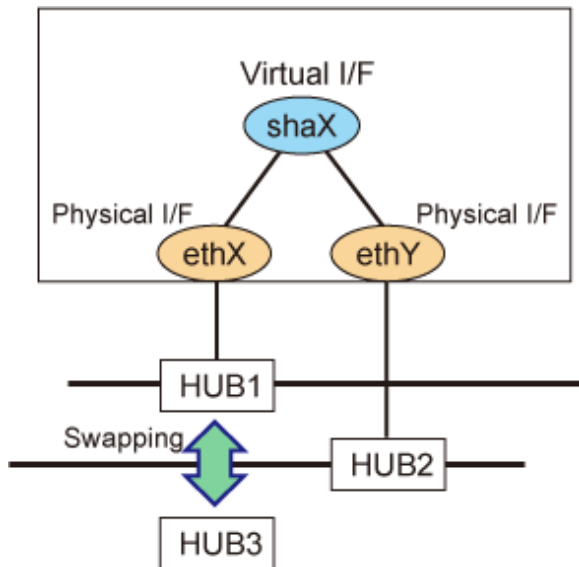
### Note

If HUBs are to be maintained during operation, perform the operation, such as preparing a procedure manual, in a planned manner not to unintentionally cut off communication for operation or stop cluster applications.

## 6.2.1 Swapping or Restarting HUB procedure (Fast switching mode / GS linkage mode)

---

The following describes the procedure for swapping or restarting HUBs in the Fast switching mode and the GS linkage mode.



1. Disconnect the route of the HUB to be swapped or restarted.

```
# /opt/FJSSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

2. Swap or restart the HUB
3. Make sure that HUB3 is working correctly.

Execute a command such as the ip command to check the link up status of the physical interface (ethX). If the link up is completed, "LOWER\_UP" is displayed when using the ip command.

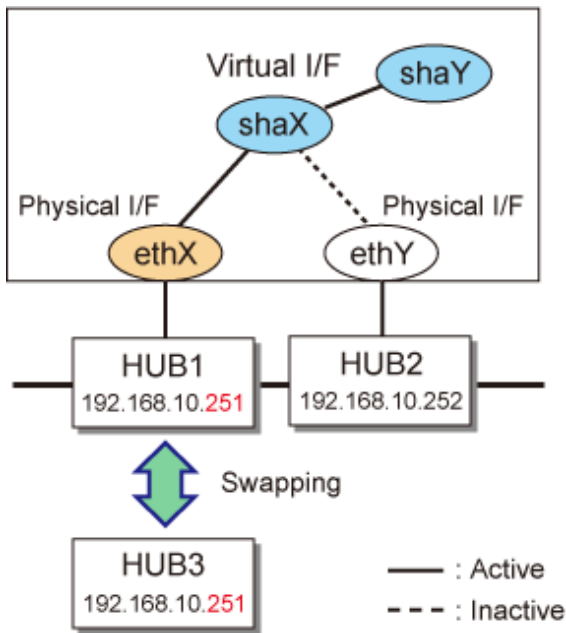
4. Reconnect the route of the HUB that was swapped or restarted.

```
# /opt/FJSSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

## 6.2.2 Swapping or Restarting HUB procedure (NIC switching mode / IP address remains unchanged)

---

The following shows the procedure in which the IP address remains unchanged even after swapping or restarting HUBs.



1. To maintain communications, switch the NIC so that the HUB to be swapped or restarted 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 or restart the HUB.

5. To make sure that HUB3 is working 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.

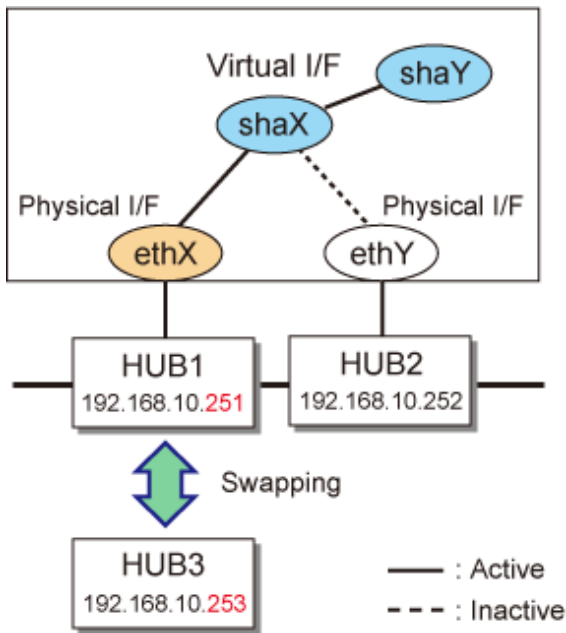
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8. Start standby patrol monitoring.

```
# /opt/FJSVhanet/usr/sbin/strctl -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. 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 standby patrol monitoring.

```
# /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. See the manual that comes with the HUB for how to set an IP address for a HUB.

5. To make sure that HUB3 is working correctly, check whether you can ping HUB3 successfully. If there is no response, check the connections of the HUB itself and other devices.

```
# ping 192.168.10.253
```

6. 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
```

7. Start HUB monitoring or HUB-to-HUB monitoring.

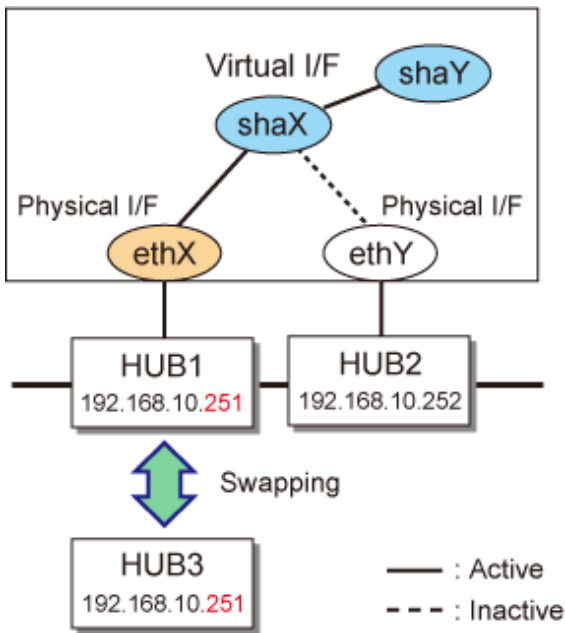
```
# /opt/FJSVhanet/usr/sbin/hanetpoll on
```

8. Start standby patrol monitoring.

```
# /opt/FJSVhanet/usr/sbin/strctl -n shaY
```

## 6.2.4 Swapping or Restarting HUB procedure (Virtual NIC mode / IP address remains unchanged)

The following shows the procedure in which the IP address remains unchanged even after swapping or restarting 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 or restart the HUB.

4. To make sure that HUB3 is working 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.

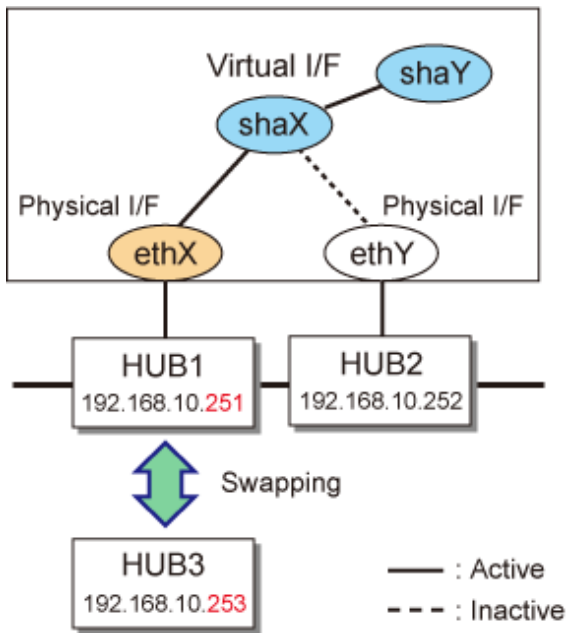
```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

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 HUB3 is working correctly, check whether you can ping HUB3 successfully. If there is no response, check the connections of the HUB itself and other devices.

```
# ping 192.168.10.253
```

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

This section describes NIC maintenance procedures. The following two types of procedures are available depending on the system state. Note that the hot 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.

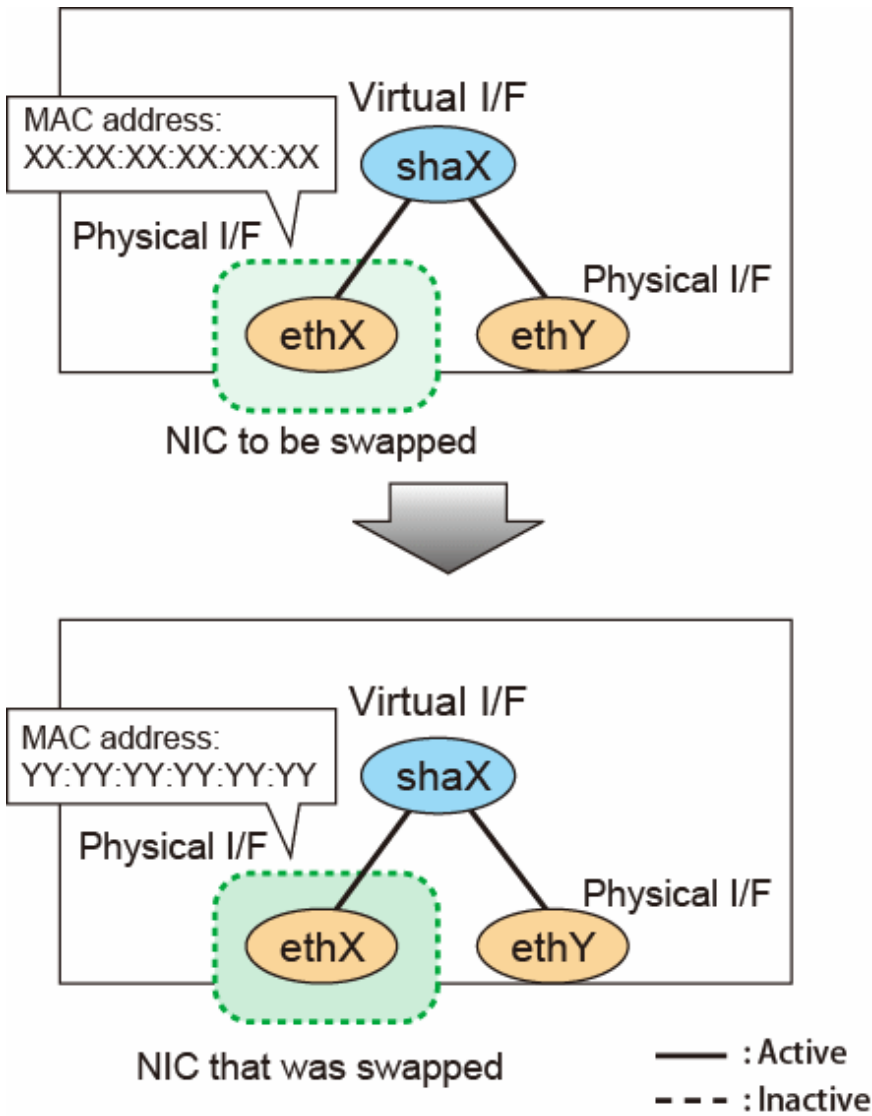
- Swapping NICs after stopping the system (shutdown maintenance)
- Swapping NICs while the system is in operation (hot maintenance)

The format of the name given to NIC varies depending on where the NIC is mounted. Here, ethX is used as the format. Replace it with the actual NIC name as necessary.

### 6.3.1 Shutdown maintenance for a NIC

The following describes the procedure for swapping a NIC after stopping the system. If the interface names are switched before and after swapping NIC, the operating system network configuration file must be modified.

When swapping multiple NICs, replace them one at a time without replacing them at once. Perform the swapping procedure for each swapped NIC.



1. Collect the interface name of NIC.

Collect the interface name from /sys/class/net directory.

```
# cd /sys/class/net
# ls
eth0 eth1 lo
```

2. Check the correspondence between NICs and MAC addresses.

Check the MAC address for all the interface name collected in step 1.

```
# cat eth0/address
<MAC_address>
```

3. Check the correspondence between NICs and bus addresses.

Check the bus address of NIC for all the interface name collected in step 1.

```
# ls -l eth0/device
lrwxrwxrwx 1 root root 0 Apr 9 09:17 eth0/device -> ../../../../0000:01:06.0
```

The bus address is the file name (directory) of the lowest layer of the symbolic link destination file displayed in the output command result.

The bus address is the address information for identifying the device configuring the following information.

```
[<segment_number>:]<bus_number>:<slot_number>.<function_number>
```

The segment number is not displayed depending on the model, because it is used as a part of bus number.

4. Create a hardware address description of NIC from the information collected in steps 1 to 3.

Table 6.1 Hardware address description of NIC (Example)

Interface name	MAC address	Bus address
eth0	<MAC_address>	<bus_number>:<slot_number>.<function_number>
...	...	...

5. Shut down the system.

```
# shutdown -h now
```

6. Swap NIC.

### Information

In the following procedure, edit the interface configuration file to deal with the swapping of interface name. If "HWADDR" is not stated in the interface configuration file of NIC before swapping, the following procedures are not necessary. Start the system and modify the MAC address of the hardware address description of NIC created in step 4.

7. Boot the system in rescue mode.
8. Modify the operating system network configuration file.

8-1. Collect the interface name from the /sys/class/net directory.

```
# cd /sys/class/net
# ls
eth2 eth3 lo
```

If the collected interface name is not in the hardware address description of the NIC created in step 4, a new name will be attached to the swapped NIC. Continue the following procedure.

8-2. Check the MAC address and bus address that corresponds to the interface name that did not exist in the system before NIC swapping.

```
## cat eth2/address
<MAC_address>
```



```
# ls -l eth2/device
lrwxrwxrwx 1 root root 0 Apr 9 09:17 eth2/device -> ../../../../0000:01:06.0
```

8-3. When comparing the checked bus address with the bus address string of the hardware address description of NIC created in step 4, the line of the corresponding interface can be seen. Set the checked MAC address in "HWADDR" of the configuration file corresponding to this interface.

### Note

For multiple NIC ports, all ports of the interface configuration file must be edited.

Repeat step 8.

9. Reboot the system.

```
# shutdown -r now
```

10. Modify the hardware address description of NIC.

Modify the MAC address of the hardware address description of NIC created in step 4.

## 6.3.2 Hot maintenance of NIC

This section describes the PCI Hot Plug for redundant NIC by Redundant line control function.

The target devices for PCI Hot Plug provided by PRIMEQUEST are as follows. The procedures vary depending on the target to be swapped:

- SB
- IOU
- PCI Express card

For details, see the following manual:

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

### Note

- Make sure to check the procedure for the PCI Hot Plug in the latest manual before performing the hot maintenance for NIC.
- For information about replacing the NIC used for the cluster interconnect, refer to "PRIMECLUSTER Installation and Administration Guide."

The following table shows the compatibility of PCI Hot Plug for the redundant line control function.

Table 6.2 Compatibility of PCI Hot Plug for redundant line control function

Mode	System configuration	PCI Hot Plug		
		Add	Remove	Swap
Fast switching mode	Single	A	A	A
	Cluster	B (*1)	B (*2)	A
NIC switching mode	Single	A	A	A
	Cluster	B (*1)	B (*2)	A
Virtual NIC mode	Single	A	A	A
	Cluster	B (*1)	B (*2)	A

Mode	System configuration	PCI Hot Plug		
		Add	Remove	Swap
GS linkage mode	Single	N	N	A
	Cluster	N	N	A

[Meaning of the alphabets]

A: The hot maintenance is enabled when GLS is running.

B: The hot maintenance is enabled after GLS is stopped.

N: Not supported.

\*1) The procedure to add the PCI Hot Plug in the cluster configuration

1. Add NIC.

For details, see the following manuals.

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

2. Add the configuration for virtual interfaces.

For details, see "[5.2.1 Adding configuration](#)".

\*2) The procedure to delete PCI Hot Plug in the cluster configuration

1. Delete virtual interfaces.

For details, see "[5.2.3 Deleting configuration](#)".

2. Delete NIC.

For details, see the following manuals.

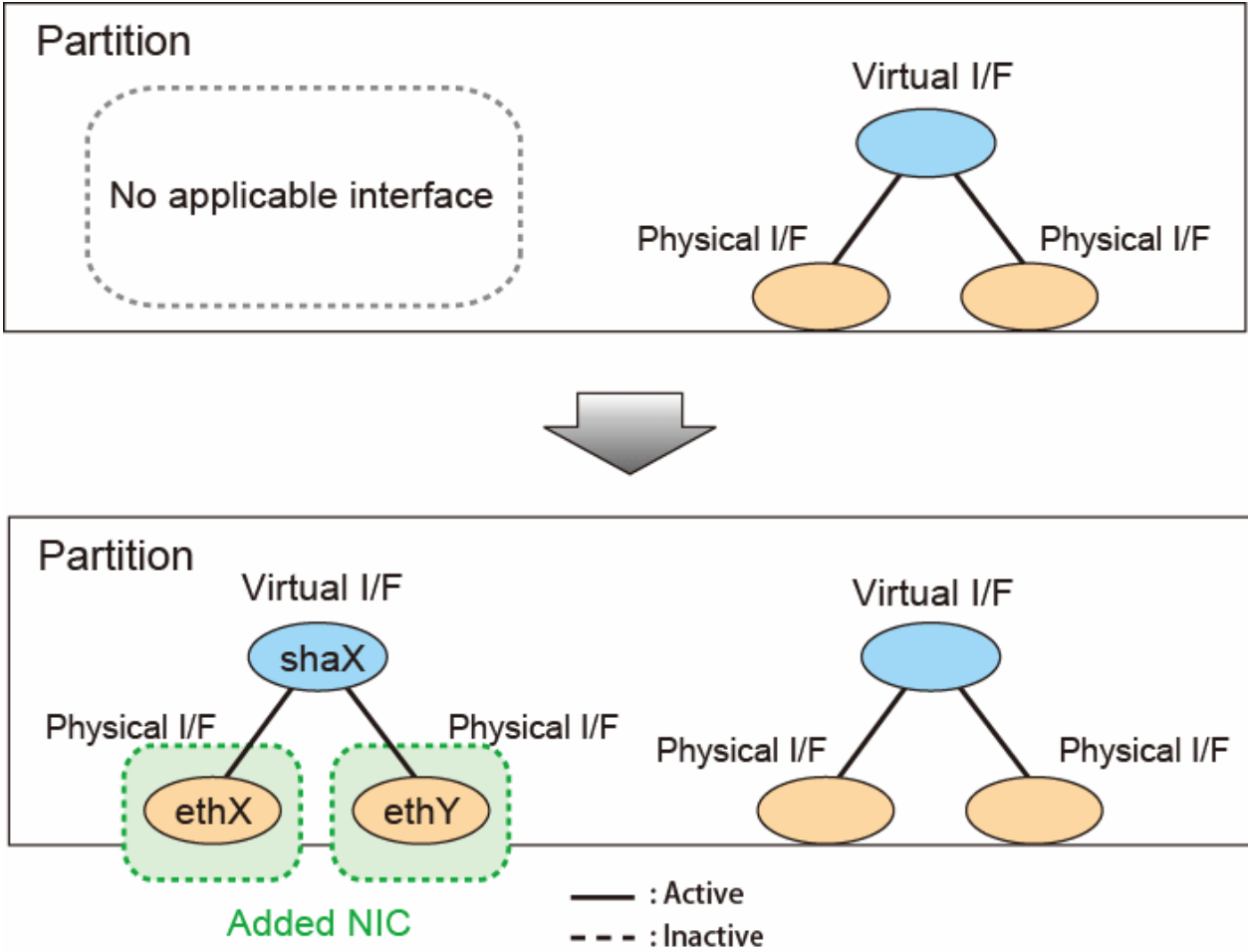
- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

### 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



1. Adding NIC

Add NIC. For procedures, see the following manuals:

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

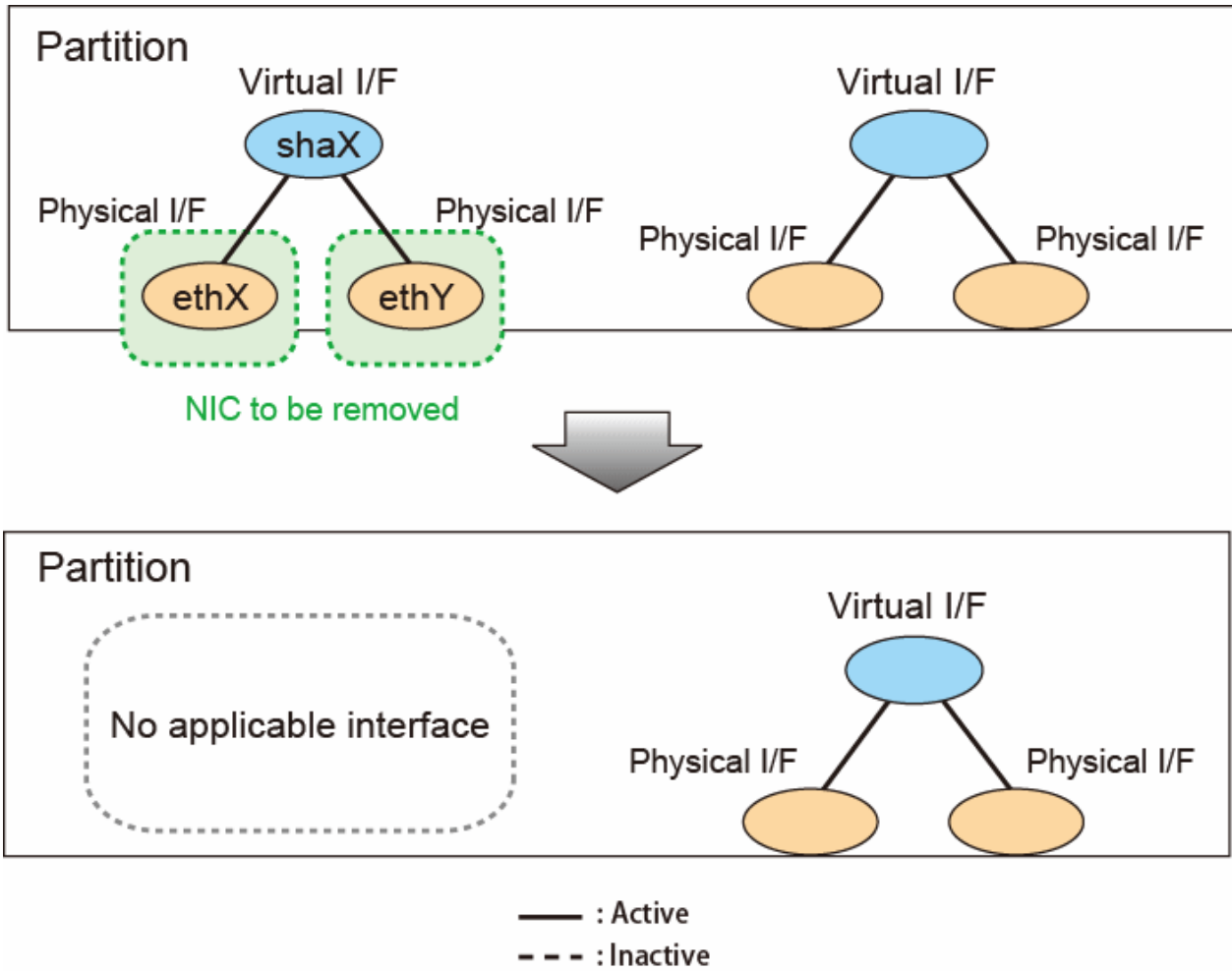
2. Creating virtual interface

Refer to "3.3 Additional system setup" and create a virtual interface to duplicate the added NIC.

### 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)



1. Preparation for removing NIC

See "[3.5 Deleting configuration information](#)" to remove the virtual interface that uses the NIC to be removed.

2. Removing NIC

Remove NIC. For the procedures, see the following manuals:

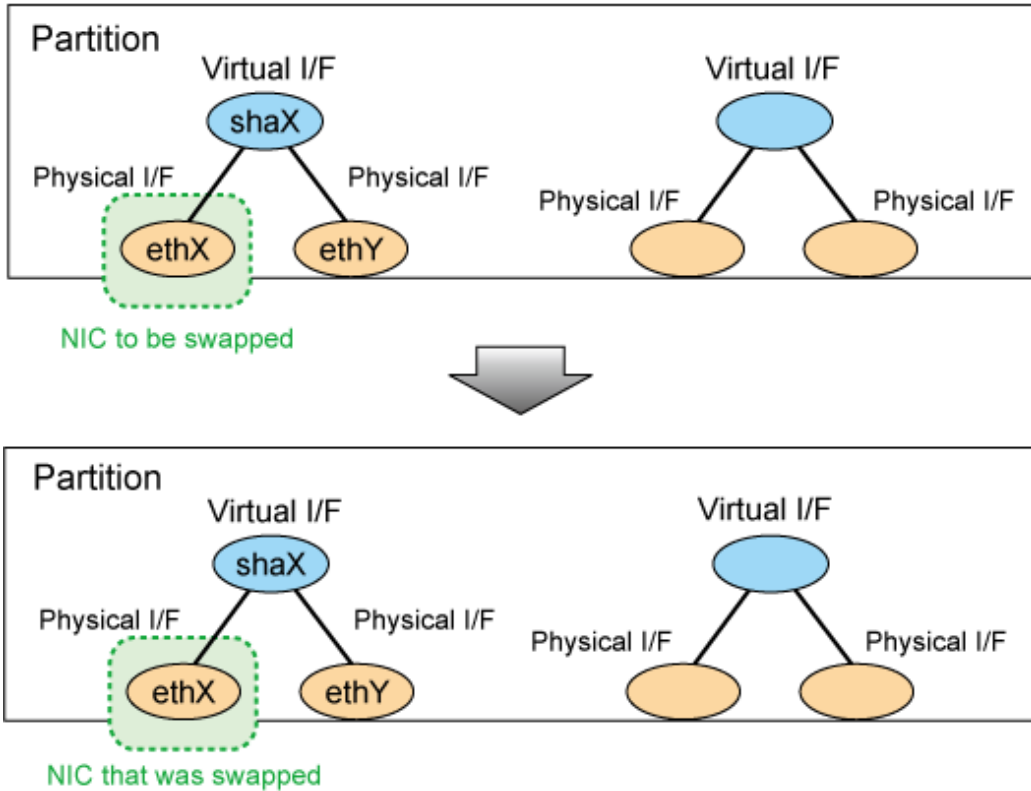
- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

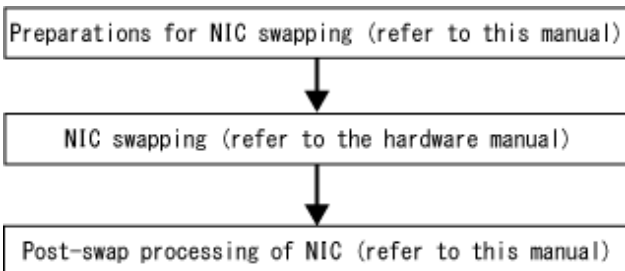
### 6.3.2.3 Swapping procedure

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)



Perform the operation in the following:



Detailed procedures for each redundant line switching mode are shown below.

Replace the virtual interface name (shaX) and physical interface name (ethX, ethY) described in this procedure with the interface suitable for your environment.

### For Fast switching mode

#### 1. Preparations for NIC swapping

1-1. From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped (The interface name of the target NIC is ethX).

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

1-2. Enter the dsphanet command to confirm that the device status of the target NIC (interface name: ethX) is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
-----+-----+-----+-----+-----+
shaX      Active  t    OFF  ethX(CUT),ethY(ON)
```

## 2. NIC swapping

Perform NIC swapping. For details, see the manuals below.

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

## 3. Post-swap processing of NIC

3-1. Restore the NIC (interface name: ethX) that was temporarily deleted in step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

3-2. Enter the dsphanet command to confirm that the device status of the swapped NIC (interface name: ethX) 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. Preparations for NIC swapping

1-1. Stop HUB monitoring.

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

1-2. Stop standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/stpctl -n shaY
```

1-3. Enter the dsphanet command to check the status of the NIC (Interface name: ethX) to be swapped. The NIC must be in a different state from that of an active NIC (the NIC must be in the "OFF" or "STOP" state). If the NIC is active, follow step 1-4 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)
```

1-4. 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)
```

1-5. Stop interface status monitoring.

```
# /bin/touch /var/opt/FJSVhanet/tmp/disable_watchif
```

## 2. NIC swapping

Perform NIC swapping. For details, see the manuals below.

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

## 3. Post-swap processing of NIC

3-1. Perform the following operations

[For RHEL8]

Change HWADDR of the interface setting file (ifcfg-ethX) of the swapped NIC to the MAC address of the swapped NIC (when HWADDR is described in the file).

ifcfg-ethX (swapped NIC)

```
HWADDR=XX:XX:XX:XX:XX:XX
...
...
```

[For RHEL9]

Set the MAC address of the NIC after the replacement to 802-3-ethernet.mac-address with the "nmcli connection modify" command.

```
# /usr/bin/nmcli connection modify "ethX" 802-3-ethernet.mac-address
"XX:XX:XX:XX:XX:XX"
```

3-2. Set the state of the swapped NIC to that of a standby NIC of GLS.

Make sure that an IPv4 address is not assigned, the UP flag exists, and the setting of the kernel parameter is reflected.

```
# sysctl -w net.ipv4.conf.ethX.arp_filter=1
# /usr/sbin/ip link set dev ethX up
# /usr/sbin/ip addr show ethX
N: ethX: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether XX:XX:XX:XX:XX:XX brd ff:ff:ff:ff:ff:ff
    inet6 fe80::XXXXXXXXXXXXXXXX/64 scope link
    valid_lft forever preferred_lft forever
# sysctl -n net.ipv4.conf.ethX.arp_filter
1
```

3-3. If necessary, fail-back the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX
```

3-4. Start standby patrol monitoring. If the standby patrol function is not used, skip this step.

```
# /opt/FJSVhanet/usr/sbin/strptl -n shaY
```

3-5. Restart HUB monitoring.

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

3-6. Restart interface status monitoring.

```
# /bin/rm /var/opt/FJSVhanet/tmp/disable_watchif
```

## For Virtual NIC mode

### 1. Preparations for NIC swapping

#### 1-1. Stop network monitoring.

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

1-2. From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped (The interface name of the target NIC is ethX).

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```

1-3. Enter the dsphanet command to confirm that the device status of the target NIC (interface name: ethX) is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status   Mode CL  Device
+-----+-----+-----+-----+
shaX      Active   v    OFF  ethX(CUT),ethY(ON)
```

### 2. NIC swapping

Perform NIC swapping. For details, see the manuals below.

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

### 3. Post-swap processing of NIC

3-1. Restore the NIC (interface name: ethX) that was temporarily deleted in step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

3-2. Enter the dsphanet command to confirm that the device status of the swapped NIC (interface name: ethX) is "OFF".

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

3-3. If necessary, fail-back the NIC.

```
# /opt/FJSVhanet/usr/sbin/hanetnic change -n shaX -i ethX
```

3-4. Restart network monitoring.

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

## For GS linkage mode

### 1. Preparations for NIC swapping

1-1. From the virtual interface definition, temporarily delete the definition information about the NIC to be swapped (The interface name of the target NIC is ethX).

```
# /opt/FJSVhanet/usr/sbin/hanetnic delete -n shaX -i ethX
```



1-2. Enter the dsphanet command to confirm that the device status of the target NIC (interface name: ethX) is "CUT".

```
# /opt/FJSVhanet/usr/sbin/dsphanet
[IPv4,Patrol / Virtual NIC]
Name      Status  Mode CL  Device
+-----+-----+----+----+-----+
shaX      Active  c    OFF  ethX(CUT),ethY(ON)
```

2. NIC swapping

Perform NIC swapping. For details, see the manuals below.

- PRIMEQUEST 3000 Series

"Hot Maintenance in Red Hat Enterprise Linux 7 or later" in "PRIMEQUEST 3000 Series Administration Manual"

3. Post-swap processing of NIC

3-1. Restore the NIC (interface name: ethX) that was temporarily deleted in step 1.

```
# /opt/FJSVhanet/usr/sbin/hanetnic add -n shaX -i ethX
```

3-2. Enter the dsphanet command to confirm that the device status of the swapped NIC (interface name: ethX) 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

### Note

This version does not support IPv6 addresses for the NIC Switching mode and Fast Switching mode.

When using the NIC Switching mode or Fast Switching mode, it is not possible to execute commands or specify parameters related to IPv6 addresses.

### [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 interface1[,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 interface1[,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 interface1[,interface2]
NIC switching mode (Physical IP address takeover function):
/opt/FJSVhanet/usr/sbin/hanetconfig create -n devicename -m e -i
ipaddress1 [-e ipaddress2] -t interface1[,interface2]
Standby patrol function (automatic fail-back if a failure occurs /
immediate automatic fail-back):
```

```

/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
interface1[,interface2] [-s SHAMACADDR]
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
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 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. The host name that can be specified is 16 characters or less.

**[/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.

**-s SHAMACADDR:**

Specify the method for assigning a MAC address to a virtual interface. This option is available on RHEL9.  
If you specify a MAC address for SHAMACADDR, the MAC address is assigned. The MAC address format you can specify is XX:XX:XX:XX:XX:XX. where XX is a 16 number separated by a colon (:).  
If you specify "auto", a MAC address is automatically assigned.  
If you specify "primary", the same MAC address as the primary NIC which it binds is assigned.  
If you omit this option, the configuration information is created with "primary" specified.

## (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/FJShanet/usr/sbin/hanetconfig copy [inet] -n devicename1,devicename2 -i ipaddress
```

[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,...]] [-s]
```

-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   192.168.10.10  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
```

-s

If you specify this option, the SHAMACADDR setting for the Virtual NIC mode is additionally displayed. This option is available on RHEL9.

The following shows an example of displaying configuration information with SHAMACADDR by using -s option.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig print -s
[IPv4,Patrol / Virtual NIC]
Name      Hostname      Mode Physical ipaddr  SHAMACADDR      Interface List
+-----+-----+-----+-----+-----+-----+
sha0      192.168.10.100 d   192.168.10.10  eth0,eth1
sha1      -              p   -              sha0
sha2      hostC          d   hostC1         eth2,eth3
sha3      -              p   -              sha2
sha4      -              v   -              00:0B:5D:9F:A0:22 eth6,eth7
sha5      -              v   -              primary          eth8
```

sha6	v	auto	eth9
[IPv6]			
Name	Hostname/prefix	Mode	Interface List
-----+	-----+	-----+	-----+
sha2	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
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.)
SHAMACADDR	The method for assigning a MAC address to a virtual interface (operation mode "v")
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/FJShanet/usr/sbin/hanetconfig modify [inet] -n devicename {[-i ipaddress1] [-t interface1[,interface2,...]]}
NIC switching mode (IPv4: Logical IP address takeover function):
/opt/FJShanet/usr/sbin/hanetconfig modify [inet] -n devicename {[-i ipaddress1] [-e ipaddress2] [-t interface1[,interface2]]}
NIC switching mode (Physical IP address takeover function):
/opt/FJShanet/usr/sbin/hanetconfig modify -n devicename {[-i ipaddress1] [-e ipaddress2] [-t interface1[,interface2]]}
Standby patrol function:
/opt/FJShanet/usr/sbin/hanetconfig modify -n devicename {[-t interface1]}
Virtual NIC Mode:
/opt/FJShanet/usr/sbin/hanetconfig modify -n devicename -s SHAMACADDR
GS linkage mode
/opt/FJShanet/usr/sbin/hanetconfig modify -n devicename {[-i ipaddress] [-t interface1[,interface2,...]]}
```

- When changing configuration information of a logical virtual interface

```
Fast switching mode (IPv4):
/opt/FJShanet/usr/sbin/hanetconfig modify [inet] -n devicename -i ipaddress
GS linkage mode
/opt/FJShanet/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").

-s SHAMACADDR:

Specify the method for assigning a MAC address to a virtual interface. This option is available on RHEL9.

If you specify a MAC address for SHAMACADDR, the MAC address is assigned. The MAC address format you can specify is XX:XX:XX:XX:XX:XX, where XX is a 16 number separated by a colon (:).

If you specify "auto", a MAC address is automatically assigned.

If you specify "primary", the same MAC address as the primary NIC which it binds is assigned.

## (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 2.20
```

## [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.
- 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](#)".
- If the network corresponding to the IPv4 address was specified by -i option or -e option of the create command, copy command, and the modify command and this network does not exist in the setting of hanetmask command, the default netmask is used according to the address class.

## [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 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 the setting when the virtual interface (sha0) bundles two physical interfaces (eth0 and eth1) in Virtual NIC mode, and how to set the MAC address for sha0 to 00:0B:5D:9F:A0:22.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1 -s 00:0B:5D:9F:A0:22
```

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
```

The following is an example of modifying the method for assigning a MAC address to the virtual interface (sha0) to automatic assignment.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -s auto
```

The following is an example of modifying the MAC address of the virtual interface (sha0) to be the same as the primary physical interface.

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -s primary
```

### (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
```

### (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 the strhanet command to activate a virtual interface. Do not use a command such as the ip command to perform the activation. Do not operate physical interfaces that the virtual interface bundles with a command such as the ip command while activating the 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 the sphanet command to deactivate a virtual interface. Do not use a command such as the ip command to perform the deactivation.
- 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 sphanet 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.
- If a tagged VLAN interface exists on the virtual interface, delete the tagged VLAN interface in advance by executing the ip command or other commands.
- The following message may be output on the system log in the environment where the firewalld service is working. However, the interface is normally inactivated.

```
firewalld[*]: ERROR: UNKNOWN_INTERFACE: shaX
```

## [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.

```
# /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.
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 active 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 is inactive. For the Fast switching mode and the GS linkage mode, the status is also displayed when the failure is detected in the remote systems. For the NIC switching mode, the status is displayed in the following cases.  <ul style="list-style-type: none"> <li>- Standby patrol is stopped.</li> <li>- Standby patrol suspends the use of the interface.</li> <li>- The interface is on standby.</li> </ul> For the Virtual NIC mode, the status is displayed for the interface on standby when the virtual interface is active.
	(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/FJShanet/usr/sbin/dsphanet -o
NIC      Destination Host Status
+-----+-----+-----+
eth0     hahostA      Active
         hahostB      Active
         hahostC      Inactive
eth1     hahostA      Active
         hahostB      Active
         hahostC      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".)
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]**

- Virtual interface of standby patrol cannot be specified using the -n option.
- 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/FJShanet/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/FJShanet/usr/sbin/dsphanet -o

```

## 7.5 hanetmask Command

---

**[Name]**

hanetmask - Sets, modifies, deletes, and prints a subnet mask.

**[Synopsis]**

```

/opt/FJShanet/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/FJSVhanet/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/FJSVhanet/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/FJSVhanet/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/FJShanet/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.
- Set the mask length of subnet mask which is set by this command as the same as the default netmask according to the address class or longer.
- In NIC switching mode, change the prefix value (a value set in /etc/sysconfig/network-scripts/ifcfg-ethX file) set to the physical IP address to the subnet mask value and set to the network address of a virtual IP.
- The setting by this command is required in the following cases: when the NIC switching mode, the Fast switching mode, or the GS linkage mode is used in the IPv4 configuration, when the NIC switching mode or the Fast switching mode is used in the dual configuration, or when the cluster takeover IP address of IPv4 is used in the Virtual NIC mode. This setting is not required for IPv6 configuration only. The subnet mask you have set is for the host name or the IP address specified by the **-i** option or the **-e** option of the hanetconfig command or the hanethvrs command.
- Do not change the settings with the hanetmask command while activating the virtual 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/FJShanet/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 the cluster failover function.

Specify how many times (count) communication with the communication target can fail consecutively before cluster failover is performed. A value from 0 to 100 can be specified. No cluster failover is performed if 0 is specified in value. When performing Cluster 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 constant monitoring is "a set value of this option x 2" immediately after the standby patrol is started.

### < 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. 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 (nsswitch.conf). Disabling this option allows you to change the host name by using the DNS server or the /etc/hosts file, depending on the OS setting (nsswitch.conf).  
As the initial value, YES (using only the /etc/hosts file to change the host name) is set.  
On the virtual interface in Virtual NIC mode, however, only the /etc/hosts file is used to change the host name regardless of this option 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).  
YES (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)     :YES
  Self-checking function(e)         :YES
```

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.
Cluster failover in unnormality(c)	ON	Cluster switching immediately occurs.
	OFF	Cluster switching does not occur at activating a userApplication.
Line status message output (s)		With or without a message output when a physical interface changed the status.
Line status message output (s)	ON	A message is output.
	OFF	A message is not output.
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.
LinkDown detection time (q)		Standby time for link down detection
LinkUp detection time (r)		Standby time for link up detection
Link monitor starting delay (g)		Standby time for startup of link status monitoring
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.

GLS: Global Link Services

### [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

command	Process outline	Authority
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}] or
/opt/FJSVhanet/usr/sbin/hanetpoll create -n devicename -p _none_

```

**-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] | \_none\_:**

When using ping response monitoring, specify the host name or IP address of the HUB connected as a monitoring target.

For single physical interface configuration (single bundled interface by virtual interface):

Set at least one monitoring target. Up to two monitoring targets can be set.

Specify the host name or IP address of the monitoring target to polladdress1.

If there is a second monitoring target, specify the host name or IP address of the monitoring target to polladdress2.

For redundant configuration (two bundled interfaces by virtual interface):

It is recommended to set two monitoring targets. At least set 1 monitoring target.

If there are two monitoring targets, specify the host name or IP address of the HUB to which the Primary interface connects to polladdress1, and specify the host name or IP address of the HUB to which the Secondary interface connects to polladdress2.

Specify the host name or IP address of the monitoring target to polladdress1 for one monitoring target.

Specify "\_none\_" if ping response monitoring is not to be used.

### Note

When setting the monitoring target using an IP address, IPv4 address or IPv6 address can be set as an address form.

When setting IPv6 address, do not set the prefix value.

If IPv6 address is to be set in an environment where address auto-configuration by IPv6 router is not performed, set the link-local address.

Also, do not use a host name that has the same name in IPv4 and IPv6 when setting the host name as the monitoring target.



sha0	OFF	hostA,192.168.10.10
sha1	OFF	_none_

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.
time		The monitoring count. Monitoring count is not used if monitoring by ping command is not used.
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. If monitoring by ping command is not used, _none_ is displayed. Each example,  sha0: Indicates that "hostA" is the primary monitoring destination and "192.168.10.10" is the secondary monitoring destination. sha1: Indicates that the monitoring by ping command does not operate.

#### (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}]}
or
/opt/FJSVhanet/usr/sbin/hanetpoll modify -n devicename -p _none_

```

**-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] | \_none\_:**

When changing the monitoring destination of ping response monitoring function specify the host names or IP addresses. When monitoring is not used "\_none\_" is specified. For details on the procedure, see -p option of (1)create command.

**-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.



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 the parameter of HUB monitoring function, use the on command:

```
/opt/FJSVhanet/usr/sbin/hanetpoll on [-s sec] [-c time] [-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 the HUB-to-HUB monitoring is enabled, or when setting two monitoring destinations in a single physical interface configuration, set 2 seconds or more. If this option is not specified, the previous setting is enabled. Initially, 5 (seconds) is specified.

**-c time:**

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. When not using monitoring by ping command, the set value in this option is not used.

**-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 "yes".

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
  link detection = YES
FAILOVER Status    = YES

[ Polling Parameter of each interface ]
Name  intvl idle time - link Fover
-----+-----+-----+-----+-----+-----+
sha0   2    60   5  --- YES  NO
sha1   3    60   5  --- YES  YES
sha2   ---   ---   --- ---  ---  ---
```

Display		Contents
[ Standard Polling Parameter ]		The current status of the monitoring function.
[ 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. Monitoring count is not used if monitoring by ping command is not used.
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, enable the monitoring again (execute the "hanetpoll on" command).

```
/opt/FJSVhanet/usr/sbin/hanetpoll devparam -n devicename [-s sec] [-c time]
[-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 time:**

Specify the monitoring count. 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").
- When monitoring the virtual interface to be used in a cluster environment of the physical IP address takeover II, that virtual interface is monitored only when 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.

- 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 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/dsppoll
Polling Status      = ON
interval(idle)     = 5( 60)
times               = 5
link detection      = YES
FAILOVER Status    = YES

Status  Name  Mode  Primary Target/Secondary Target          HUB-HUB
+-----+-----+-----+-----+-----+-----+-----+
  ON   sha0   d    192.168.74.2(ON)/192.168.74.3(WAIT)        ACTIVE
  ON   sha1   d    fec0:1::100(ON)/fec0:1::101(WAIT)         ACTIVE
  ON   sha2   d    ----(ON)/----(WAIT)                      OFF
```

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. Cannot be used if monitoring is not performed by ping command.	
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.	
		(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/FJShanet/usr/sbin/dsppoll
```

## 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



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.

**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 the "/usr/sbin/ip link set dev ethX up" 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.

- In the following cases, "hanetnic change" command cannot be executed.
  - For NIC switching mode
    - Virtual interface state is inactive in a single configuration.
    - userApplication of physical IP address takeover II state is Offline or Standby.
  - For Virtual NIC mode
    - Standby interface state is cut off.
    - Standby interface state is link down.
    - Virtual interface state is inactive.
- 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]

stpctl

### [Notes]

The standby patrol is automatically started when the system is started up. Use this command to start the standby patrol manually after the system is started up.

### [Examples]

The following shows an example of starting the standby patrol defined in a virtual interface (sha4).

```
# /opt/FJShanet/usr/sbin/strptl -n sha4
```

## 7.11 stpctl Command

---

### [Name]

stpctl - Stopping the standby patrol

### [Synopsis]

```
/opt/FJShanet/usr/sbin/stpctl -n devicename1[,devicename2,...]
```

### [Feature description]

The stpctl command stops the standby patrol in NIC switching mode.

### [Option]

You can specify the following option:

`-n devicename1[,devicename2,...]:`

Specify the name of a virtual interface of the standby patrol to be stopped. You can specify more than one virtual interface by listing them delimited with a comma (.).

### [Related commands]

strptl

### [Notes]

The standby patrol is automatically stopped when the system is shut down. Use this command to stop the standby patrol manually after the system is started up.



## [Examples]

The following shows an example of stopping the standby patrol defined in a virtual interface (sha4).

```
# /opt/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
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 0 is specified or when this option 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 (not multiplexed), 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/FJSVhanet/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	Virtual interface name When monitoring a tagged VLAN interface, the name of the virtual interface from which the tagged VLAN interface is originally generated is displayed.
VID	When monitoring a virtual interface, a hyphen ("-") is displayed. When monitoring a tagged VLAN interface, the tag ID is displayed.
Target	Target IP addresses in HUB monitoring are displayed in the order of primary and secondary monitoring targets. If no monitoring target is specified, a hyphen ("-") is displayed.

 **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

Name      Monitoring Parameter
+-----+-----+
sha1      auto_startup      =    NO
          interval      =    5 sec
          times         =    5 times
          repair_times  =    5 times
          idle          =    30 sec
          Auto fail-back =    YES
          FAILOVER Status =    NO
```

Display		Contents
Name		Virtual interface name When monitoring a tagged VLAN interface, the name of the virtual interface from which the tagged VLAN interface is originally generated is displayed.
VID		When monitoring a virtual interface, a hyphen ("-") is displayed. When monitoring a tagged VLAN interface, the tag ID is displayed.
Monitoring Parameter		The monitoring parameter currently set is displayed.
auto_startup	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.
interval		The monitoring interval is displayed in seconds.
times		The number of error monitoring
repair_times		The number of recovery monitoring
idle		In seconds the wait time that elapses after monitoring starts and before the HUB links up.
Auto fail-back	YES	Automatic fail-back is enabled.

Display		Contents
	NO	Automatic fail-back is disabled.
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.

### Note

When network monitoring is started, you cannot change the settings of monitoring parameters. Stop network monitoring before executing this command.

### (3) on command

Use the on command to start network monitoring. Execute this command for every virtual interface.

Normally, network monitoring is started along with the activation of a virtual interface, but this command is used to resume network monitoring after suspending the network monitoring by the off command.

```
/opt/FJSVhanet/usr/sbin/hanetpathmon on [-n devicename]
```

-n devicename

Specify the names of virtual interfaces (such as sha0 and sha1) for which to start network monitoring. When this parameter is omitted, monitoring all virtual interfaces for which monitoring is enabled is started.

### (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.
	----	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 in RHEL8, be sure to add the route information in the `/etc/sysconfig/network-scripts/route-"interface name"` file to use the virtual gateway to communicate with the remote host. In RHEL9, static routing information is set automatically and does not need to be defined manually.

**[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

Command	Process outline	Authority
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.

**routeraddressX:**

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)
	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.

## 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.
- 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 ["I.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 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 vipl -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 address 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 address 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 address. The host name that can be specified is 16 characters or less.

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 address.

## 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`).
- In Virtual NIC mode, the name format "shaX-NN" cannot be used for the host name. (Example: sha0-65)
- 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.

### Point

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     takeovervip1  -              -
sha1:65     -              takeovervip2/64 -
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.

Display	Contents
takeover-ipv4	A host name or an IP address of a takeover IP address (IPv4) to add to a logical virtual interface.
takeover-ipv6	A host name or an IP address of a takeover IP address (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	In Virtual NIC mode, VLAN ID of a tagged VLAN interface to which a takeover IP address 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.
- If the network corresponding to the IPv4 address was specified by -i option or -e option of the create command and this network does not exist in the setting of hanetmask command, the default netmask is used according to the address class.

### [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.
- After recovering the configuration file, if a numeric string is specified as the host name, change the numeric string to the IP address before rebooting the system.

Here is the example to change a numeric string to the host name by using hanetconfig.

1) Check the current configuration status.

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

Name	Hostname	Mode	Physical ipaddr	Interface List
sha0	123456	d	123457	eth2,eth3

```
[IPv6]
```

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

2) Use the modify command to change a numeric string used as the host name

This is when changing the numeric string to the IP address.

Change 123456 to 0.1.226.64

Change 123457 to 0.1.226.65

```
# /opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 0.1.226.64 -e 0.1.226.65
```

3) Confirm the changed configuration status.

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

Name	Hostname	Mode	Physical ipaddr	Interface List
sha0	0.1.226.64	d	0.1.226.65	eth2,eth3

```
[IPv6]
```

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

## [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.

### [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.
- Execute the dsphanet command after executing the resethanet -s command to check if the status of virtual interface is displayed. If the status is not displayed, the Redundant Line Control Function may fail to restart. Execute the resethanet -s command again.

### [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 EEEE FFFF  
(1)    (2)    (3)    (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.

### (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)

---

The information message described in this section is output when the command is executed, but some information is also output to the system log.

The message number, facility and priority that are output to the system log are as follows.

Facility	Priority	Message number
user	info	001

Message number	Message	Meaning	Action
000	normal end.	Execution of the command was successfully completed.	None
001	The virtual interface is excluded from HUB monitoring. (shaX)	This virtual interface is excluded from the monitoring target of HUB monitoring function.	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.

The message described in this section is output when the command is executed, but some message is also output to the system log.

The message number, facility and priority that are output to the system log are as follows.

Facility	Priority	Message number
user	error	111, 168, 301, 322, 357, 359, 501, 502, 510, 511, 512, 513, 538, 547, 548, 551, 552, 553, 555, 556, 557, 558, 559, 561, 780
user	warning	780

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.

Message number	Message	Meaning	Action
105	invalid ip_address.	An invalid IP address is specified.	Specify the correct IP address for re-execution.
111	invalid parameter.	An invalid parameter is specified.	Read the appropriate command reference, and execute the command again.
112	invalid argument.	An invalid command argument was found.	Read the appropriate command reference, and execute the command again.
114	-r option value is invalid.	An invalid value is specified.	Read the appropriate command reference to get the correct value, and execute the command again.
115	-s -c option total value is invalid.	An invalid value is specified.	Specify the values (-s and -c) so that the product of the two values does not exceed 300, and execute the command again.
116	-s -c option value is invalid.	An invalid value is specified.	The values (-s and -c) must be selected from within a range of 1 to 300. Specify a number 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.
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.

Message number	Message	Meaning	Action
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.
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.	One of the following events has occurred. - A virtual interface configured with invalid operation mode or incompatible operation mode was specified. - An unsupported operation mode has been specified.	Take one of the following actions. - Specify a virtual interface configured with valid operation mode or compatible operation mode. - Specify a supported 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

Message number	Message	Meaning	Action
			settings for redundant line control function, in /etc/hosts file. If the host name does not exist, create one and try again. If the host name exists in these files, check if the name contains characters other than alphanumeric characters, hyphen, and period. Also make sure it does not use non-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 In Virtual NIC mode, see also

Message number	Message	Meaning	Action
			"2.10.4 Duplicated operation via Virtual NIC mode."
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.
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.
177	polling is active.	The monitoring function is operating.	Stop (OFF) the monitoring function using the hanetpoll command, and execute the command again.
178	invalid version.	An incorrect version is specified.	Specify the version of the backed up Redundant Line Control Function, and execute the command again.
179	invalid virtual interface count(max 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.
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.
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	Review the number of the physical interfaces that

Message number	Message	Meaning	Action
		specified virtual interface has reached the maximum number possible to bundle. Therefore, it is not possible to add an actual interface dynamically.	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.
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

Message number	Message	Meaning	Action
			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 cannot 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.
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.
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.



Message number	Message	Meaning	Action
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.

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.

Message number	Message	Meaning	Action
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.	One of the following events has occurred. - An invalid operation mode is specified in the configuration information. - An unsupported operation mode is included.	Review the configuration information.
314	target is not defined.	The destination information for monitoring does not contain the address information of the monitoring destination.	Review the destination information for monitoring.
315	polling device is already defined.	The destination information for monitoring contains multiple specification entries with the same virtual interface name.	Review the destination information for monitoring.
316	same polling addresses are specified.	Primary/Secondary interfaces specified the same monitor-to address.	Review the destination information for monitoring.
317	interface name is not defined.	The virtual interface name is not specified in the destination information for monitoring.	Review the destination information for monitoring.
318	invalid device count(max 64).	The number of specified virtual interfaces exceeds 64.	Review the configuration information or destination information for monitoring.

Message number	Message	Meaning	Action
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.
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.
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

Message number	Message	Meaning	Action
			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 Redundant Line Control Function and cluster system.
361	virtual interface is not defined.	A virtual interface is not set.	Review the setting of Redundant Line Control Function and cluster system.
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.
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.
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".
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,

Message number	Message	Meaning	Action
			uninstall the package of the GLS and install it again.

GLS: Global Link Services

Table A.3 Message number 5xx

Message number	Message	Meaning	Action
501	socket() fail.	An error was found in the internal system call.	Make sure that the Redundant Line Control Function and the cluster system are 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 the cluster system, and then contact field engineers to report the error message. See the manual of the cluster system as to the materials necessary for examining the cluster system.
502	ioctl(SIOCGIFCONF) fail.	An error was found in the internal system call.	Make sure that the Redundant Line Control Function and the cluster system are 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 the cluster system, and then contact field engineers to report the error message. See the manual of the cluster system as to the materials necessary for examining the cluster system.
510	could not allocate memory.	An error was found in the internal system call.	Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control Function and cluster system, and then contact field engineers to report the error message. See the manual of a cluster system as to the materials necessary for examining a cluster system.
511	could not open file.	An error was found in the internal system call.	Execute a command again. If the same phenomenon occurs, collect materials for examination of Redundant Line Control Function, and then

Message number	Message	Meaning	Action
			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.	Make sure 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 then contact field engineers to report the error message.
516	ioctl(I_PUNLINK) fail.	An error was found in the internal system call.	Make sure 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 then contact field engineers to report the error message.
519	ioctl(SHAIOCPLUMB) fail.	An error was found in the internal system call.	Make sure 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

Message number	Message	Meaning	Action
			then contact field engineers to report the error message.
525	ioctl(SHAIOCGETINFO) fail.	An error was found in the internal system call.	Make sure 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 then contact field engineers to report the error message.
538	total entry is negative value.	An unexpected error occurred during reading configuration information.	Make sure 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 then contact field engineers to report the error message.
539	ioctl(SHAIOCNODENAME) fail.	An unexpected system call error occurred.	Make sure 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 then contact field engineers to report the error message.
540	ioctl(SHAIOCIPADDR) fail.	An unexpected system call error occurred.	Make sure 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 then contact field engineers to report the error message.
541	ioctl(SHAIOCSAP) fail.	An unexpected system call error occurred.	Make sure 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

Message number	Message	Meaning	Action
			Line Control Function, and then contact field engineers to report the error message.
542	ioctl(SHAIOCDEBUG) fail.	An unexpected system call error occurred.	Make sure 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 then contact field engineers to report the error message.
543	ioctl(SHAIOCWATCHDOG) fail.	An unexpected system call error occurred.	Make sure 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 then contact field engineers to report the error message.
545	ioctl(SHAIOCMESSAGE) fail.	An unexpected system call error occurred.	Make sure 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 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.	Make sure 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 then contact field engineers to report the error message.



Message number	Message	Meaning	Action
548	ioctl(SIOCGIFNUM) fail.	An unexpected system call error occurred.	Make sure 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 then contact field engineers to report the error message.
550	opendir failed.	An unexpected system call error occurred.	Make sure 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 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 detach failed.	An error was found in the internal system call.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
555	IPC key generate failed.	An error was found in the internal system call.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
556	get semaphore failed.	An error was found in the internal system call.	No action is required because recovery is automatically made. However, the message is output repeatedly, follow the procedure described below. The following system resources

Message number	Message	Meaning	Action
			<p>are required for Redundant Line Control Function:</p> <ul style="list-style-type: none"> <li>* semsys:seminfo_semmni (The maximum number of the semaphore identifiers) : One or greater</li> <li>* semsys:seminfo_semmns (The maximum number of the semaphores in a system) : One or greater</li> </ul> <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 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 Redundant Line Control Function:</p> <ul style="list-style-type: none"> <li>* shmsys:shminfo_shmmax (The maximum size of the shared memory segment) : 5120 or greater</li> <li>* shmsys:shminfo_shmmni (The maximum number of the shared memory segments) : two or greater</li> </ul> <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</p>

Message number	Message	Meaning	Action
			(minimum size of the shared memory segment). 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. If the problem still remains even after the identifier has been changed, collect examination materials of Redundant Line Control Function and contact field engineers.
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.
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 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.
567	ioctl(SIOCGIFADDR) fail.	An error occurred in the internally used system call.	Make sure 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,

Message number	Message	Meaning	Action
			collect materials for the examination of the Redundant Line Control Function, and then contact field engineers to report the error message.
568	ioctl(SIOCGIFNETMASK) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the 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 then contact field engineers to report the 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 then contact field engineers to report the error message.
571	failed to send request.	An error occurred in the internally used system call.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
572	failed to receive response.	An error occurred in the internally used system call.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
573	request timeout.	An error occurred in the internally used system call.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the 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 Redundant Line Control Function, and then contact field engineers to report the error message.
575	failed to restart hanet.	Failed to reactivate the Redundant Line Control Function.	Execute the command again. If the same phenomenon still occurs, collect the examination materials of Redundant Line Control Function, and then

Message number	Message	Meaning	Action
			contact field engineers to report the error message.
576	failed to enable configuration.	An error has occurred while processing the configured values.	If you are modifying /etc/hosts file, you must reboot the system. If /etc/hosts file has not been changed, restart the Redundant Line Control function; (/opt/FJShanet/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 then contact field engineers to report the 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

Message number	Message	Meaning	Action
			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.	Make sure 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 then 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 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.

GLS: Global Link Services

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.

Message number	Message	Meaning	Action
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.
707	the name of the virtual interface is already used. name=xxx	The name of the virtual interface has already been used.	With the ip command, find the interface which has the same name. If it is the virtual bridge, delete it with the ip 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 the ip command. If so, delete the VLAN interface with the ip command and execute the command again.
750	no hanetmask setting for specified IP address, the default netmask is used. (ip address= <i>ipaddress</i> , default netmask= <i>netmask</i> )	The setting of hanetmask corresponding to the set IP address does not exist. The default netmask is used. <i>ipaddress</i> : set IP address <i>netmask</i> : netmask to use	No action is required if the subnet is not used for allocation. The default netmask is used for the set IP address. When using the subnet for allocation, set the subnet mask by using the hanetmask command. Execute the hanetmask print command and make sure that following settings for subnet mask are done:  - The subnet mask is set  - <i>ipaddress</i> belongs to the network address
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

Message number	Message	Meaning	Action
			materials for the examination of the Redundant Line Control function and contact field engineers to report the error message.
766	ioctl(SHAIOCSETNICCHANGE) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the error message.
767	ioctl(SHAIOCGETSHADEVATR) fail.	An error occurred in the internally used system call	Make sure 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 then contact field engineers to report the error message.
768	ioctl(SHAIOCSETLBMODE) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the error message.
769	ioctl(SHAIOCCLBCTL) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the error message.
770	ioctl(SHAIOCGETLBPARAM) fail.	An error occurred in the internally used system call.	Make sure that the Redundant Line Control Function is correctly set. After confirming that there is no problem, execute the command again. If the same



Message number	Message	Meaning	Action
			phenomenon occurs, collect materials for the examination of the Redundant Line Control Function, and then contact field engineers to report the error message.
771	ioctl(SHAIOCGETLINFO) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the error message.
772	ioctl(SHAIOPREUNPLUMB) fail.	An error occurred in the internally used system call.	Make sure 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 then contact field engineers to report the error message.
780	nmcli failed.	An error occurred in the internally used nmcli command(1).	Make sure 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 then contact field engineers to report the error message.

### A.1.3 Console output messages (numbers 800 to 900)

The following describes the messages output on the console by Redundant Line Control Function, explanation, and operator response.

The following table shows facilities and priorities for the message numbers output to the system log.

Facility	Priority	Message number
kern	info	800, 801, 990, 991, 992
kern	error	910, 911, 912, 913, 914
user	info	888, 889, 890, 891, 892, 893, 894, 895
user	warning	848
user	error	other than those above



## Note

Messages with the following message numbers are not output on the console but output only on the system log.

888, 889, 890, 891, 892, 893, 894, 895

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 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.	Check if the operating system configuration file (ifcfg-ethX) is correct. 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.

Message number	Message	Meaning	Action
			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.
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.
822	no data in cluster event.	No data was found in the cluster event.	Make sure that the Redundant Line Control Function and the cluster system are correctly set. If there is no problem, collect materials for the examination of the Redundant Line Control Function and the cluster system, and then contact field engineers to report the error message. See the manual of the cluster system as to the materials necessary for examining the cluster system.
823	ClSetStat failed.	The cluster resource status could not be set.	Make sure that the Redundant Line Control Function and the cluster system are correctly set. If there is no problem, collect materials for the examination of the Redundant Line Control Function and the cluster system, and then contact field engineers to report the error message. See the manual of the cluster system as to the materials necessary for examining the 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

Message number	Message	Meaning	Action
			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.
833	ioctl(SHAIOCSETIPADDR) failed.	Failed to notify the IP address.	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
847	internal error retry over. polling stop.	A HUB monitoring internal error occurred. The HUB monitoring is stopped.	Make sure that the system, the Redundant Line Control Function, and the cluster system are correctly set. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and the cluster system, and then contact field engineers to report the error message. See the manual of the cluster system as to the materials necessary for examining the 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.
850	cannot down interface.	Failed to inactivate the physical interface.	Check if the Redundant Line Control function and the system are correctly set, and check if the operating system configuration file (ifcfg-ethX) is correct. 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

Message number	Message	Meaning	Action
			engineers to report the error message.
853	physical interface up failed.	Failed to activate a physical interface.	Make sure that the Redundant Line Control Function and the system are correctly set. If there is no problem, collect materials for the examination of the Redundant Line Control Function, and then contact field engineers to report the error message.
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) polling status changed: Primary polling failed. (ifname,target=pollip, vlan=vlanid)	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="#">H. 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.
871	polling status changed: Secondary polling failed. (ifname,target=pollip) polling status changed: Secondary polling failed. (ifname,target=pollip, vlan=vlanid)	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="#">H. 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.
872	polling status changed: PrimaryHUB to SecondaryHUB polling failed. (ifname,target=pollip)	An error in the secondary HUB was detected by HUB-to-HUB communication monitoring from the primary interface.	Check for any failure on the communication path to the monitoring destination. If monitoring fails even though possible to communicate normally,

Message number	Message	Meaning	Action
		ifname: Interface name pollip: Monitoring destination address	tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command. Review " <a href="#">H.3.1 Error messages(870) and corresponding actions for HUB monitoring</a> ".
873	polling status changed: SecondaryHUB to PrimaryHUB polling failed. (ifname,target=pollip)	An error in the primary HUB was detected by HUB-to-HUB communication monitoring from the secondary interface. ifname: Interface name pollip: Monitoring destination address	Check for any failure on the communication path to the monitoring destination. If monitoring fails even though possible to communicate normally, tune the intervals and the number of the times of monitoring, and the time to wait for a linkup with the hanetpoll command. Review " <a href="#">H.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.	No action is required.
	polling status changed: HUB repair (target=pollip,vlan=vlanid)	pollip: Monitoring destination address vlanid: VLAN for monitoring destination	
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="#">H.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.

Message number	Message	Meaning	Action
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) (code)	Since the interface was unjustly activated by the user, the state of an interface is restored. ifname: interface name code: detailed code	Check that the interface has been recovered correctly. If this message was output except when a user has intentionally performed Up/Down of the physical interface, investigate the cause of Up/Down.
884	unexpected interface deactivation has been detected. (ifname) (code)	Since the interface was unjustly deactivated by the user, the state of an interface is restored. ifname: interface name code: detailed code	Check that the interface has been recovered correctly. If this message was output except when a user has intentionally performed Up/Down of the physical interface, investigate the cause of Up/Down.
885	standby interface recovered. (ifname) standby interface recovered. (ifname, vlan=vlanid)	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.
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.

Message number	Message	Meaning	Action
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)	The immediate automatic fail-back to the primary interface by the standby patrol was restrained. ifname: A name of an interface. This message is output when the monitor-to information to set by a hanetpoll create command is other than HUB.	It is not necessary to deal with.
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 ifname: Physical interface name	No action is required.
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 /usr/sbin/ip addr show ifname command (LOWER_UP 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.

Message number	Message	Meaning	Action
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 "hanetnic change" command is executed.  *vlantype The "vlantype" is output when a tagged VLAN interface is created on the virtual interface. Take note that depending on the OS version, the "vlantype" is output even when a virtual bridge is created on the virtual interface.
916	monitoring function detected failures in the entire transfer route. (ifname) monitoring function detected failures in the entire transfer route. (ifname, vlan=vlanid)	Failures in all transfer routes are detected by the network monitoring function. ifname: Interface name vlanid: VLAN for monitoring destination	Check that there is no problem in transfer routes to the monitoring destination and transfer routes between the operating NIC and the standby NIC.
923	physical interface is already linked by another network device. (device:ifname)	The specified physical interface cannot be bundled. It has already been used by another network device such as bonding. device: Virtual interface name ifname: Physical interface name	Review the setting of the interface.
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 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 on VMware or on Hyper-V. Check the setting of SHAMACADDR in the virtual

Message number	Message	Meaning	Action
			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.
931	hangup of ping command has been detected. (target=pollip)	A hang-up of the ping command for the monitoring destination is detected. pollip: Monitoring destination IP address	Collect materials for examination of Redundant Line Control Function, and then contact field engineers to report the error message.
932	cannot send fhsp message. (dest=hostip, code)	The message of Fujitsu Hot Standby Protocol failed to be sent. hostip: Destination IP address code: Detailed code	Check if the setting to pass through the firewall is correctly set for Fujitsu Hot Standby Protocol (UDP: port number 1807). 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.
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.
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 is installed. # rpm -qi kmod-FJSVhanet-drv
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

Message number	Message	Meaning	Action
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.	Make sure that the system, the Redundant Line Control Function, and the cluster system are correctly set. If the same phenomenon occurs, collect materials for the examination of the Redundant Line Control Function and the cluster system, 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.
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 /usr/sbin/ip addr show ifname command (LOWER_UP 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	Check the link state based on the execution results of the /usr/sbin/ip addr show ifname command (LOWER_UP flag displayed)

Message number	Message	Meaning	Action
		polip: monitoring destination address	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.
995	failed to start daemon.	Control daemon of GLS failed to be started.	Restart the redundant line control function (/opt/FJShanet/usr/sbin/resethanet -s) for the restoration. If the restoration fails, reboot the system.
996	polling status changed: Primary polling recovered. (ifname,target=pollip)	Primary monitoring has recovered. ifname: interface name pollip: monitoring destination address	No action is required.

GLS: Global Link Services

## A.2 Messages Displayed in the Cluster System Logs

This section explains the meaning and the action to take for each message output by Redundant Line Control function if startup of the cluster system fails.

Cluster system logs are stored in the following directories:

For details on each log file (switchlog, appX.log), see "PRIMECLUSTER Reliant Monitor Services (RMS) with Wizard Tools Configuration and Administration Guide."

/var/opt/SMAWRrms/log

Message number	Message	Meaning	Action
-	(Gls): ERROR: virtual interface resource not found.	There is no resource setting.	Pay attention to the following points and make sure that the system, the Redundant Line Control Function, and the cluster system are correctly set. <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. Execute "hanethvrsc print" to check it.</li> <li>- For NIC switching mode, ensure that the ping monitoring is set. Execute "hanetpoll print" to check it.</li> </ul>
-	(Gls): ERROR: GdBegin failed. (rsc_name, host_name)	Failed to activate the Gls detector. rsc_name: Resource name of the cluster host_name: Takeover virtual IP address (host name)	

Message number	Message	Meaning	Action
			<p>- If a host name is used in GLS, ensure that host name is already recorded in /etc/hosts.</p> <p>- Ensure that the IP address setting of RMS Wizard is identical to that of the GLS takeover IP address.</p> <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 the examination of the Redundant Line Control Function and the 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 make sure that the system, the Redundant Line Control Function, and the cluster system are correctly set.</p> <p>- Ensure that the setting of the takeover IP address is identical in each node of the cluster which takes over the IP address. Execute "hanethvrsc print" to check it.</p> <p>- For NIC switching mode, ensure that the ping monitoring is set. Execute "hanetpoll print" to check it.</p> <p>- If a host name is used in GLS, ensure that host name is already recorded in /etc/hosts.</p> <p>- Ensure that the IP address setting of RMS Wizard is identical to that of the GLS takeover IP address.</p>

Message number	Message	Meaning	Action
			<p>- 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>"</p> <p>If those settings are not correct, see the following sections to configure the settings correctly. After that, reboot the system or execute <code>resethanet -s</code>.</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 the examination of the Redundant Line Control Function and the cluster system, and then contact field engineers to report the error message.</p>

GLS: Global Link Services

# Appendix B Examples of configuring system environments

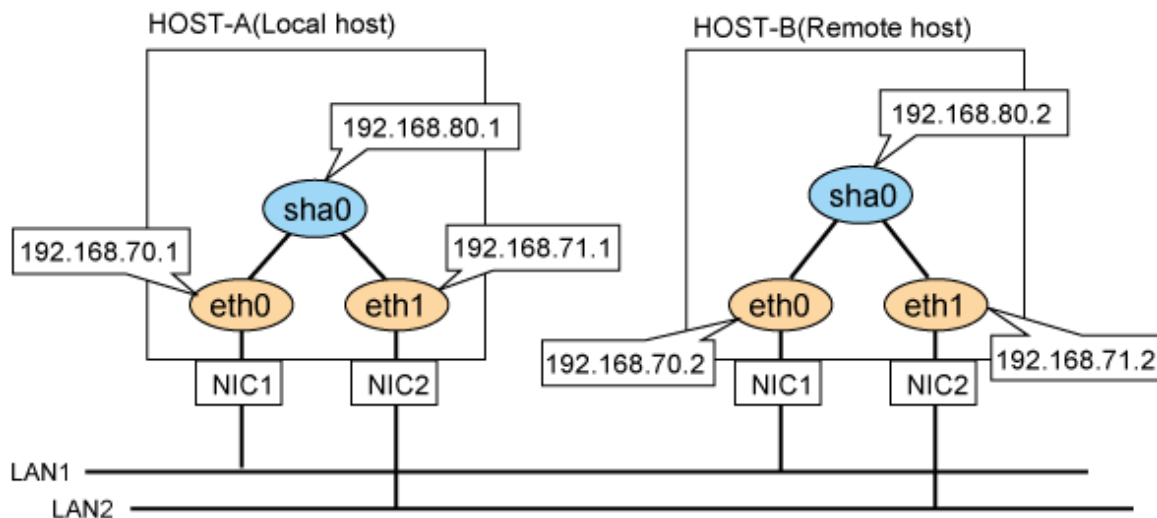
This appendix explains how to configure the system environment with redundant network control.

## 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 the /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
```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1



```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Reboot

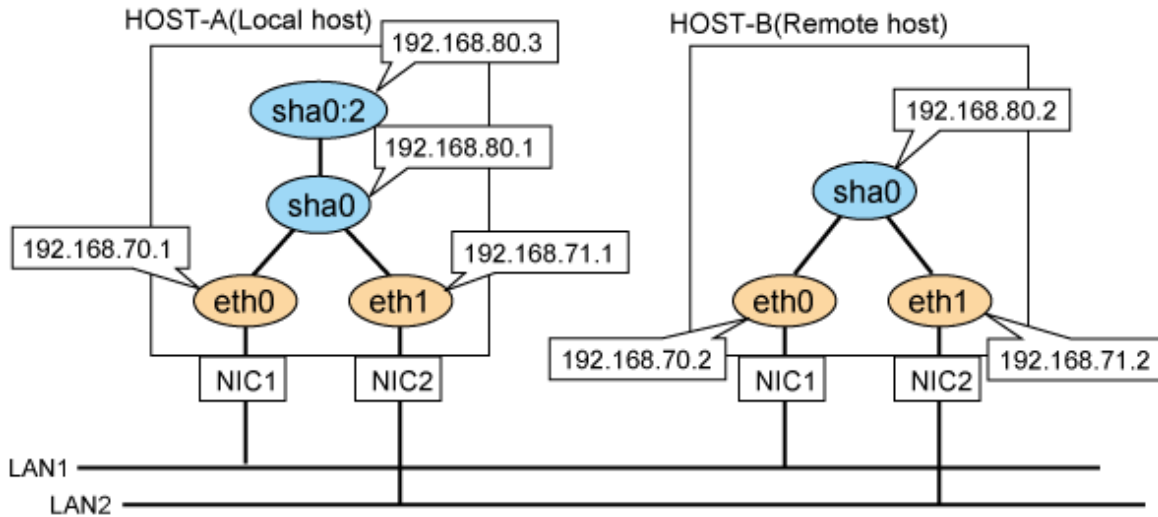
Run the following command to reboot the system.

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

## 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 the /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
```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating a logical virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0:2 -i 192.168.80.3
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
```

```
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

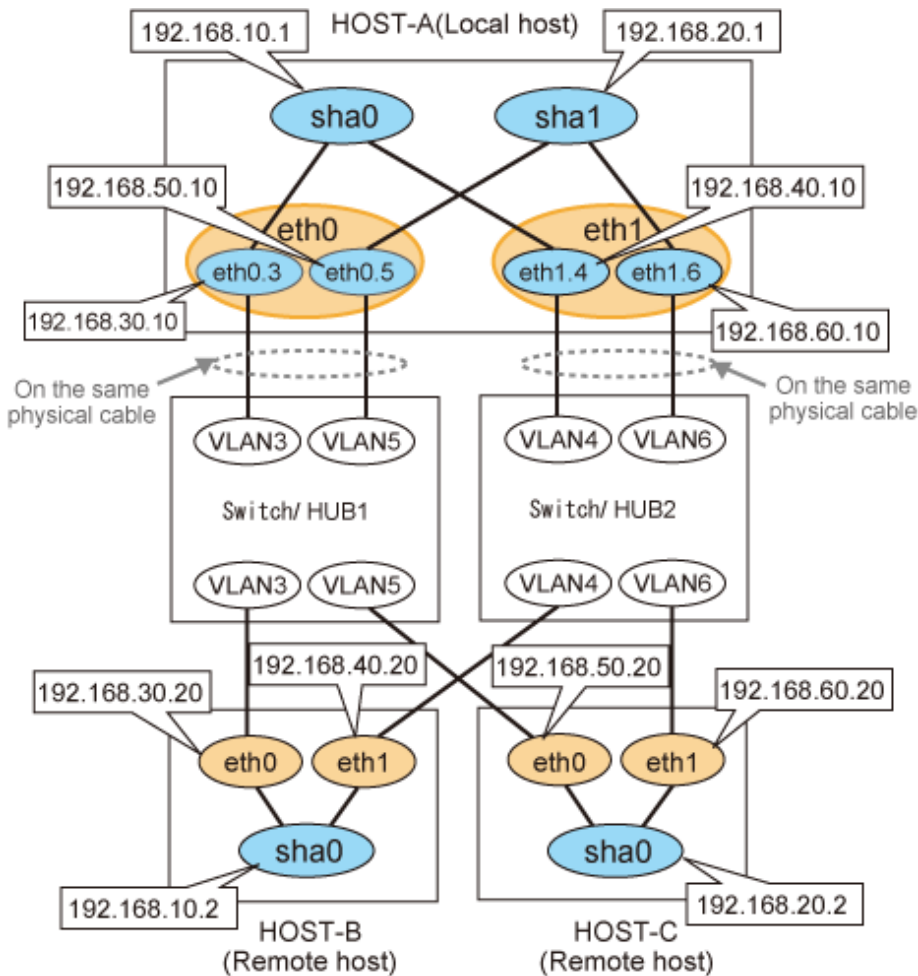
## 5) Reboot

Run the following command to reboot the system.

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

## 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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

1-3) Configure the /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=none
IPADDR=192.168.30.10
PREFIX=24
ONBOOT=yes
VLAN=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.4

```
DEVICE=eth1.4
BOOTPROTO=none
IPADDR=192.168.40.10
PREFIX=24
ONBOOT=yes
VLAN=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.5

```
DEVICE=eth0.5
BOOTPROTO=none
IPADDR=192.168.50.10
PREFIX=24
ONBOOT=yes
VLAN=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.6

```
DEVICE=eth1.6
BOOTPROTO=none
IPADDR=192.168.60.10
PREFIX=24
ONBOOT=yes
VLAN=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv4.addresses: ""
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv4.addresses: ""
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 3, 4, 5, 6.)

- Create eth0.3

```
# /usr/bin/nmcli connection add type vlan con-name eth0.3 ifname eth0.3
vlan.parent eth0 vlan.id 3
```

- Create eth1.4

```
# /usr/bin/nmcli connection add type vlan con-name eth1.4 ifname eth1.4
vlan.parent eth1 vlan.id 4
```

- Create eth0.5

```
# /usr/bin/nmcli connection add type vlan con-name eth0.5 ifname eth0.5
vlan.parent eth0 vlan.id 5
```

- Create eth1.6

```
# /usr/bin/nmcli connection add type vlan con-name eth1.6 ifname eth1.6
vlan.parent eth1 vlan.id 6
```

- Configuration of eth0.3

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.30.10/24"
connection.autoconnect: "yes"
```

- Configuration of eth1.4

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.40.10/24"
connection.autoconnect: "yes"
```

- Configuration of eth0.5

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.50.10/24"
connection.autoconnect: "yes"
```



- Configuration of eth1.6

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.60.10/24"  
connection.autoconnect: "yes"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload  
/usr/bin/nmcli connection up eth0  
/usr/bin/nmcli connection up eth1
```

## 3) Setting subnet masks

```
/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 virtual interfaces

```
/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) 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0  
BOOTPROTO=none  
IPADDR=192.168.30.20  
PREFIX=24  
ONBOOT=yes  
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1  
BOOTPROTO=none  
IPADDR=192.168.40.20  
PREFIX=24  
ONBOOT=yes  
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.30.20/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.40.20/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.10.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.10.2 -t eth0,eth1
```

## 5) 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
HOTPLUG=no
IPADDR=192.168.50.20
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
HOTPLUG=no
IPADDR=192.168.60.20
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.50.20/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.60.20/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.20.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.20.2 -t eth0,eth1
```

## 5) Reboot

Run the following command to reboot the system.

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

# 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.

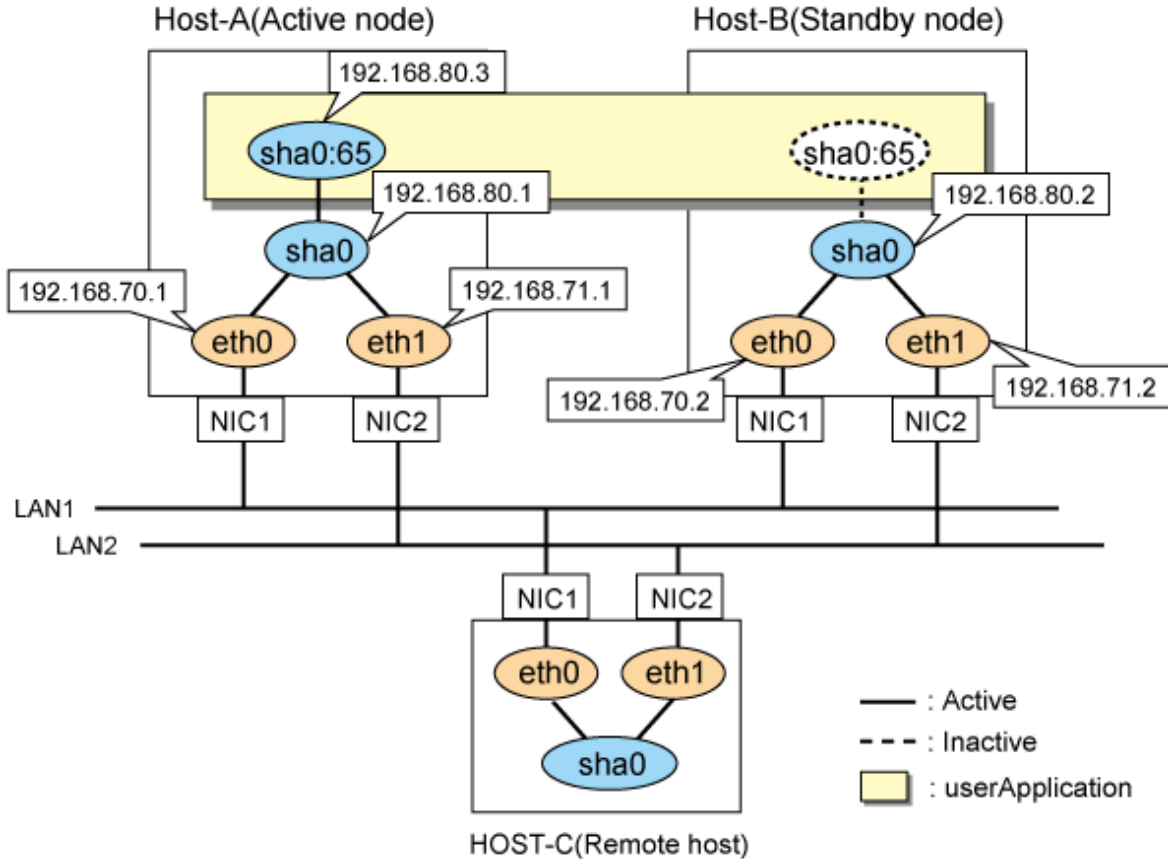
For the network configuration other than GLS, refer to "3.2.2 Network configuration".

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```

DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24

```

```
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

#### 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.3
```

#### 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 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.1.5 Example of the Cluster system (Mutual Standby)

---

This section describes an example configuration procedure of the network shown in the diagram below.

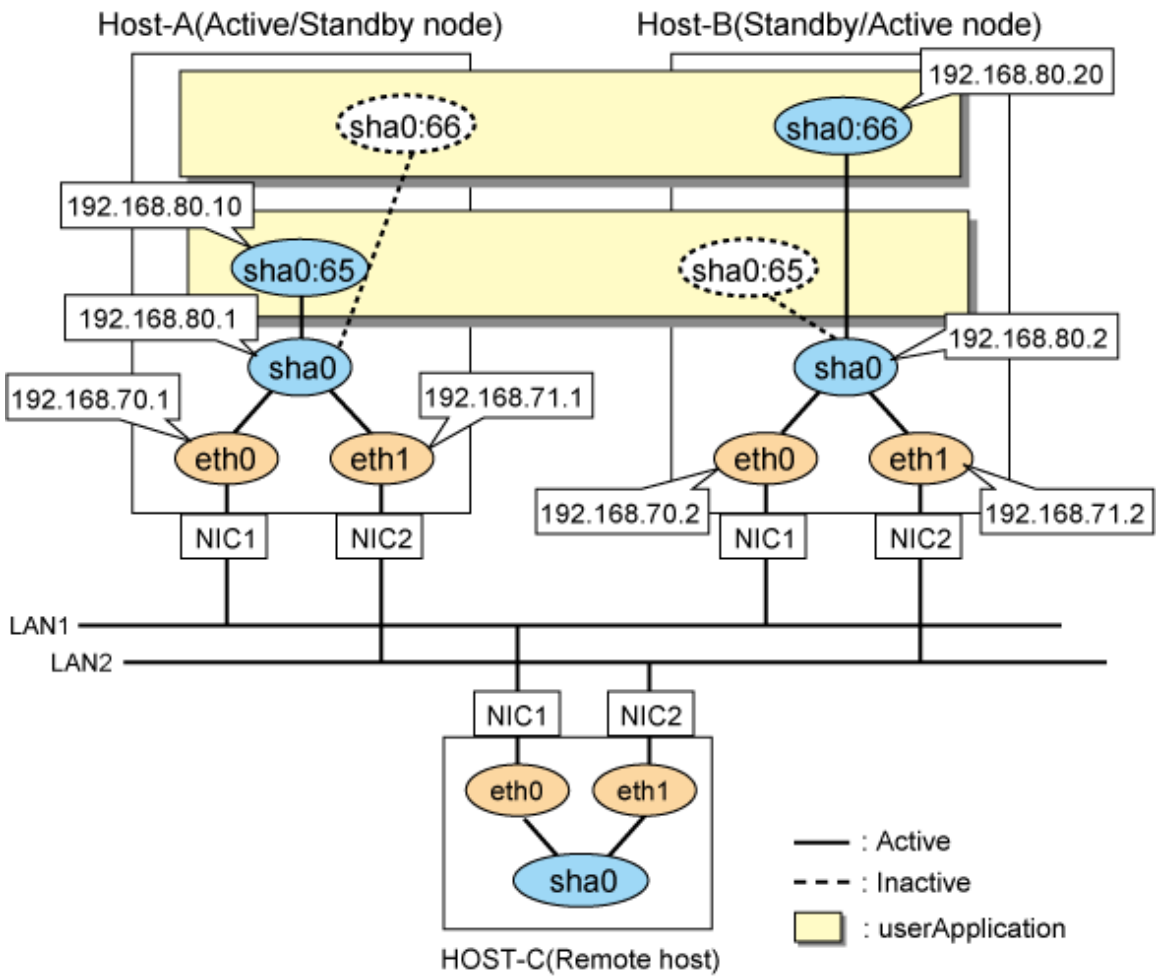
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```

DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet

```



- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating takeover virtual interfaces

```
/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
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

#### 5) Creating takeover virtual interfaces

```
/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
```

#### 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 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.1.6 Example of the Cluster system (N:1 Standby)**

---

This section describes an example configuration procedure of the network shown in the diagram below.

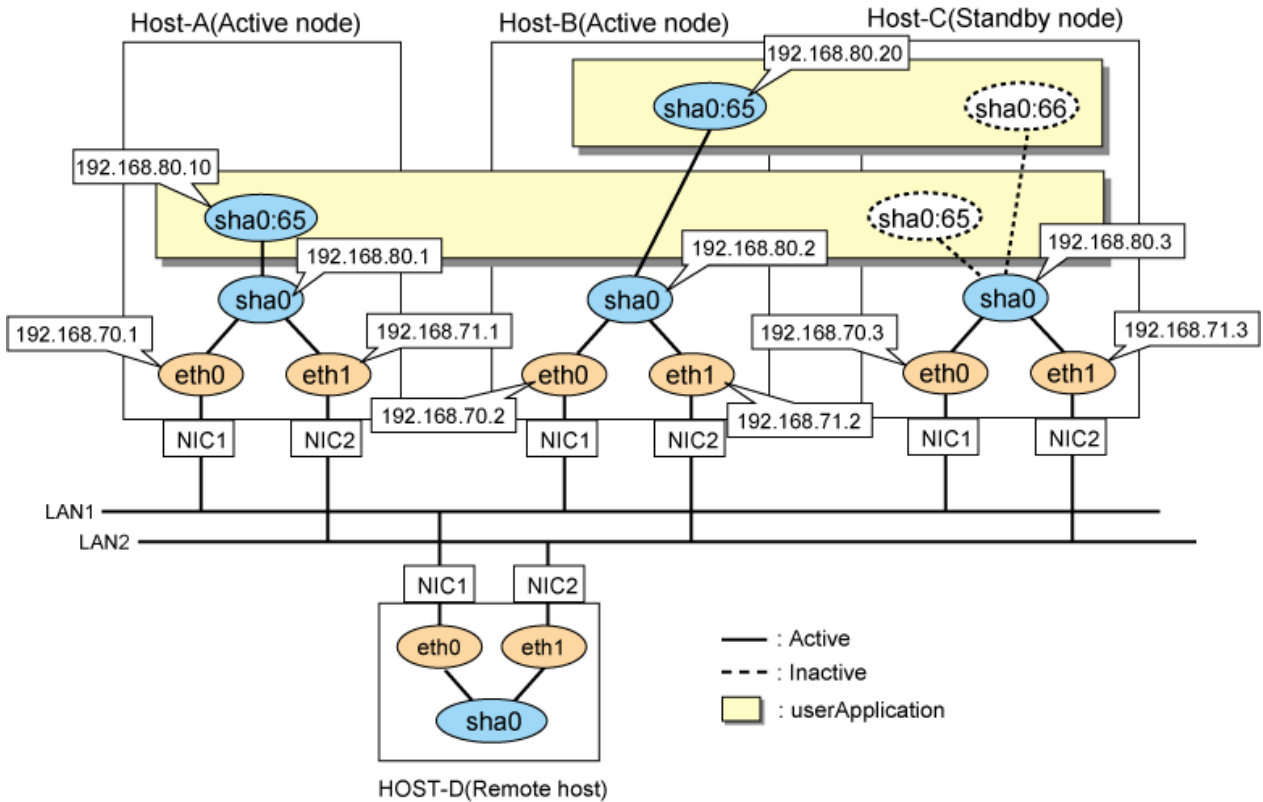
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```

DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.10
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJShanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.20
```

## 6) 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.3
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.3/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.3/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
```

## 5) Creating takeover virtual interfaces

```
/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
```

## 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, 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](#)".

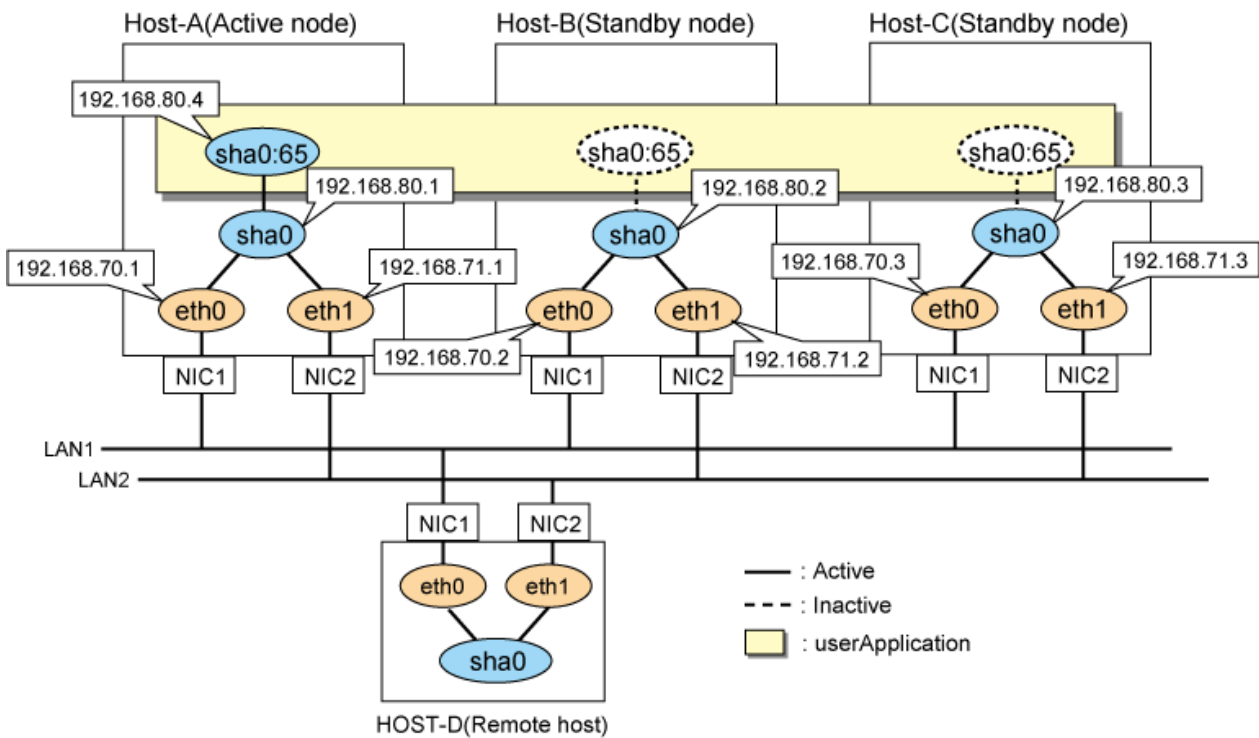
For configuring the cluster system, refer to the Cluster system manual.

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```

DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
TYPE=Ethernet

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24

```

```
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.1 -t eth0,eth1
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.2 -t eth0,eth1
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

## 6) 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0,1) file as follows.

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

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
DEVICE=eth1
BOOTPROTO=none
IPADDR=192.168.71.3
PREFIX=24
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.3/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.3/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

### 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m t -i 192.168.80.3 -t eth0,eth1
```

### 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.80.4
```

### 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, 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 NIC switching mode (IPv4)**

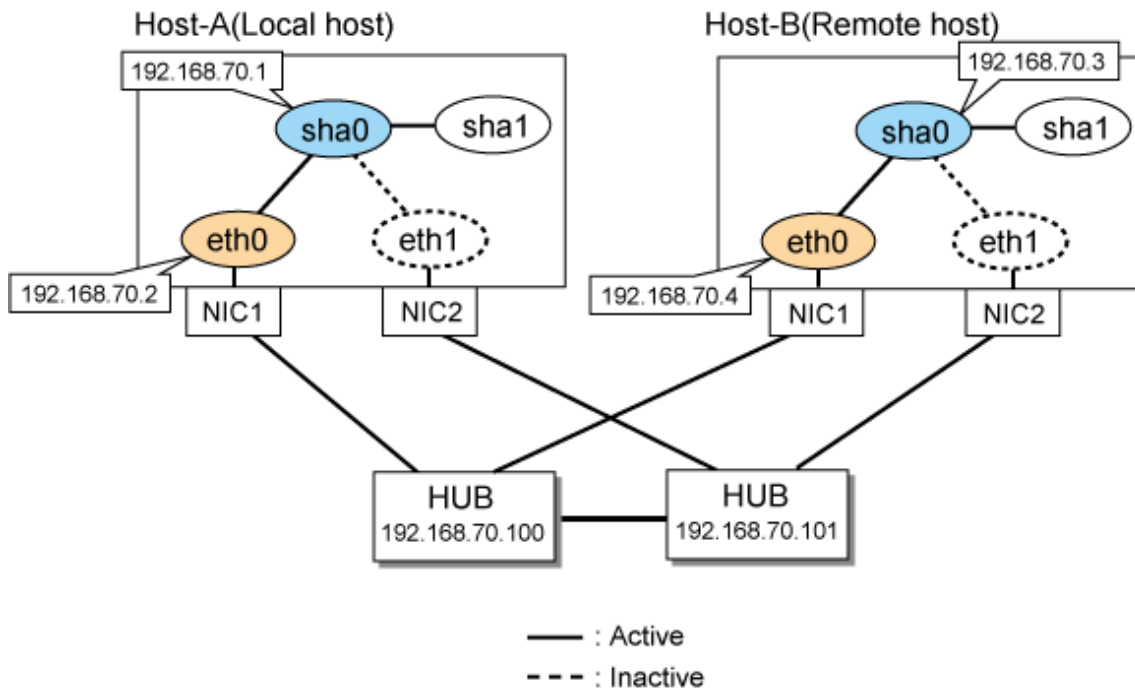
---

### **B.2.1 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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.2/24"  
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.2/24"  
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 5) Setting up the HUB monitoring function

```
/opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 6) Setting up the Standby patrol monitoring function

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 7) Reboot

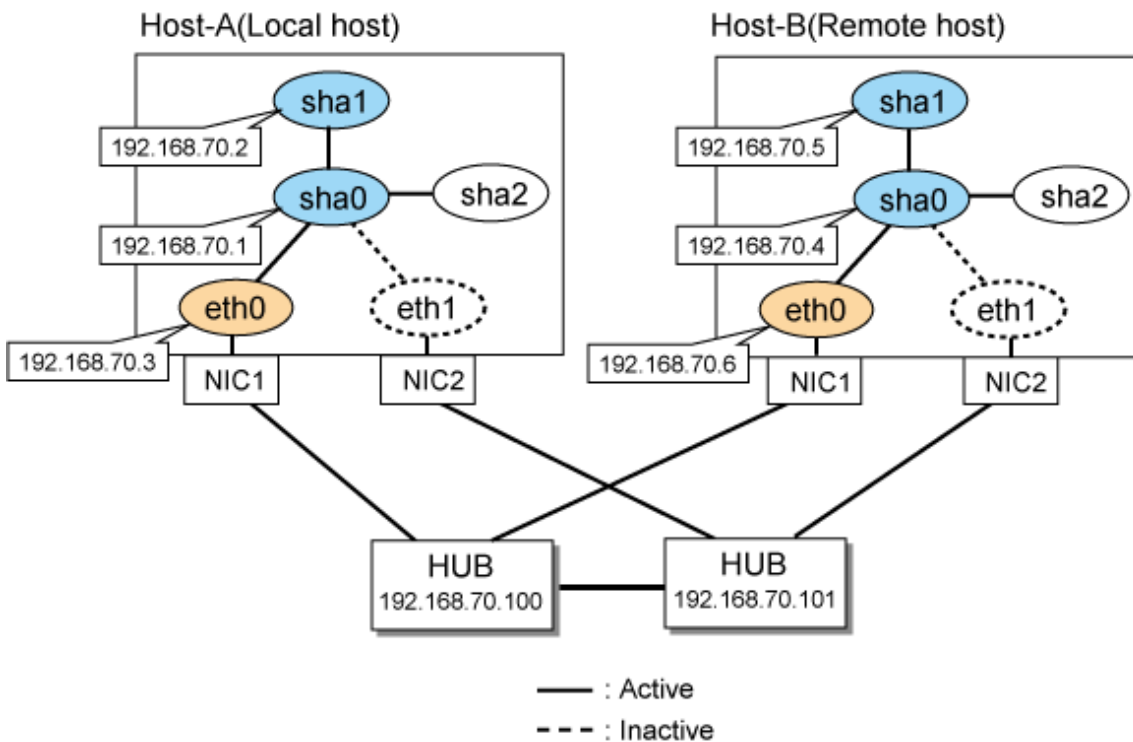
Run the following command to reboot the system.

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

## B.2.2 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    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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

#### 4) Creating virtual interfaces

```
/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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

#### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off  
/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) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet  
BOOTPROTO=none  
IPADDR=192.168.70.6  
PREFIX=24  
DEVICE=eth0  
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet  
BOOTPROTO=none  
IPADDR=192.168.70.6  
PREFIX=24  
DEVICE=eth1  
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.6/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.6/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

- For RHEL8

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/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) Reboot

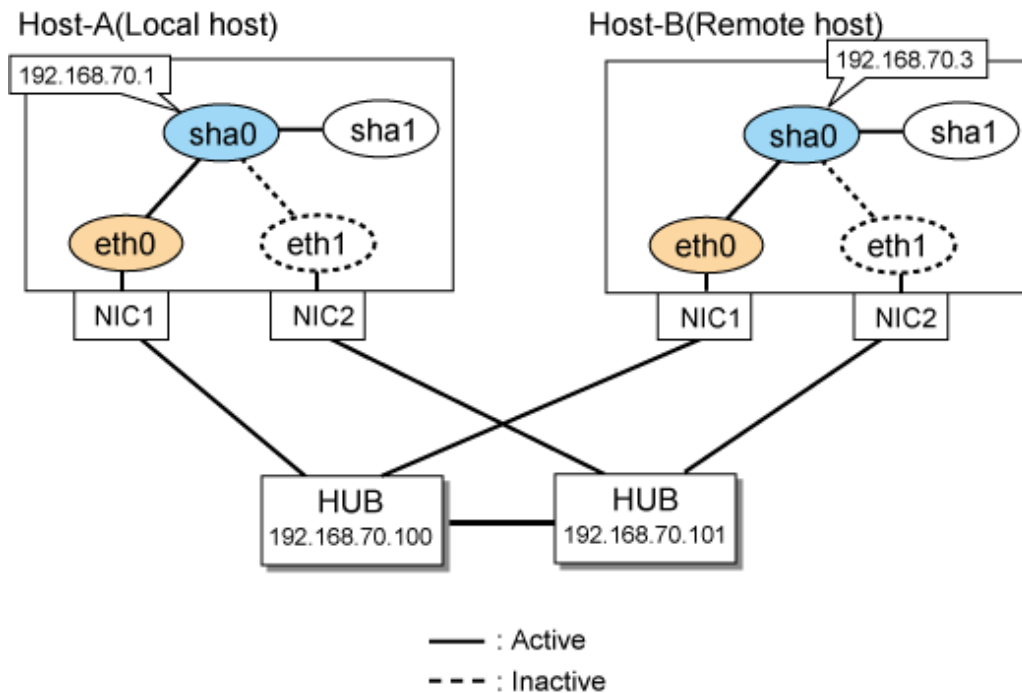
Run the following command to reboot the system.

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

## B.2.3 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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.1/24"  
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.1/24"  
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.1 -t eth0,eth1
```



Ensure that the physical IP address specified using option "-i" is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJShanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m e -i 192.168.70.3 -t eth0,eth1
```



## Note

Ensure that the physical IP address specified using option "-i" is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 7) Reboot

Run the following command to reboot the system.

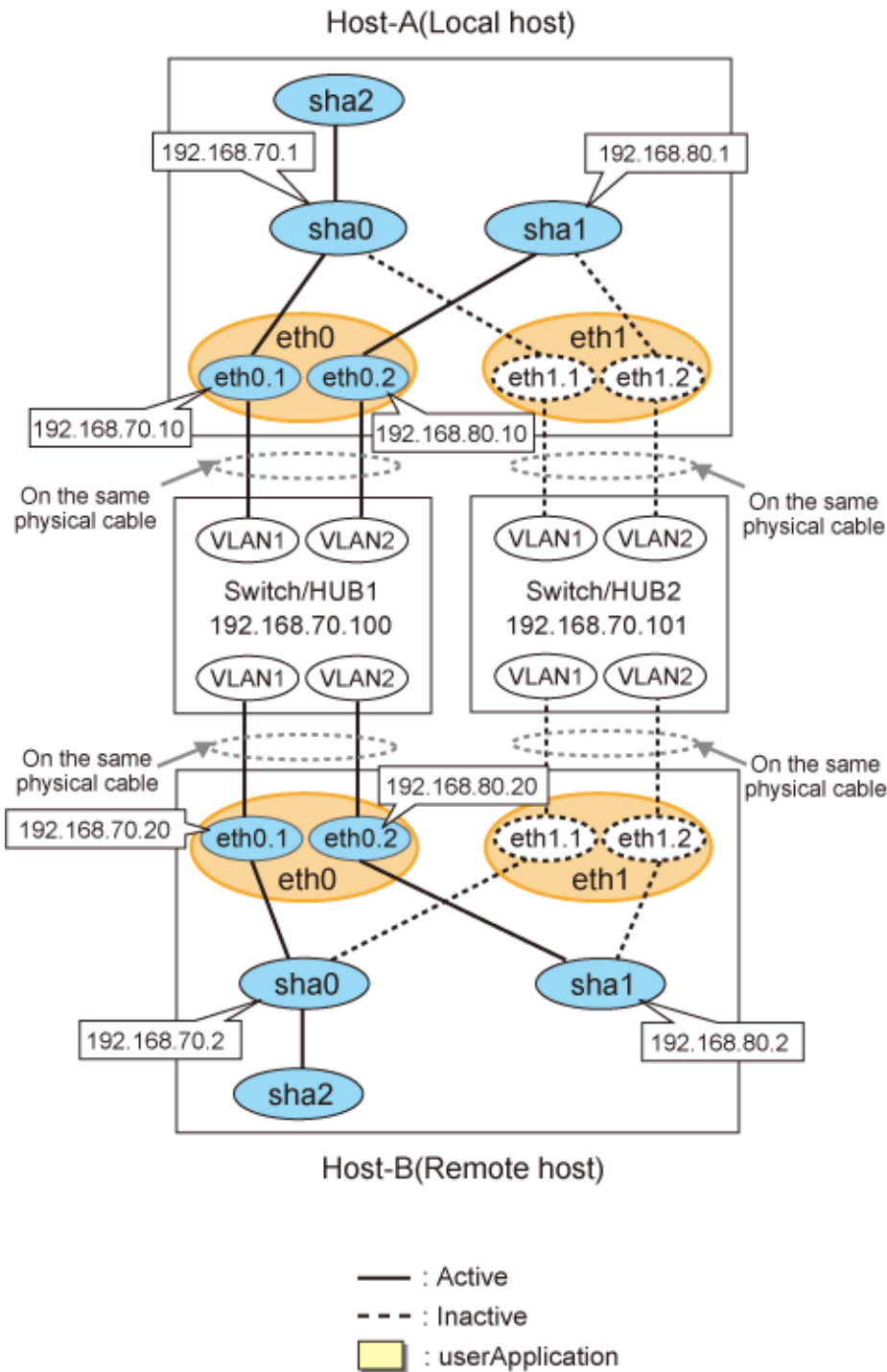
```
/sbin/shutdown -r now
```

## B.2.4 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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.10
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.10
PREFIX=24
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.10
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
```

```
BOOTPROTO=none
IPADDR=192.168.80.10
PREFIX=24
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2
vlan.parent eth1 vlan.id 2
```

- Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.10/24"
connection.autoconnect: "yes"
```

- Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.10/24"
connection.autoconnect: "yes"
```

- Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.10/24"
connection.autoconnect: "no"
```

- Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.10/24"
connection.autoconnect: "no"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth0.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.20
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.20
PREFIX=24
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.20
```

```
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.20
PREFIX=24
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2
vlan.parent eth1 vlan.id 2
```

#### - Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.20/24"
connection.autoconnect: "yes"
```

#### - Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.20/24"
connection.autoconnect: "yes"
```

#### - Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.20/24"
connection.autoconnect: "no"
```

#### - Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.20/24"
connection.autoconnect: "no"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth0.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJShanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 6) Setting up the HUB monitoring function (Synchronous switching)

```
/opt/FJShanet/usr/sbin/hanetpoll copy -n sha0,sha1
```

### 7) Setting up the Standby patrol monitoring function

Please define only one Standby patrol monitoring function.

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

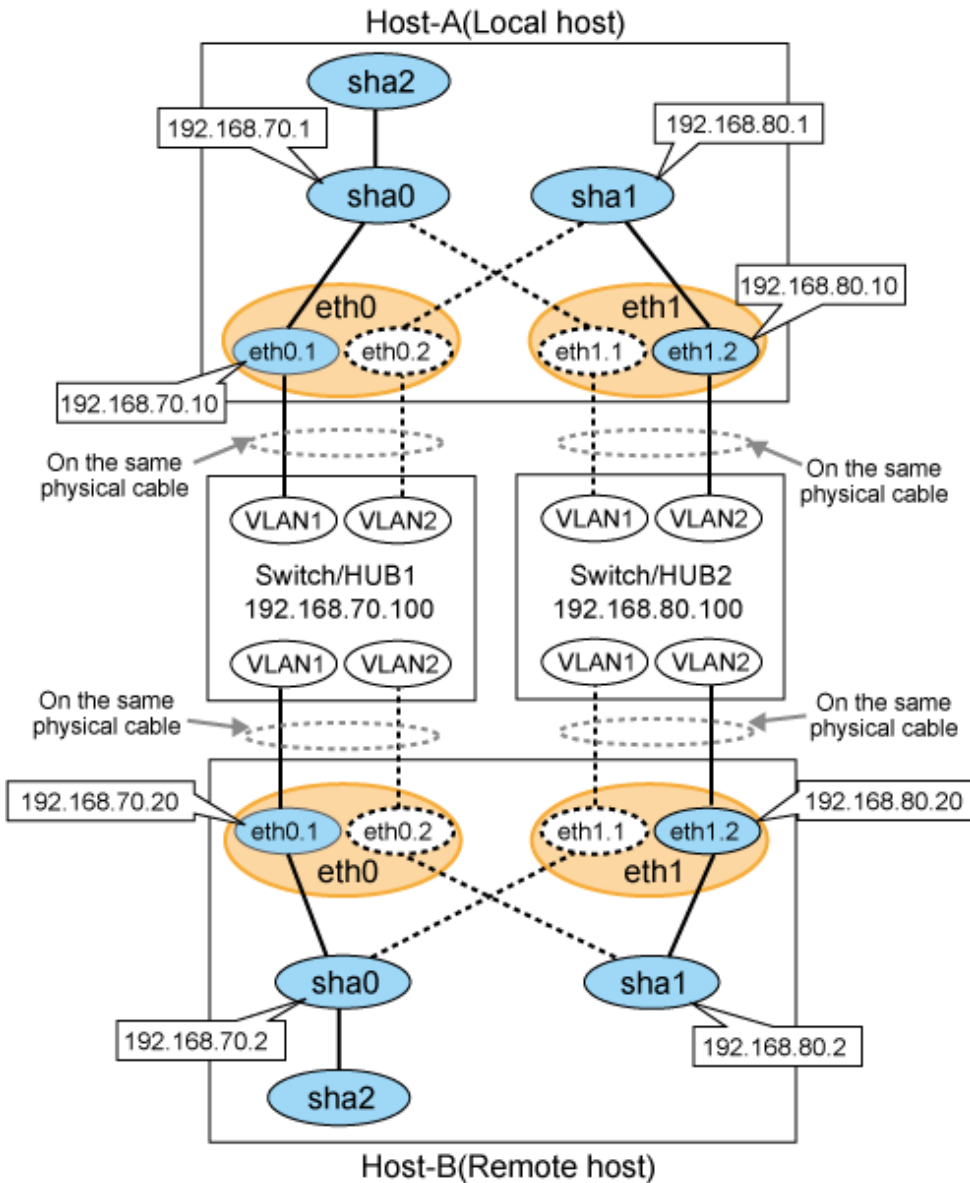
### 8) Reboot

Run the following command and reboot the system.

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

## B.2.5 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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y (X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.10
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.10
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
```

```
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.10
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.10
PREFIX=24
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2
vlan.parent eth1 vlan.id 2
```

- Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.10/24"
connection.autoconnect: "yes"
```

- Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.10/24"
connection.autoconnect: "no"
```

- Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.10/24"
connection.autoconnect: "no"
```

- Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.10/24"
connection.autoconnect: "yes"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth1.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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 in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y(X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.20
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
```

```
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.20
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.20
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.20
PREFIX=24
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2
vlan.parent eth1 vlan.id 2
```

- Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.20/24"
connection.autoconnect: "yes"
```

- Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.20/24"
connection.autoconnect: "no"
```

- Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.20/24"
connection.autoconnect: "no"
```

- Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.20/24"
connection.autoconnect: "yes"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth1.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

#### 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

#### 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

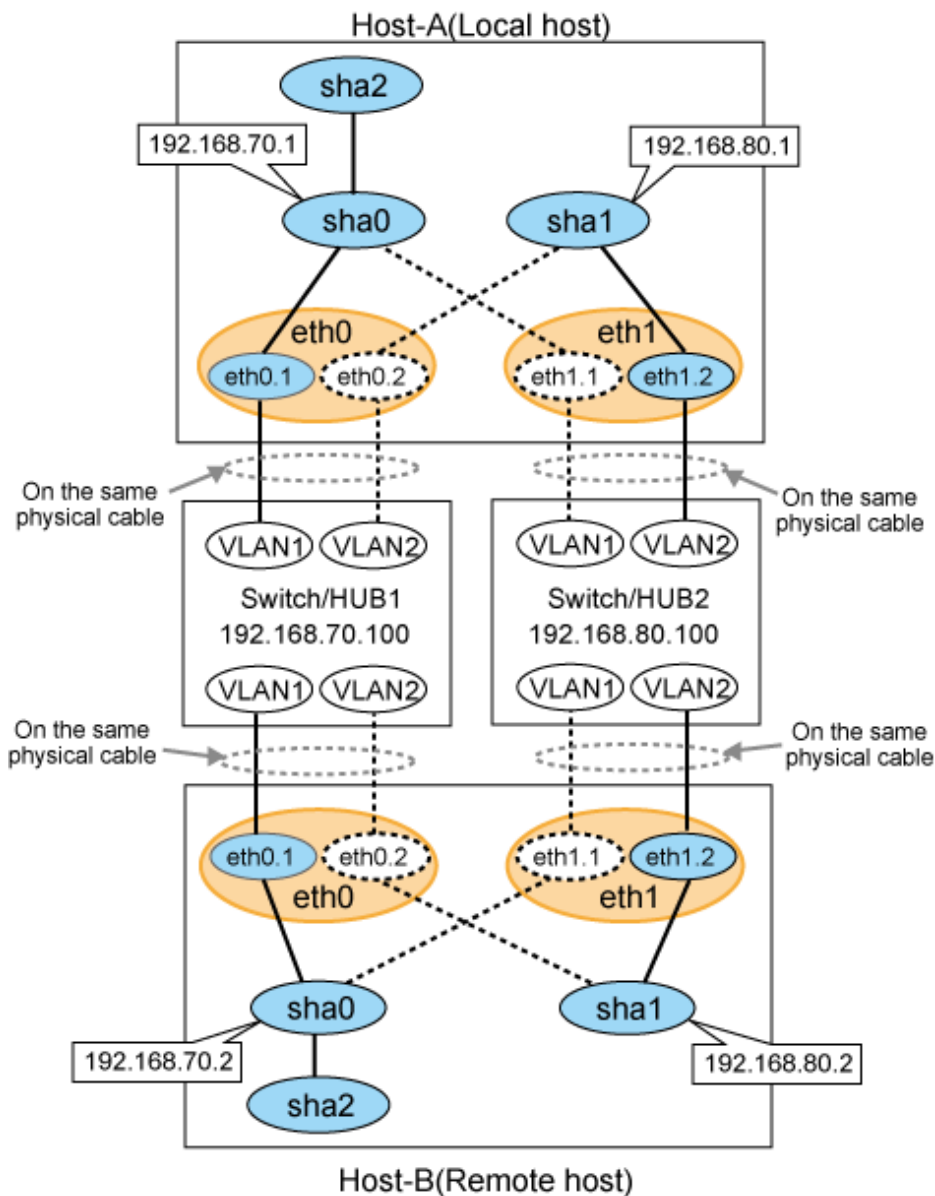
Run the following command and reboot the system.

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

## B.2.6 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

```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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



```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y(X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.1
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.1
PREFIX=24
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"  
ipv4.addresses:" "  
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"  
ipv4.addresses:" "  
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1  
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2  
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1  
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2  
vlan.parent eth1 vlan.id 2
```

- Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.70.1/24"  
connection.autoconnect: "yes"
```

- Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
connection.autoconnect: "no"
```

#### - Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "no"
```

#### - Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
connection.autoconnect: "yes"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth1.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-i' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y in RHLE8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 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

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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
DEVICE=eth1
ONBOOT=yes
```

1-3) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-ethX.Y(X is 0, 1. Y is 1, 2) file.

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=yes
```

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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.2
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.1

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=1
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1.2

```
VLAN=yes
TYPE=Vlan
PHYSDEV=eth1
VLAN_ID=2
BOOTPROTO=none
IPADDR=192.168.80.2
```

```
PREFIX=24
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"disabled"
ipv4.addresses:" "
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

1-3) Create a VLAN interface and set the following parameters for ethX.Y with the "nmcli connection add" command. (X is 0, 1. Y is 1, 2.)

- Create eth0.1

```
# /usr/bin/nmcli connection add type vlan con-name eth0.1 ifname eth0.1
vlan.parent eth0 vlan.id 1
```

- Create eth0.2

```
# /usr/bin/nmcli connection add type vlan con-name eth0.2 ifname eth0.2
vlan.parent eth0 vlan.id 2
```

- Create eth1.1

```
# /usr/bin/nmcli connection add type vlan con-name eth1.1 ifname eth1.1
vlan.parent eth1 vlan.id 1
```

- Create eth1.2

```
# /usr/bin/nmcli connection add type vlan con-name eth1.2 ifname eth1.2
vlan.parent eth1 vlan.id 2
```

- Configuration of eth0.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth0.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
connection.autoconnect: "no"
```

- Configuration of eth1.1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "no"
```

- Configuration of eth1.2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
connection.autoconnect: "yes"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0.1 and eth1.2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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 192.168.80.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option "-i" is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX.Y in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 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

Define only one Standby patrol monitoring function.

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha2 -m p -t sha0
```

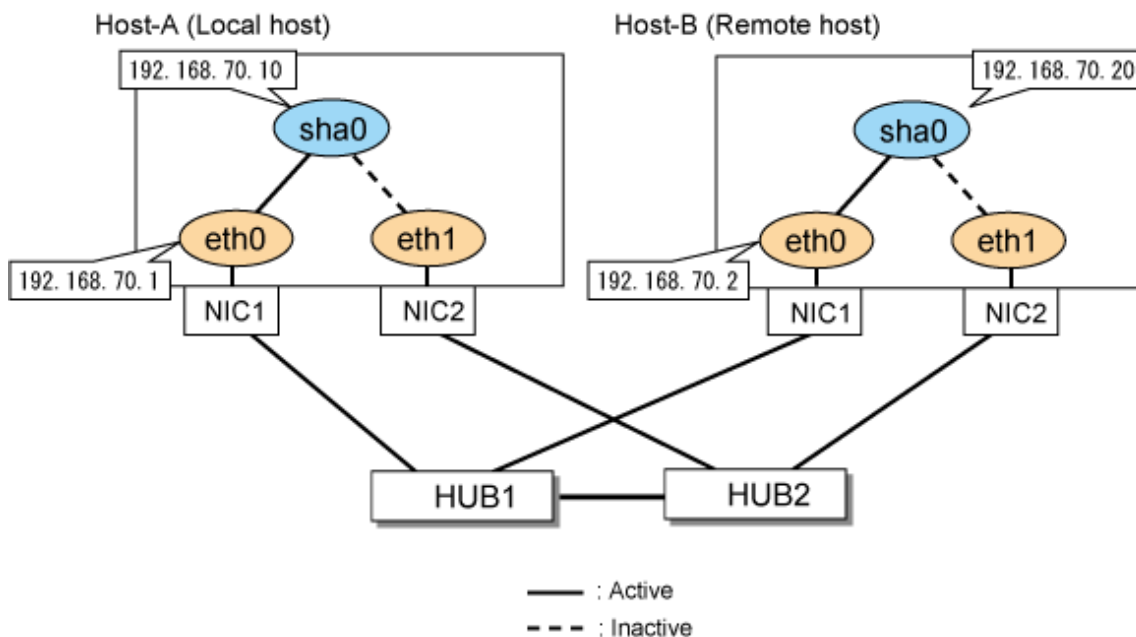
## 7) Reboot

Run the following command and reboot the system.

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

## B.2.7 Example of the Single system without IP address setting of monitoring target

This section describes an example configuration procedure of the network shown in the diagram below.



### [HOST-A]

#### 1) Setting up the system

Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

- For RHEL8

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.1/24"  
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.1/24"  
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.10 -e 192.168.70.1 -t eth0,eth1
```

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p _none_
```

## 6) Reboot

Run the following command to reboot the system.

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

## [HOST-B]

### 1) Setting up the system

Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

- For RHEL8
- Contents of /etc/sysconfig/network-scripts/ifcfg-eth0

```
TYPE=Ethernet  
BOOTPROTO=none  
IPADDR=192.168.70.2  
PREFIX=24  
DEVICE=eth0  
ONBOOT=yes
```



- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.20 -e 192.168.70.2 -t eth0,eth1
```

## 5) Setting up the HUB monitoring function

```
/opt/FJSSVhanet/usr/sbin/hanetpoll create -n sha0 -p _none_
```

## 6) Reboot

Run the following command to reboot the system.

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

## B.2.8 Example of the Cluster system (1:1 Standby)

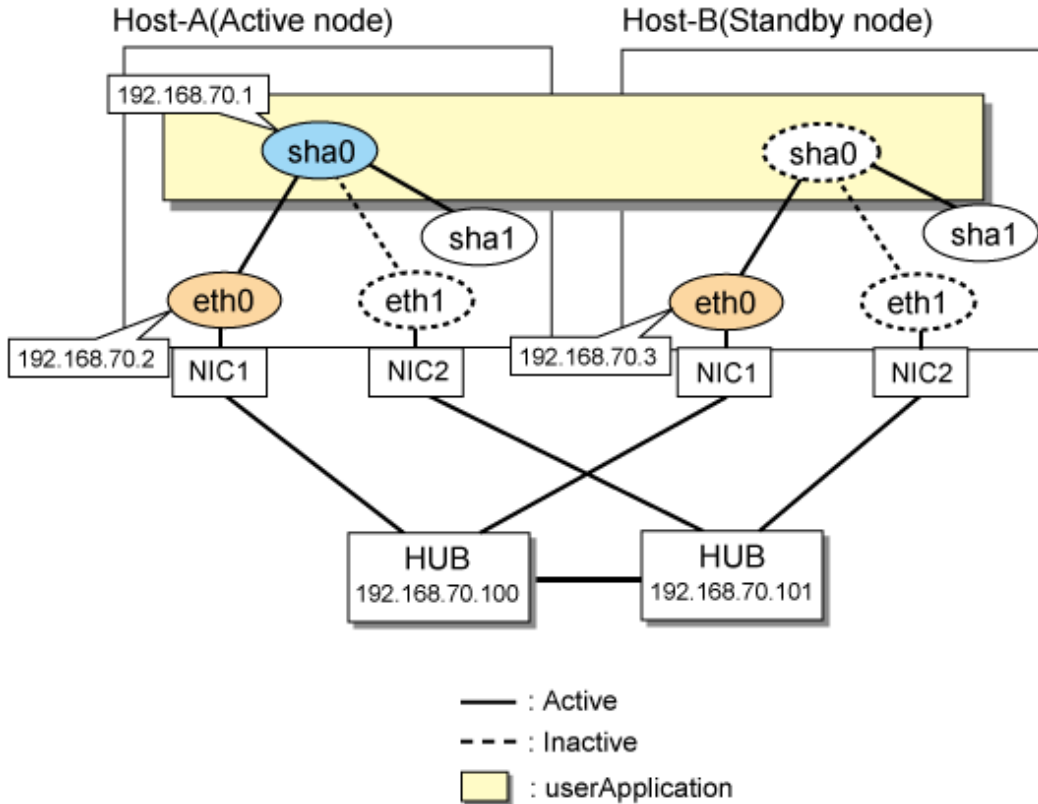
This section describes an example configuration procedure of the network shown in the diagram below.

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 address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) Creating a takeover virtual interface

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

## 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) Creating a takeover virtual interface

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

## 8) 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.2.9 Example of the Cluster system (Mutual standby) without NIC sharing

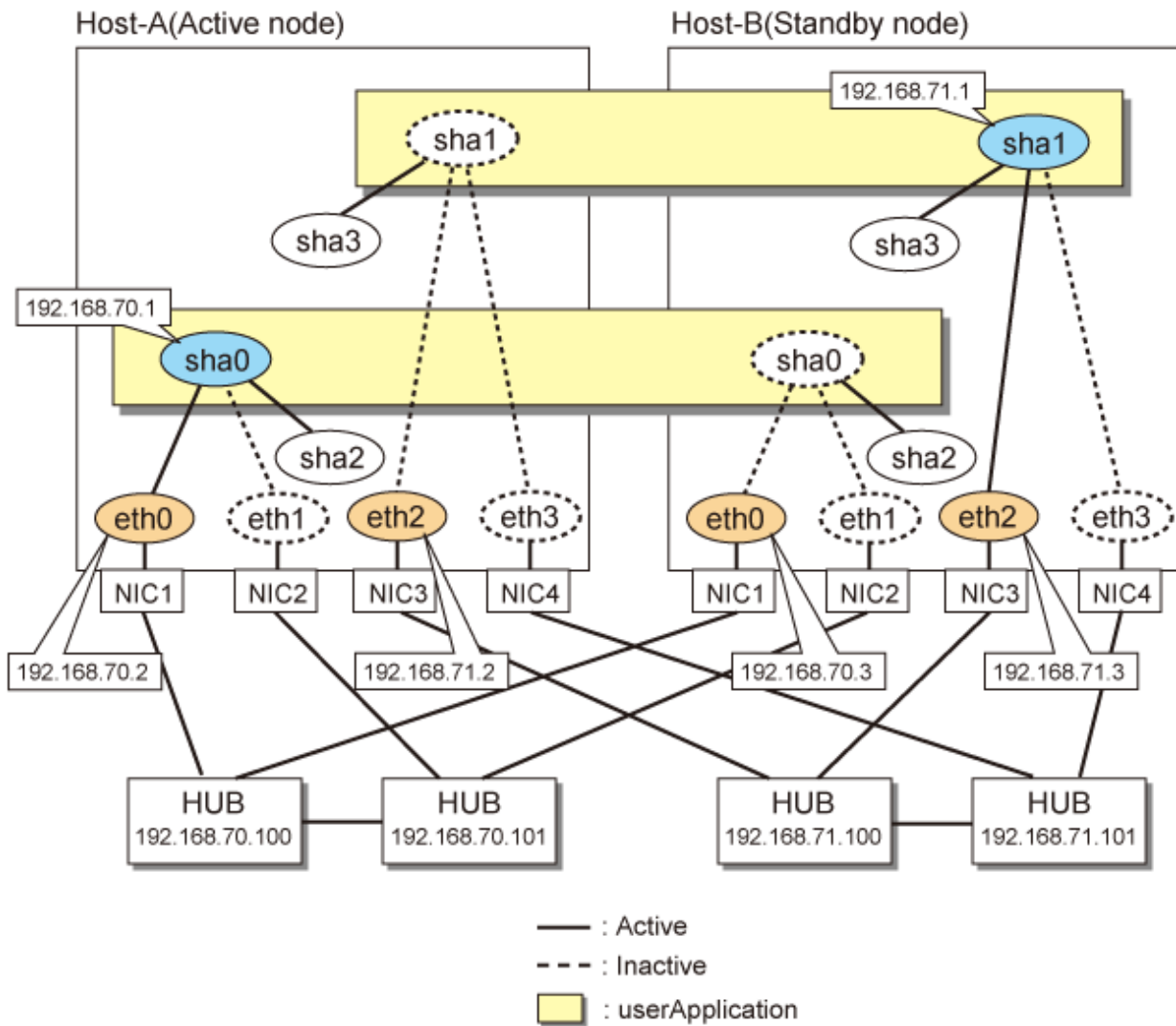
This section describes an example configuration procedure of the network shown in the diagram below.

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

```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1, 2, 3) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none

```

```
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
DEVICE=eth2
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
DEVICE=eth3
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "no"
```

- Configuration of eth2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth3

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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
```

## 4) Creating virtual interfaces

```
/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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/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 takeover virtual interfaces

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1, 2, 3) file as follows.



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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth2

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.3
PREFIX=24
DEVICE=eth2
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth3

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.3
PREFIX=24
DEVICE=eth3
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "no"
```

- Configuration of eth2

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

#### - Configuration of eth3

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth2 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) 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
```

## 4) Creating virtual interfaces

```
/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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/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 takeover virtual interfaces

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## 8) 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.2.10 Example of the Cluster system (Mutual standby) with NIC sharing

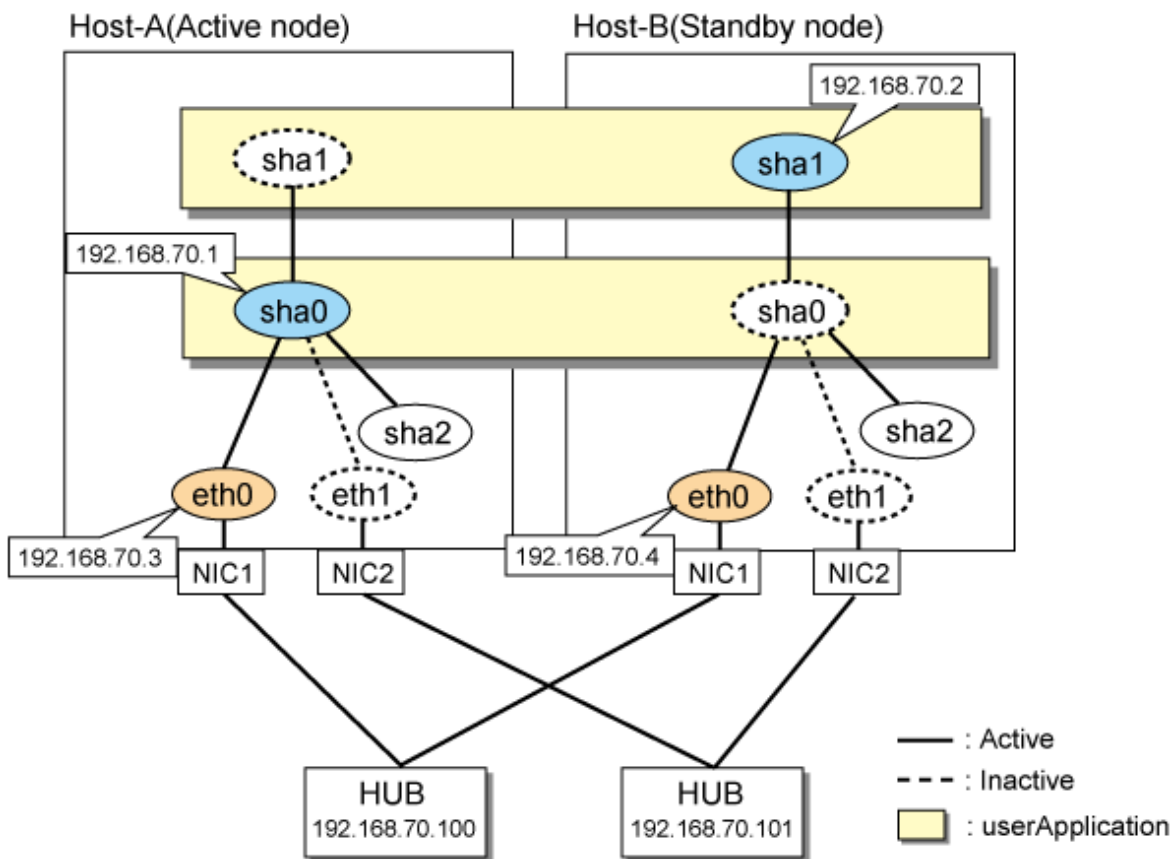
This section describes an example configuration procedure of the network shown in the diagram below.

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
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/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 takeover virtual interfaces

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

### 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"yes"
```

#### - Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating virtual interfaces

```
/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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
/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 stakeover virtual interfaces

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## 8) 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.2.11 Example of the Cluster system in Takeover physical IP address (pattern I)

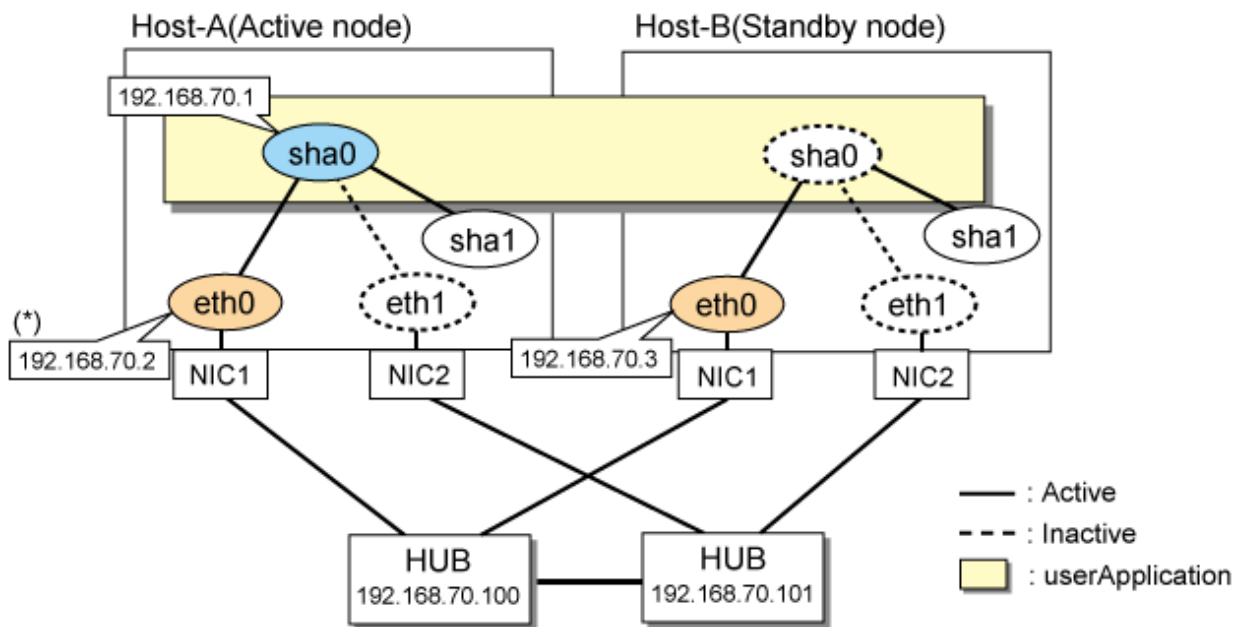
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for enabling physical interface on a standby node.)

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 address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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
```



## Note

Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 7) Creating a takeover virtual interface

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

### 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.3/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.3/24"  
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) Creating a takeover virtual interface

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

## 8) 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 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.2.12 Example of the Cluster system in Takeover physical IP address (pattern II)

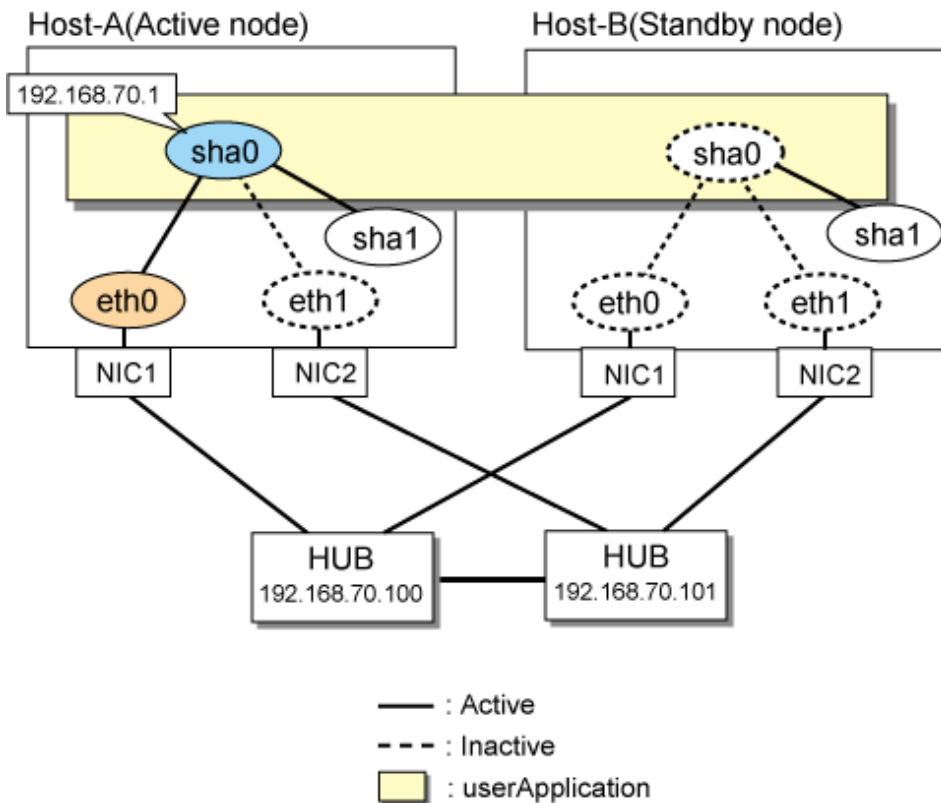
This section describes an example configuration procedure of the network shown in the diagram below. (Network configuration for not enabling physical interface on a standby node.)

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 address)
192.168.70.100 swhub1  # Primary HUB IP
192.168.70.101 swhub2  # Secondary HUB IP
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.1/24"
connection.autoconnect:"no"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.1/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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) Creating a takeover virtual interface

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

## 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=no
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.1/24"
connection.autoconnect:"no"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.1/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

### 3) Setting a subnet mask

```
/opt/FJShanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creating a 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) Creating a takeover virtual interface

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

### 8) 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.2.13 Example of the Cluster system (Cascade)

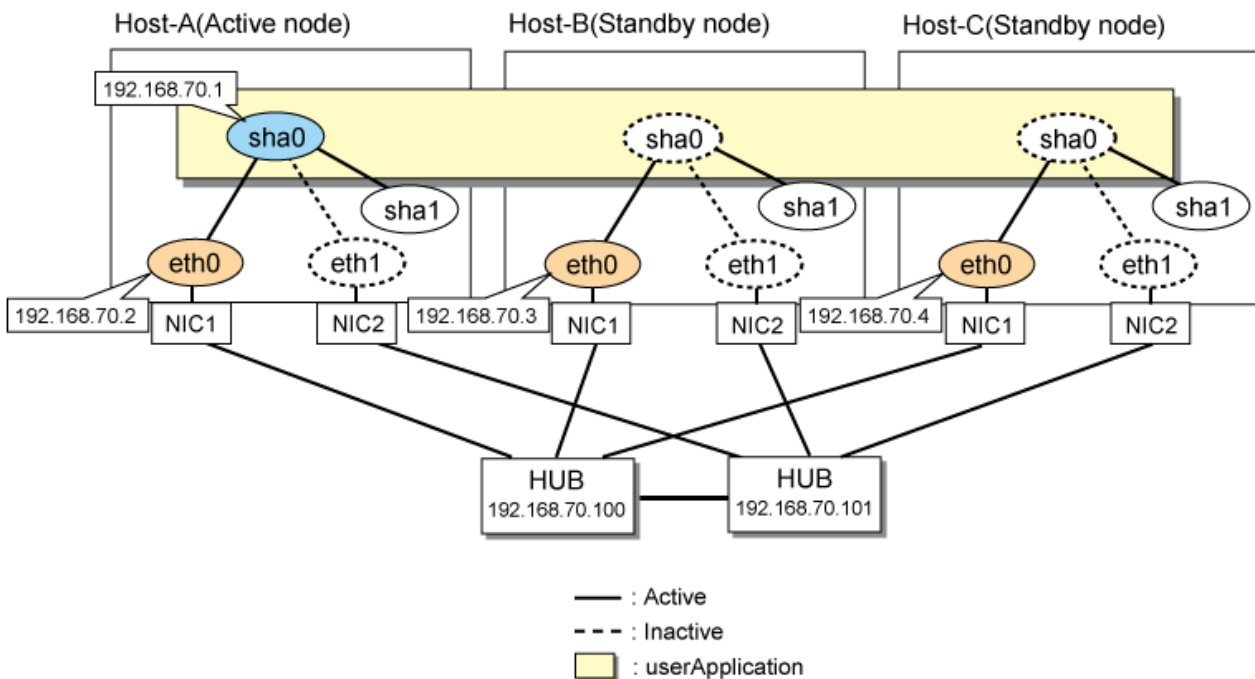
This section describes an example configuration procedure of the network shown in the diagram below.

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 address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.4    host31   # HOST-C Physical IP
192.168.70.100  swhub1   # Primary HUB IP
192.168.70.101  swhub2   # Secondary HUB IP
```

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

### 4) Creating a 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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

### 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

### 7) Creating a takeover virtual interface

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

### 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.3
PREFIX=24
DEVICE=eth1
ONBOOT=no
```



- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.3/24"  
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.3/24"  
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

## 7) Creating a takeover virtual interface

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

## 8) 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.

- For RHEL8

1-2) Configure /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.4
PREFIX=24
DEVICE=eth1
ONBOOT=no
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.4/24"
connection.autoconnect:"no"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

### 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

#### 4) Creating a 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
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-ethX in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

#### 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

#### 6) Setting up the Standby patrol monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha1 -m p -t sha0
```

#### 7) Creating a takeover virtual interface

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

#### 8) 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 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.2.14 Example of the Cluster system (NIC non-redundant)

---

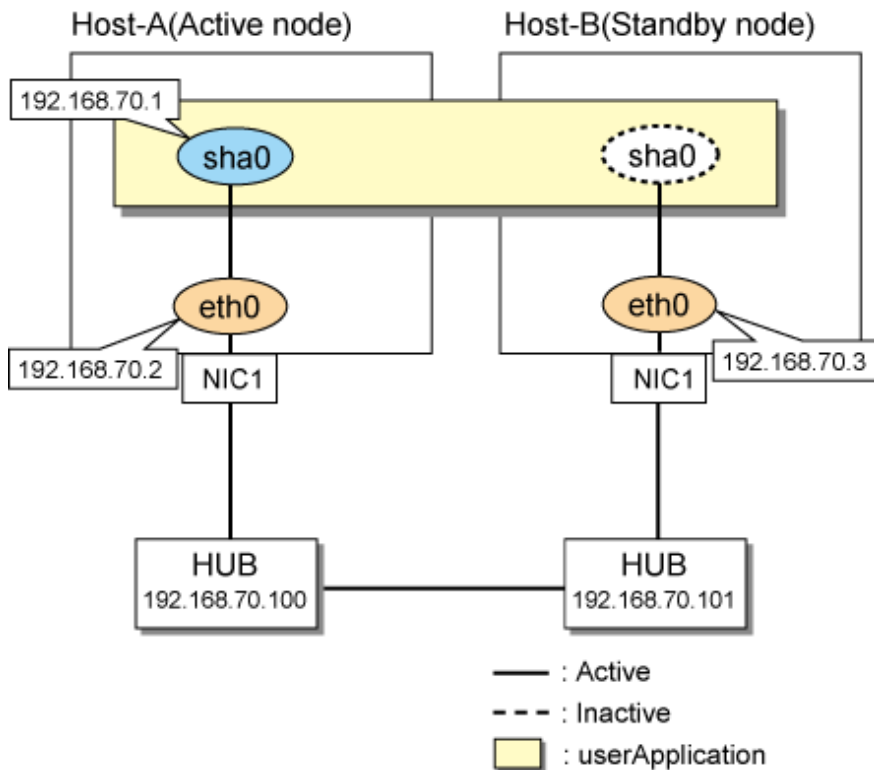
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /etc/hosts file.

```
192.168.70.1    hosta    # HOST-A/B Virtual IP (Takeover IP address)
192.168.70.2    host11   # HOST-A Physical IP
192.168.70.3    host21   # HOST-B Physical IP
192.168.70.100 swhub1  # Primary HUB IP
192.168.70.101 swhub2  # Secondary HUB IP
```

- For RHEL8

1-2) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-eth0 file.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.2/24"
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for eth0 with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes".

```
connection.type: "802-3-ethernet"  
connection.id: "eth0"  
connection.interface-name: "eth0"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a 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 in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Creating a takeover virtual interface

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

## 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 the /etc/hosts file. Defined content is same as HOST-A.

- For RHEL8

1-2) Describe the IP address defined in the above in the /etc/sysconfig/network-scripts/ifcfg-eth0 file.

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

```
TYPE=Ethernet  
BOOTPROTO=none  
IPADDR=192.168.70.3  
PREFIX=24  
DEVICE=eth0  
ONBOOT=yes
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.3/24"  
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for eth0 with the nmcli connection show command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"  
connection.id: "eth0"  
connection.interface-name: "eth0"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.1 -e 192.168.70.3 -t eth0
```



Ensure that the physical IP address specified using option '-e' is the same IP address configured in /etc/sysconfig/network-scripts/ifcfg-eth0 in RHEL8 or in the "nmcli connection modify" command in RHEL9. In RHEL8 or later, to correct mismatch of IP addresses, GLS automatically rewrites the configuration of the connection profile based on the IP address specified in the GLS command.

## 5) Setting up the HUB monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpoll create -n sha0 -p 192.168.70.100,192.168.70.101 -b off
```

## 6) Creating a takeover virtual interface

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

## 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

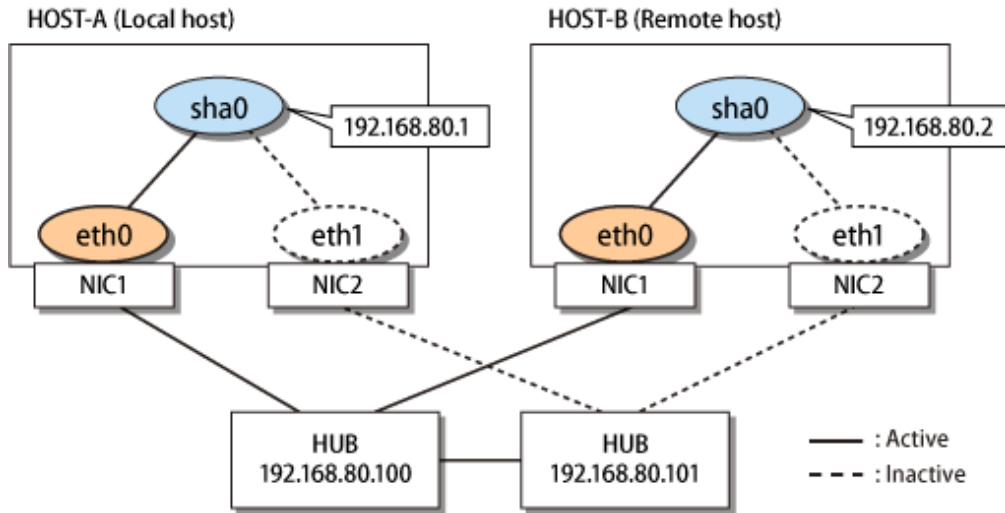
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## B.3 Example of configuring Virtual NIC mode (IPv4)

### B.3.1 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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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



```

DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"

```

#### 4) Setting the network monitoring function

```
/opt/FJSSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

#### 5) Reboot

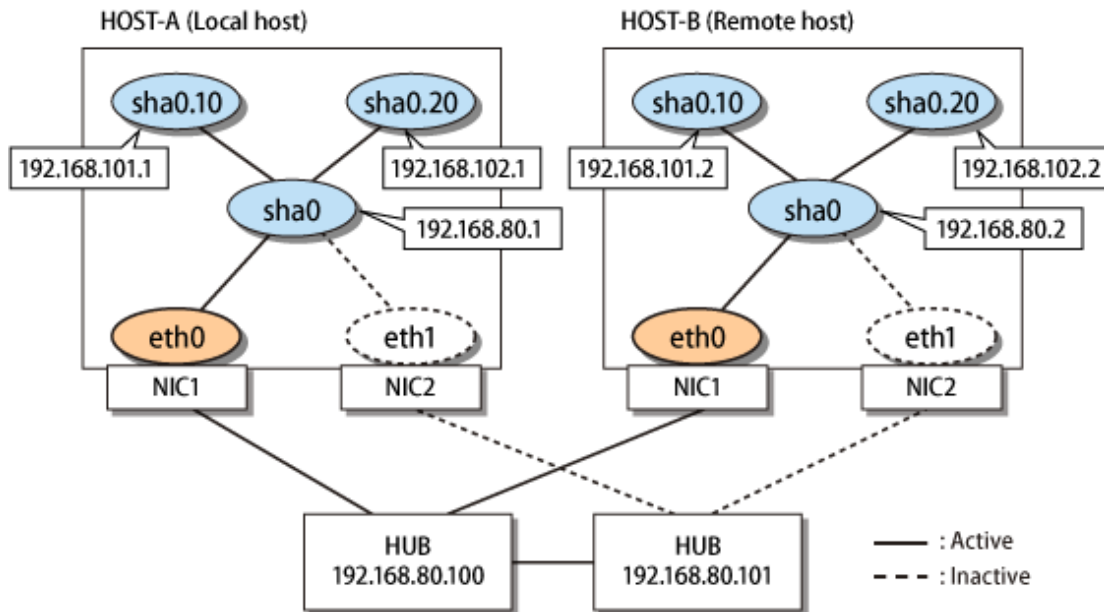
Run the following command to reboot the system.

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

## B.3.2 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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Creating a virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
```

#### 4) Setting the network monitoring function

```
/opt/FJShanet/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:

- For RHEL8

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.10

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=10
BOOTPROTO=none
IPADDR=192.168.101.1
PREFIX=24
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.20

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=20
BOOTPROTO=none
IPADDR=192.168.102.1
PREFIX=24
```

- For RHEL9

- Configuration of sha0.10

Create sha0.10 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "sha0.10"
connection.interface-name: "sha0.10"
connection.type: "vlan"
connection.autoconnect: "yes"
vlan.parent: "sha0"
vlan.id: "10"
ipv4.method: "manual"
ipv4.addresses: "192.168.101.1/24"
```

- Configuration of sha0.20

Create sha0.20 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "sha0.20"
connection.interface-name: "sha0.20"
connection.type: "vlan"
connection.autoconnect: "yes"
vlan.parent: "sha0"
vlan.id: "20"
ipv4.method: "manual"
ipv4.addresses: "192.168.102.1/24"
```

#### 6) Setting /etc/NetworkManager/NetworkManager.conf

Describe the tagged VLAN interfaces, which are set in step 5), in /etc/NetworkManager/NetworkManager.conf.

- Contents of /etc/NetworkManager/NetworkManager.conf

```
[main]
...
ignore-carrier=sha0.10, sha0.20
```

## Note

The setting of `/etc/NetworkManager/NetworkManager.conf` is required to control the processing of NetworkManager for tagged VLAN interfaces and manage the processing in GLS. Make sure to set `/etc/NetworkManager/NetworkManager.conf`.

## 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 the `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the `/etc/sysconfig/network-scripts/ifcfg-sha0` file.

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

```
DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
```

### 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:

- For RHEL8

- Contents of `/etc/sysconfig/network-scripts/ifcfg-sha0.10`

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=10
```

```
BOOTPROTO=none
IPADDR=192.168.101.2
PREFIX=24
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-sha0.20

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=20
BOOTPROTO=none
IPADDR=192.168.102.2
PREFIX=24
```

- For RHEL9

- Configuration of sha0.10

Create sha0.10 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "sha0.10"
connection.interface-name: "sha0.10"
connection.type: "vlan"
connection.autoconnect: "yes"
vlan.parent: "sha0"
vlan.id: "10"
ipv4.method: "manual"
ipv4.addresses: "192.168.101.2/24"
```

- Configuration of sha0.20

Create sha0.20 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "sha0.20"
connection.interface-name: "sha0.20"
connection.type: "vlan"
connection.autoconnect: "yes"
vlan.parent: "sha0"
vlan.id: "20"
ipv4.method: "manual"
ipv4.addresses: "192.168.102.2/24"
```

## 6) Setting /etc/NetworkManager/NetworkManager.conf

Describe the tagged VLAN interfaces, which are set in step 5), in /etc/NetworkManager/NetworkManager.conf.

- Contents of /etc/NetworkManager/NetworkManager.conf

```
[main]
...
ignore-carrier=sha0.10, sha0.20
```

### Note

The setting of /etc/NetworkManager/NetworkManager.conf is required to control the processing of NetworkManager for tagged VLAN interfaces and manage the processing in GLS. Make sure to set /etc/NetworkManager/NetworkManager.conf.

## 7) Reboot

Run the following command to reboot the system.

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

### B.3.3 Example of the Cluster system (1:1 Standby)

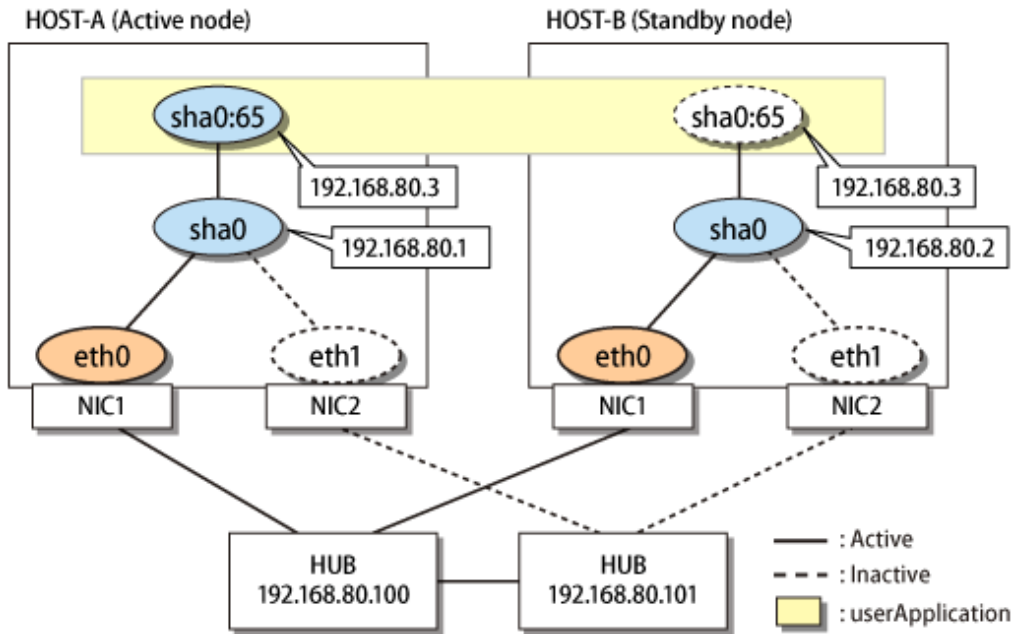
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"  
ipv6.method: "disabled"  
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0  
IPADDR=192.168.80.1  
PREFIX=24  
BOOTPROTO=none  
ONBOOT=yes  
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.80.1/24"
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the `/etc/sysconfig/network-scripts/ifcfg-sha0` file.

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

```
DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to `sha0` with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
```

## 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.3.4 Example of the Cluster system (Mutual Standby)

---

This section describes an example configuration procedure of the network shown in the diagram below.

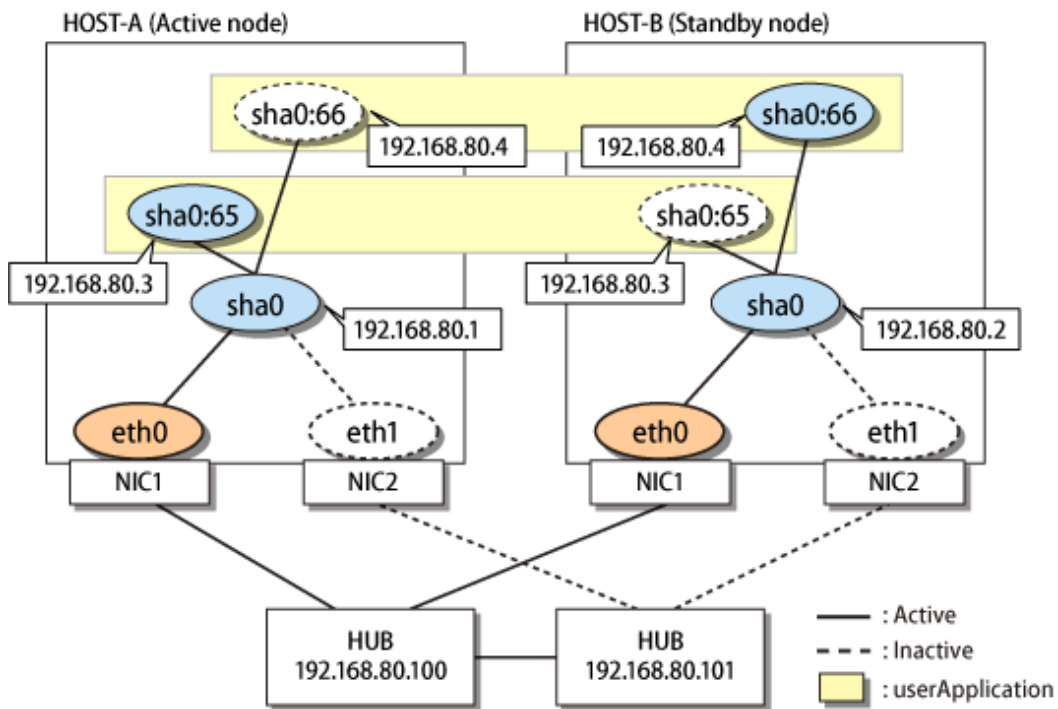
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
```

## 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 takeover virtual interfaces

```
/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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the `/etc/sysconfig/network-scripts/ifcfg-sha0` file.

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

```
DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
```

### 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 takeover virtual interfaces

```
/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.3.5 Example of the Cluster system (Cascade)

---

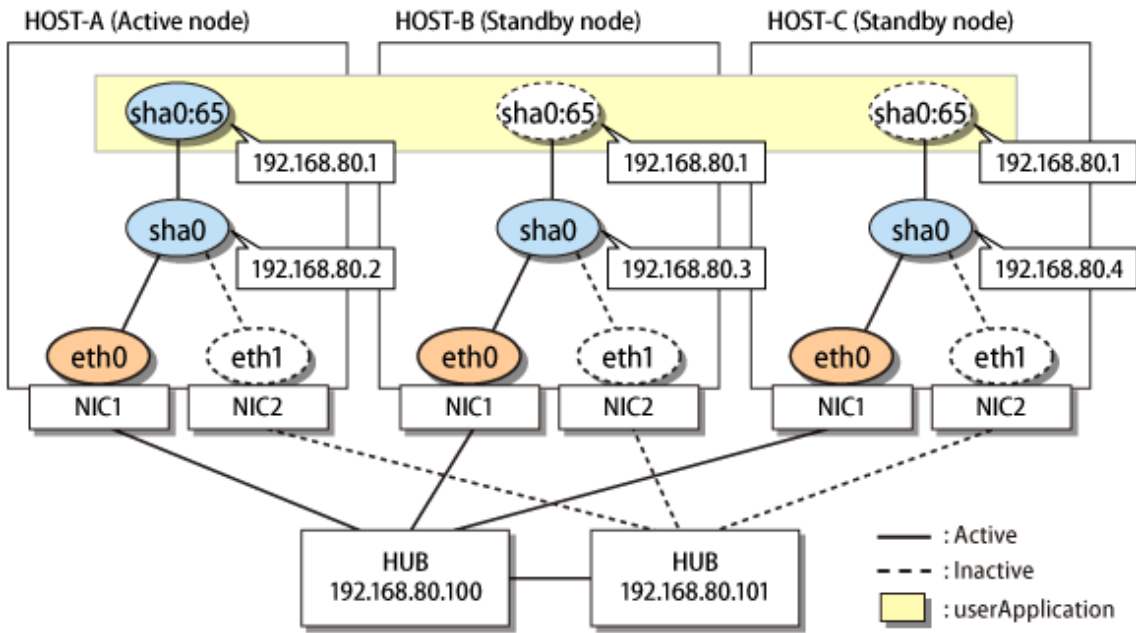
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing "[3.2.2.1 Setup common to modes.](#)"

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.3
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.3/24"
```

#### 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.4
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.80.4/24"

```

#### 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 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 (No IP takeover)

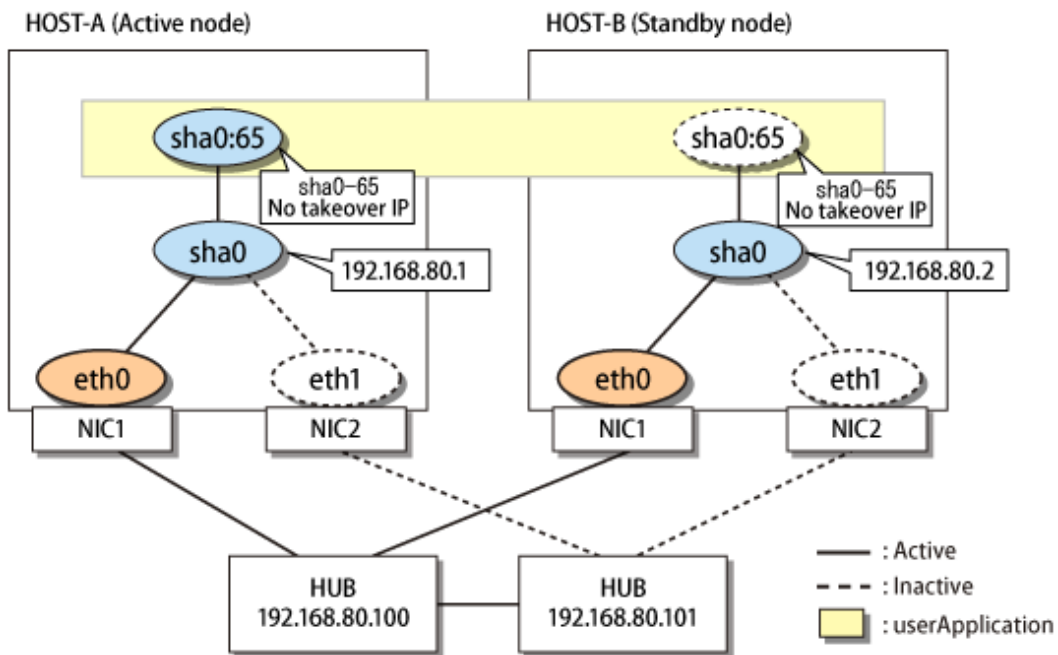
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /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
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

### 2) Creating a virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

### 3) Setting an IP address and a subnet mask

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```



- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.80.1/24"
```

#### 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0  
IPADDR=192.168.80.2  
PREFIX=24  
BOOTPROTO=none  
ONBOOT=yes  
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.80.2/24"
```

#### 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 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

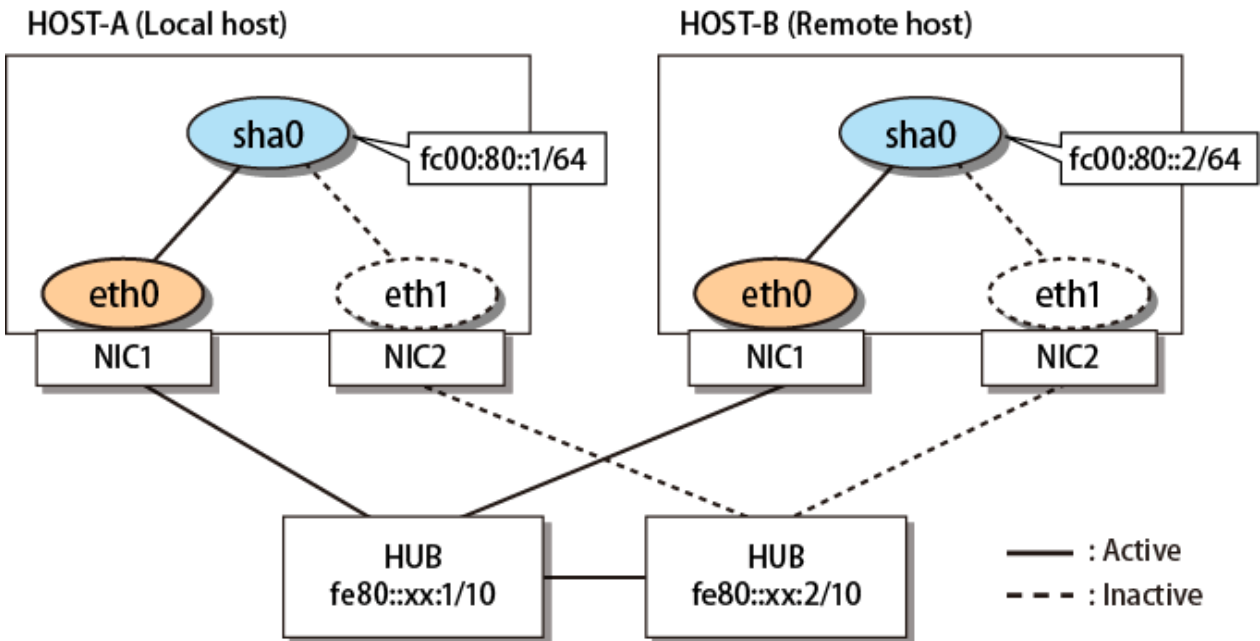
After completing the configuration, start the userApplication to activate the takeover virtual interface on the operation node.

## B.4 Example of configuring Virtual NIC mode (IPv6)

### B.4.1 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 the /etc/hosts file.

```
fc00:80::1      v6hosta      # HOST-A Virtual IP
fc00:80::2      v6hostb      # HOST-B Virtual IP
fe80::xx:1      swhub1       # Primary HUB IP
fe80::xx:2      swhub2       # Secondary HUB IP
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
```

```
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Creating a virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address

- For RHEL8

Define an IP address or other entries in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fc00:80::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv6.method: "manual"
ipv6.addresses: "fc00:80::1/64"
```

## 4) Setting the network monitoring function

```
/opt/FJShanet/usr/sbin/hanetpathmon target -n sha0 -p fe80::xx:1,fe80::xx:2
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or other entries in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fc00:80::2/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv6.method: "manual"
ipv6.addresses: "fc00:80::2/64"
```

## 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p fe80::xx:1,fe80::xx:2
```

## 5) Reboot

Run the following command to reboot the system.

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

## B.4.2 Example of the Cluster system (1:1 Standby)

---

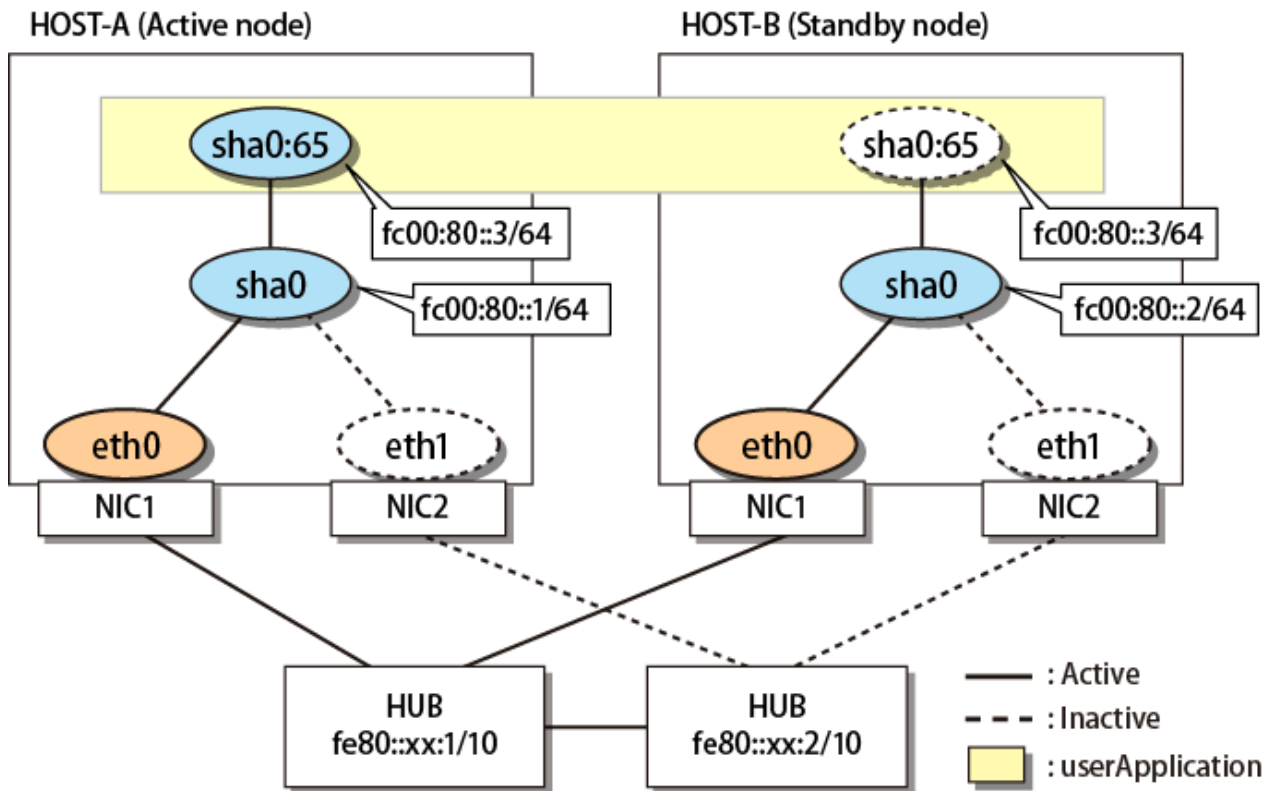
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /etc/hosts file.

```
fc00:80::1    v6hosta    # HOST-A Virtual IP
fc00:80::2    v6hostb    # HOST-B Virtual IP
fc00:80::3    v6host1    # HOST-A/B (Takeover virtual IP)
fe80::xx:1    swhub1     # Primary HUB IP
fe80::xx:2    swhub2     # Secondary HUB IP
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address

- For RHEL8

Define an IP address or other entries in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fc00:80::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv6.method: "manual"
ipv6.addresses: "fc00:80::1/64"
```

## 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p fe80::xx:1,fe80::xx:2
```

## 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fc00:80::3/64
```

## 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or other entries in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPV6INIT=yes
IPV6ADDR=fc00:80::2/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv6.method: "manual"
ipv6.addresses: "fc00:80::2/64"
```

#### 4) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p fe80::xx:1,fe80::xx:2
```

#### 5) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i fc00:80::3/64
```

#### 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 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 Virtual NIC mode (IPv4/IPv6)

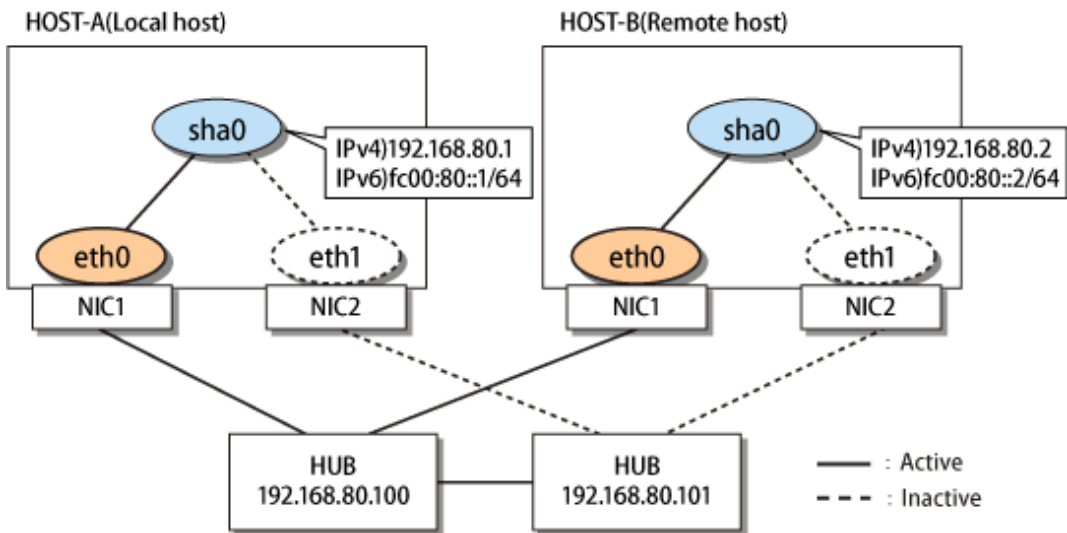
---

### B.5.1 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 the /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
fc00:80::1     v6hosta  # HOST-A Virtual IP
fc00:80::2     v6hostb  # HOST-B Virtual IP
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)



```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 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

- For RHEL8

Define an IP address or a subnet mask in the `/etc/sysconfig/network-scripts/ifcfg-sha0` file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
IPV6INIT=yes
IPV6ADDR=fc00:80::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to `sha0` with the `"nmcli connection modify"` command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
ipv6.method: "manual"
ipv6.addresses: "fc00:80::1/64"
```

## 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 the `/etc/hosts` file. Defined content is same as HOST-A.

1-2) Edit `ethX` (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the `/etc/sysconfig/network-scripts/ifcfg-sha0` file.

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

```
DEVICE=sha0
IPADDR=192.168.80.2
PREFIX=24
```

```

IPV6INIT=yes
IPV6ADDR=fc00:80::2/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.80.2/24"
ipv6.method: "manual"
ipv6.addresses: "fc00:80::2/64"

```

#### 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.5.2 Example of the Cluster system (1:1 Standby)

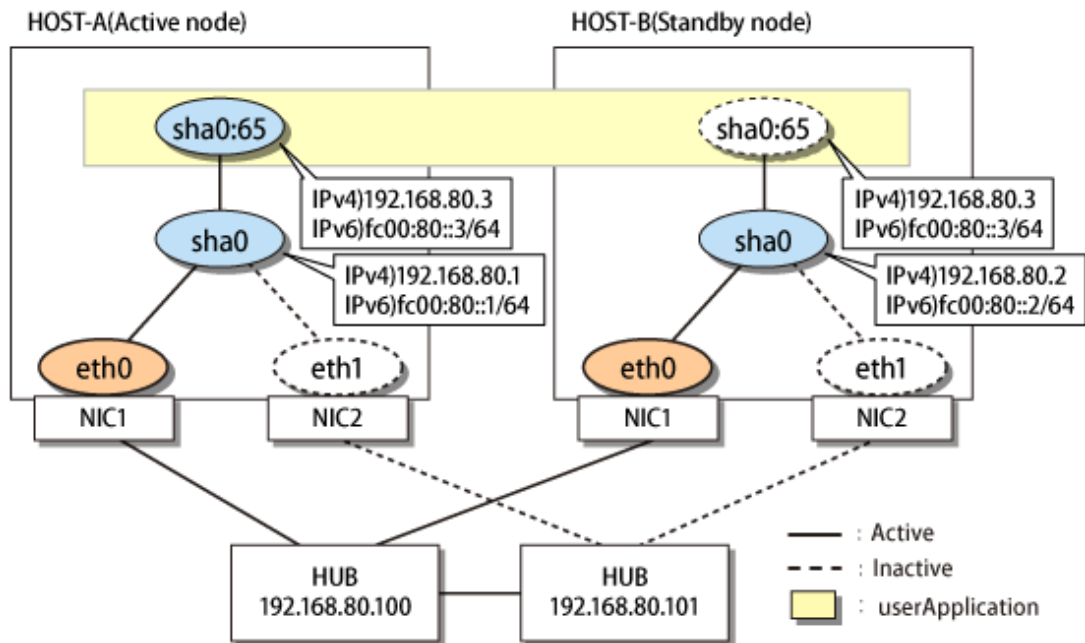
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /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
fc00:80::1     v6hosta  # HOST-A Virtual IP
fc00:80::2     v6hostb  # HOST-B Virtual IP
fc00:80::3     v6host1  # HOST-A/B (Takeover virtual IP)

```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes

```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```

ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"

```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```

connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"

```

## 2) Creating a virtual interface

```
/opt/FJShanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting an IP address and a subnet mask

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```

DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
IPV6INIT=yes
IPV6ADDR=fc00:80::1/64
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.80.1/24"  
ipv6.method: "manual"  
ipv6.addresses: "fc00:80::1/64"
```

#### 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,fc00:80::3/64
```

#### 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 the /etc/hosts file. Defined content is same as HOST-A.

1-2) Edit ethX (X is 0, 1). 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

- For RHEL8

Define an IP address or a subnet mask in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0  
IPADDR=192.168.80.2  
PREFIX=24  
IPV6INIT=yes  
IPV6ADDR=fc00:80::2/64  
BOOTPROTO=none  
ONBOOT=yes  
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"  
ipv4.addresses: "192.168.80.2/24"  
ipv6.method: "manual"  
ipv6.addresses: "fc00:80::2/64"
```

#### 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,fc00:80::3/64
```

### 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 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.

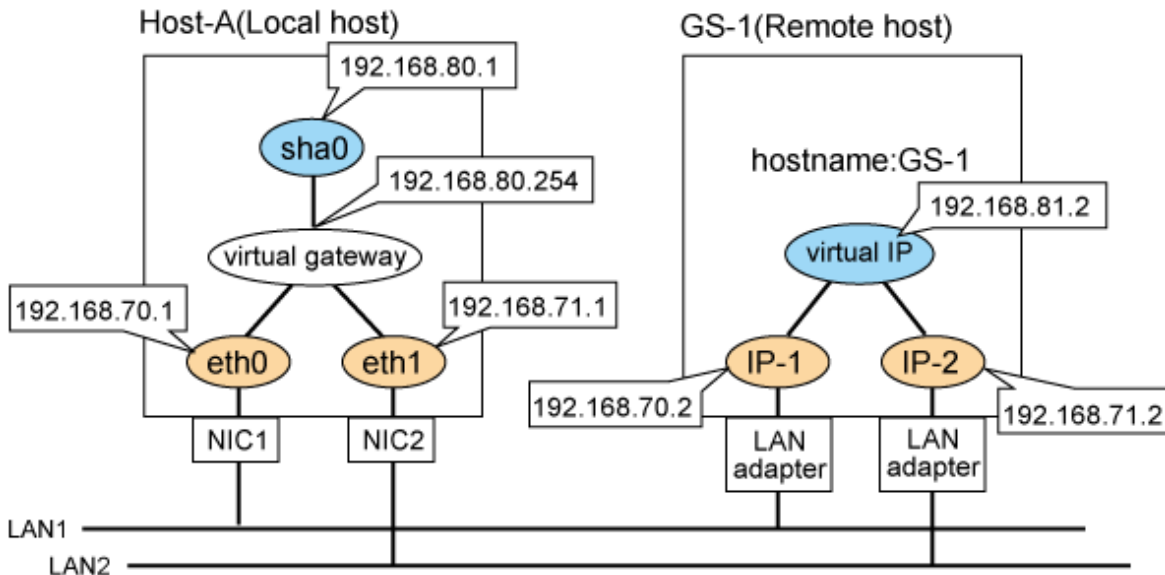
## B.6 Example of configuring GS linkage mode

### B.6.1 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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes

```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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

```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"

```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"

```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"  
connection.id: "ethX"  
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload  
/usr/bin/nmcli connection up eth0  
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a 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) Reboot

Run the following command to reboot the system.

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

## [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.

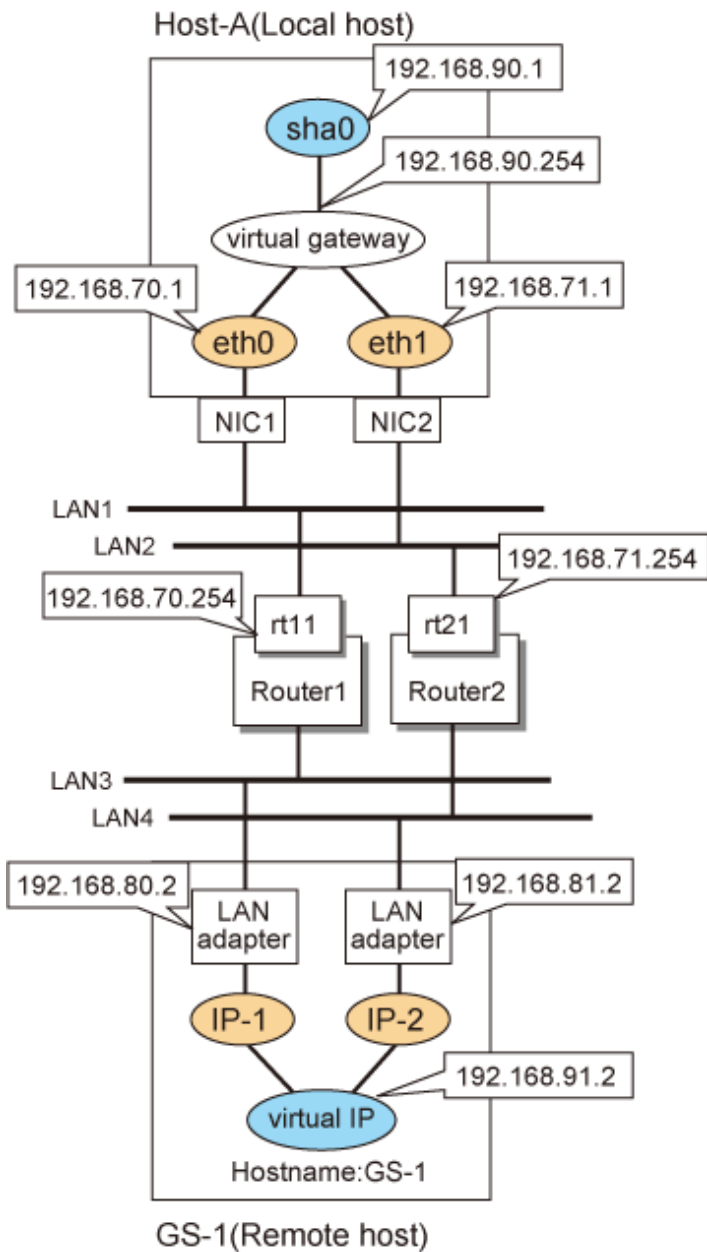
## B.6.2 Example of the Single system on remote network

---

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 the /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
```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.



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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) 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 the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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)
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
ipv4.routes: "192.168.80.0/24 192.168.70.254"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
```

```
ipv4.routes: "192.168.81.0/24 192.168.71.254"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

**2) Reflecting system setting**

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

**3) Setting a subnet mask**

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.90.0 -m 255.255.255.0
```

**4) Creating a 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) Reboot**

Run the following command to reboot the system.

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

**[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.

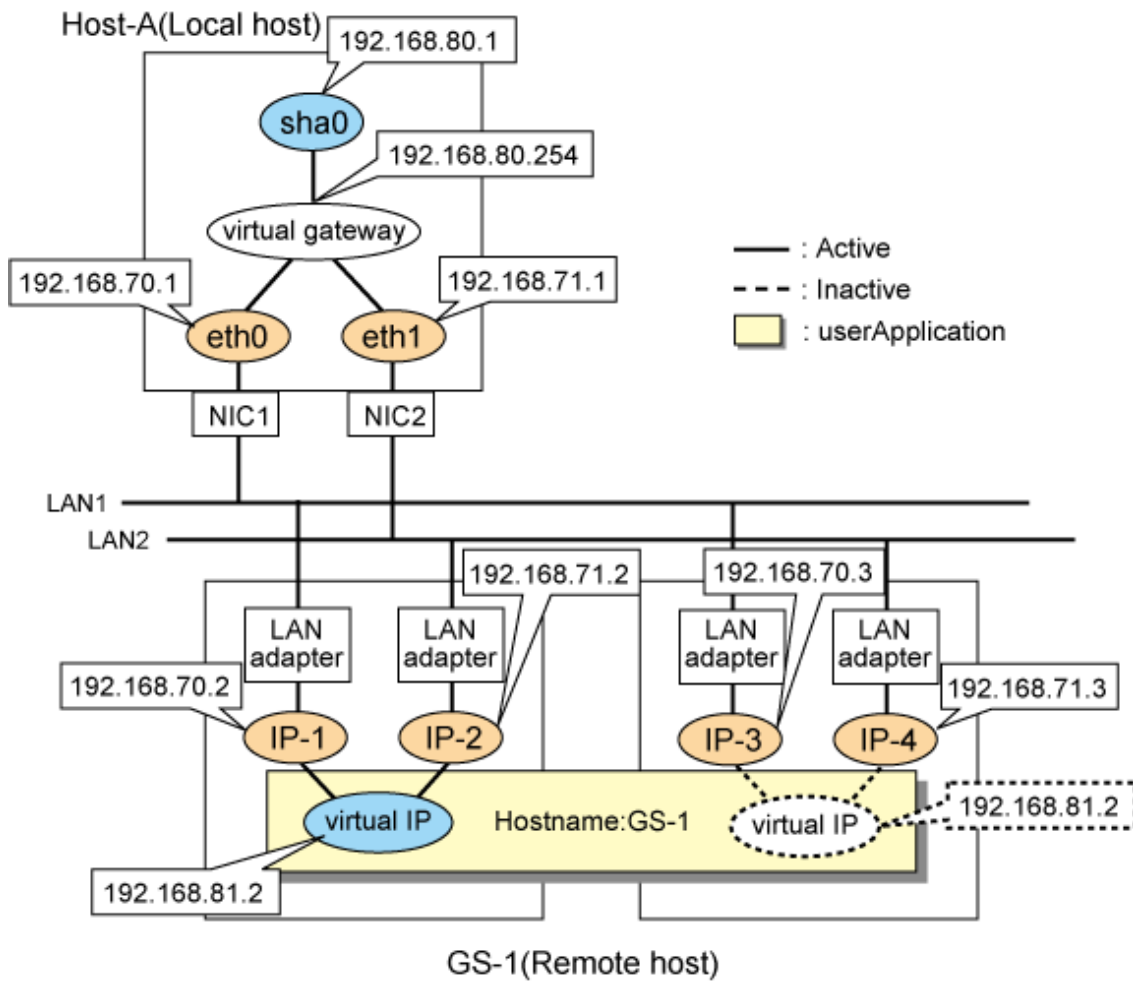
**B.6.3 Example of the Single system (GS Hot-standby)**

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a 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) Reboot

Run the following command to reboot the system.

```

/sbin/shutdown -r now

```

## [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.

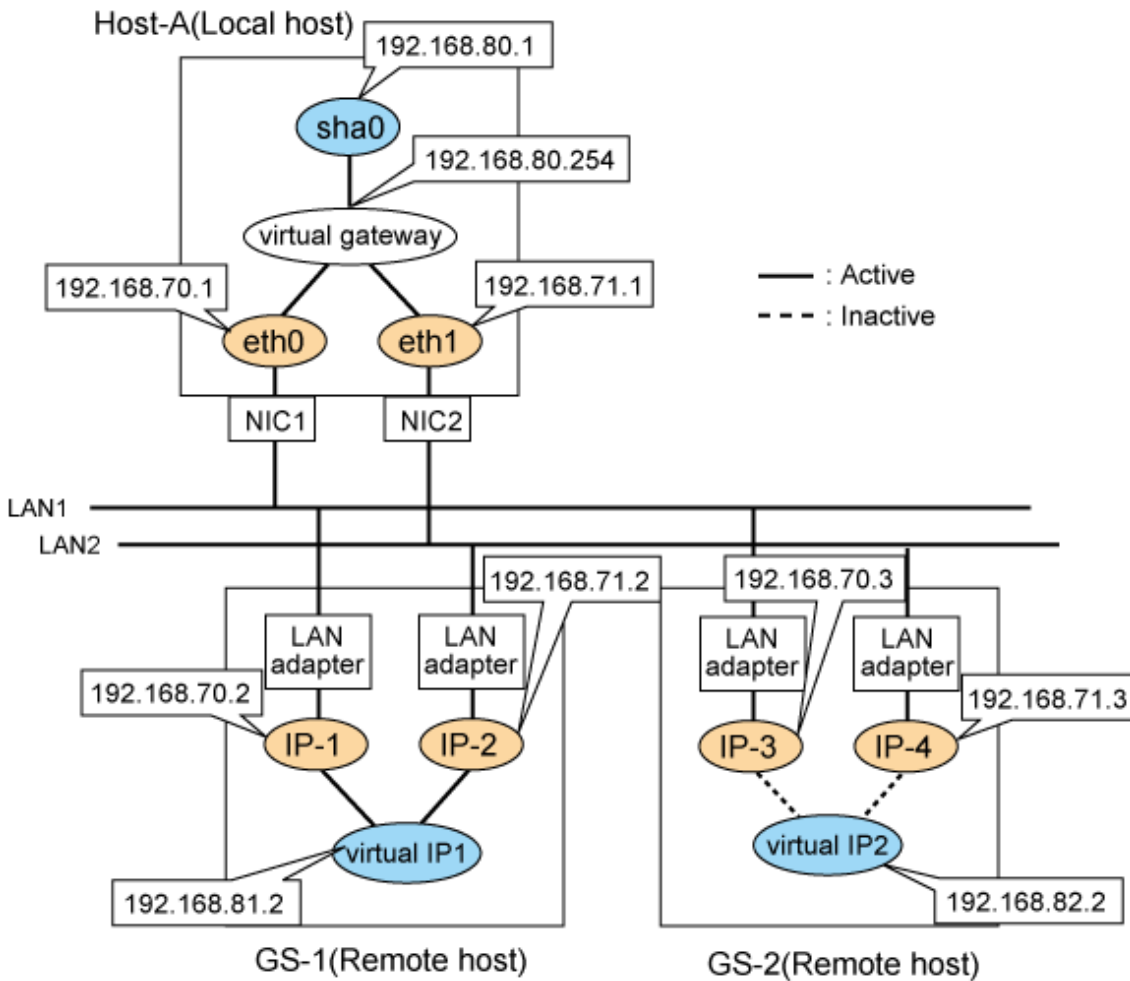
## B.6.4 Example of the Single system (GS Load Sharing)

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 the /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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes

```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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

```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```

ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"

```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a 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) Reboot

Run the following command to reboot the system.

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

## [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.6.5 Example of the Cluster system (1:1 Standby)

---

This section describes an example configuration procedure of the network shown in the diagram below.

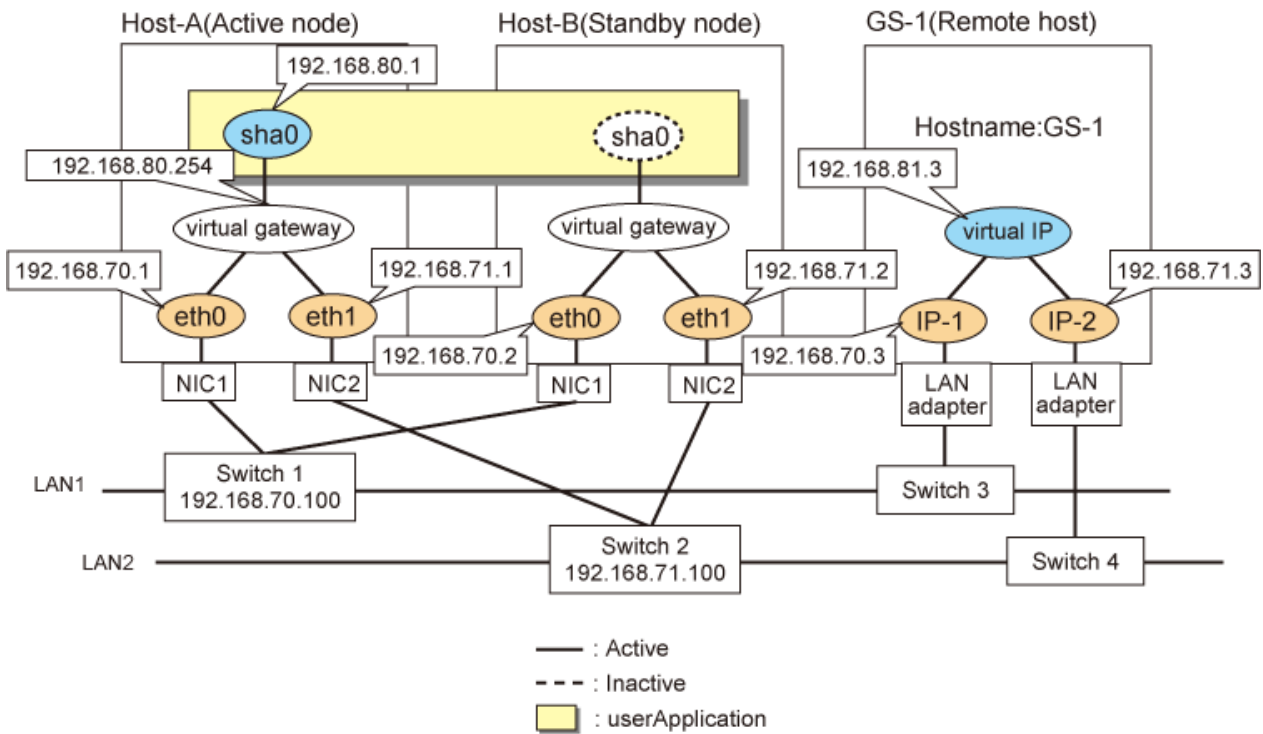
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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 the /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    host21  # HOST-B Physical IP
192.168.71.2    host22  # 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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes

```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```

TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24

```



```
DEVICE=eth1
ONBOOT=yes
```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a 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 a takeover virtual interface

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

### 8) 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 the /etc/hosts file. Defined information is the same as for HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file. The information is set in the same way as for HOST-A.

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 3) Setting a subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.80.0 -m 255.255.255.0
```

## 4) Creating a 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
```



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 a takeover virtual interface

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

## 8) Reboot

Run the following command to reboot the system.

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

## [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.6.6 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.

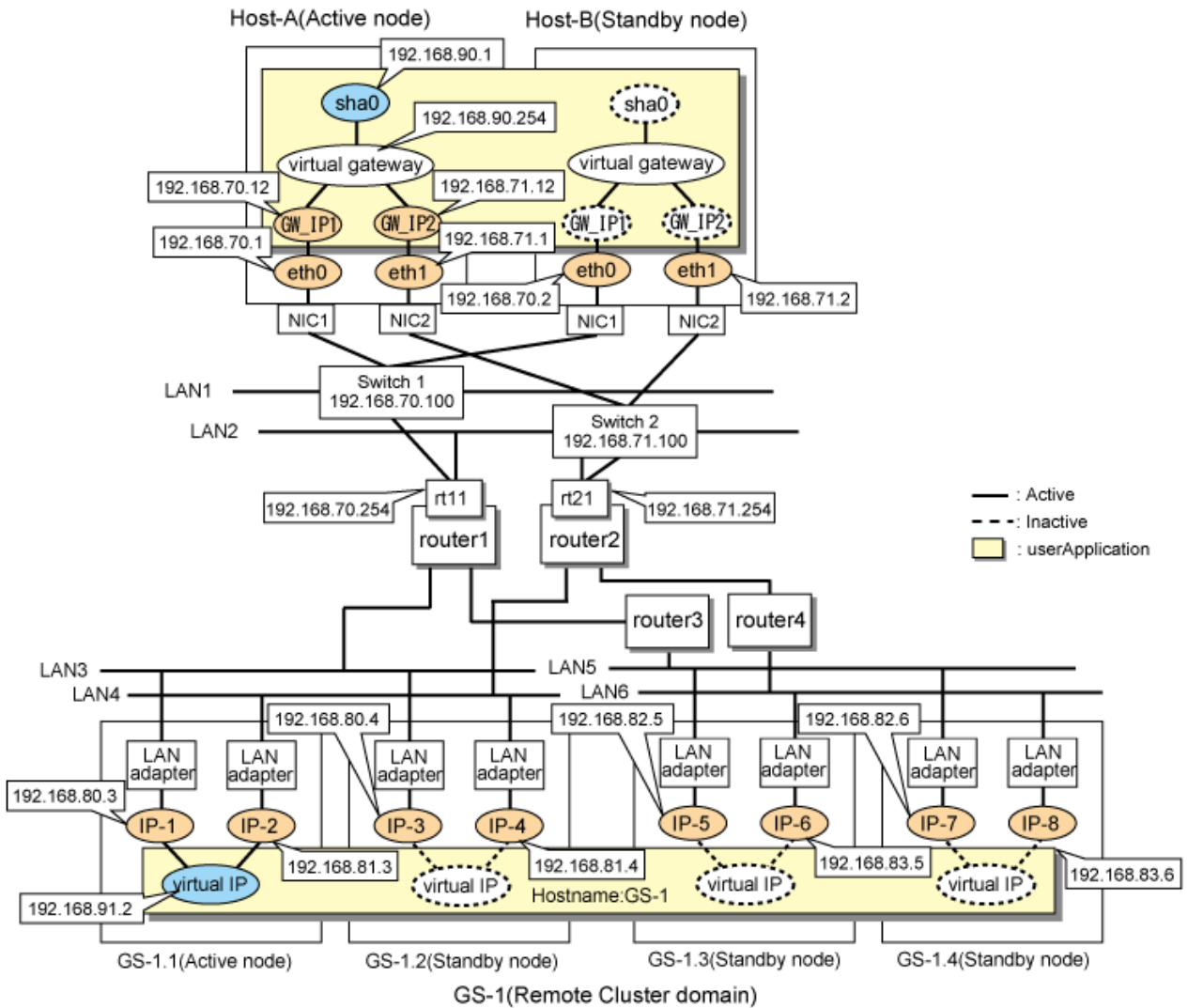
For the network configuration other than GLS, refer to "[3.2.2 Network configuration](#)".

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 the /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    host21  # HOST-B Physical IP
192.168.71.2    host22  # 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

```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) 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 the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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)
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
ipv4.routes: "192.168.80.0/24 192.168.70.254,192.168.82.0/24
192.168.70.254"
connection.autoconnect: "yes"
```

#### - Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses: "192.168.71.1/24"
ipv4.routes: "192.168.81.0/24 192.168.71.254,192.168.83.0/24
192.168.71.254"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 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 a 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 a 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.

### 8) 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 the /etc/hosts file. Defined information is the same as for HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) 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 the /etc/sysconfig/network-scripts/route-"interface name" file. The information is set in the same way as for HOST-A.

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.



```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
ipv4.routes: "192.168.80.0/24 192.168.70.254,192.168.82.0/24
192.168.70.254"
connection.autoconnect: "yes"
```

#### - Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses: "192.168.71.2/24"
ipv4.routes: "192.168.81.0/24 192.168.71.254,192.168.83.0/24
192.168.71.254"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 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 a 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 a 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.

### 8) Reboot

Run the following command to reboot the system.

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

## [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.6.7 Example of the Cluster system (Mutual Standby)

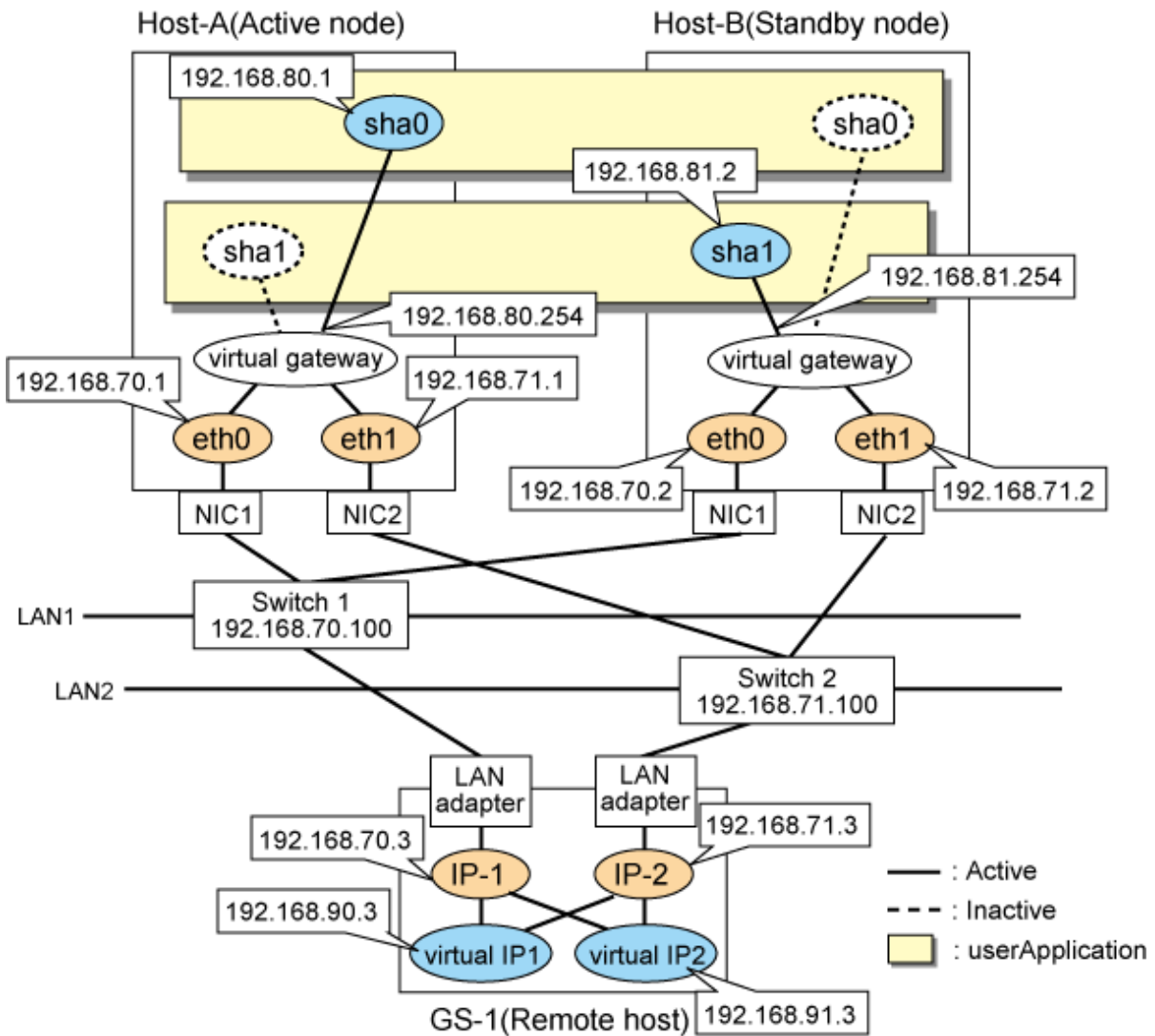
This section describes an example configuration procedure of the network shown in the diagram below.

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 the /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    host21  # HOST-B Physical IP
192.168.71.2    host22  # 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
  
```

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.1
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file.

- 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
```

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.1/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.1/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

### 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 a 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 sha1 -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
```



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 sha1 -g 192.168.81.254
```

### 7) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

### 8) 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 the /etc/hosts file. Defined information is the same as for HOST-A.

- For RHEL8

1-2) Configure the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) file as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.71.2
PREFIX=24
DEVICE=eth1
ONBOOT=yes
```

1-3) Set the static route information of the virtual gateway for the remote host's virtual IP address in the /etc/sysconfig/network-scripts/route-"interface name" file. The information is set in the same way as for HOST-A.

- For RHEL9

1-2) Set the IP address defined above with the "nmcli connection modify" command.

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.70.2/24"
connection.autoconnect: "yes"
```

- Configuration of eth1

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.71.2/24"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the nmcli connection show command.

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 and eth1 are enabled using the ip command.

```
/usr/bin/nmcli connection reload
/usr/bin/nmcli connection up eth0
/usr/bin/nmcli connection up eth1
```

## 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 a 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 sha1 -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
```



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 sha1 -g 192.168.81.254
```

## 7) Creating a takeover virtual interface

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0  
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha1
```

## 8) 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 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.

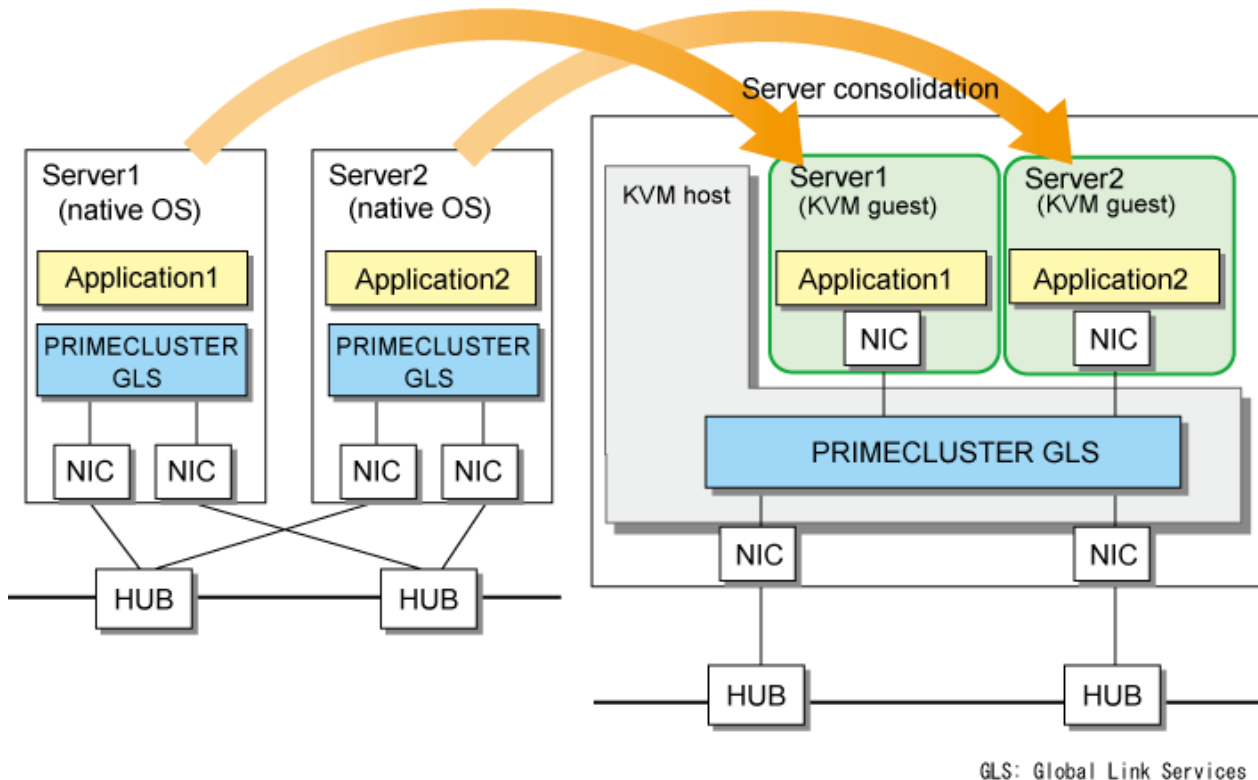
# Appendix C Operation on the Virtual Machine Function

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.

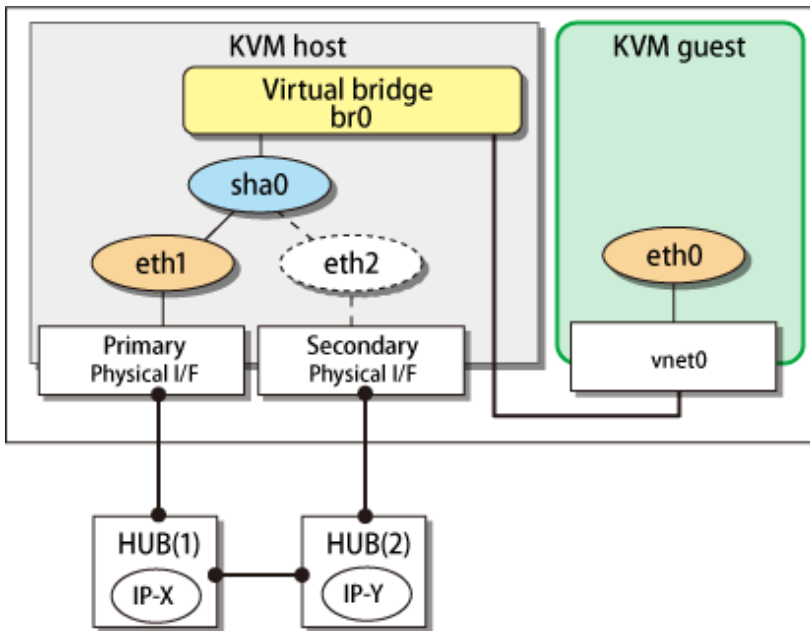


## C.2 Configuration of the Virtual Machine Function

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.





Note

Do not create a tagged VLAN interface on the virtual bridge connected to the virtual interface of Virtual NIC mode. The tagged VLAN interface created cannot be used for communication.

## C.3 Virtual Network Design in Virtual Machine Function

### C.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

### C.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). For the detail of each redundant network method, see the following table.

Table C.1 Redundant network methods available on the KVM host (host OS) or the guest domain (guest OS)

Redundant network methods	KVM host (host OS)		KVM guest (guest OS)
	Connecting the virtual bridge to the virtual interface	Bundling the virtual bridge on the virtual interface	
Fast switching mode	B	B	A
NIC switching mode	B	B	A
Virtual NIC mode	A	B	A
GS linkage mode	B	B	A

A: Supported (RHEL8 or later), B: Not supported

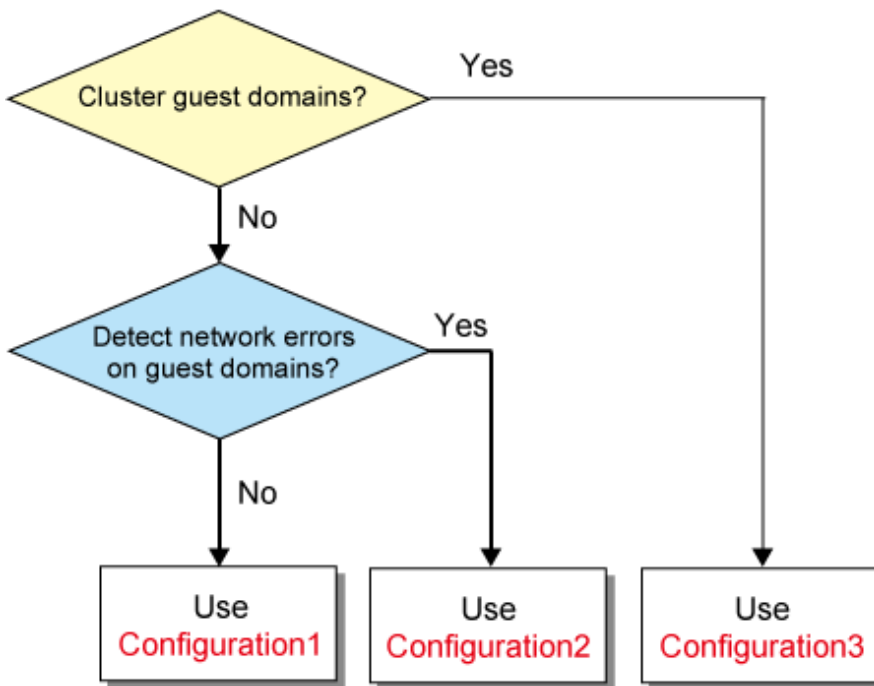
 Note

- On the virtual interface of the host OS, the highly reliable communication of the guest OS cannot be configured.
- To configure the highly reliable communication of the guest OS, install GLS on the guest OS as well.
- When duplicating the interface that was created by SR-IOV, use the NIC switching mode.

### 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.



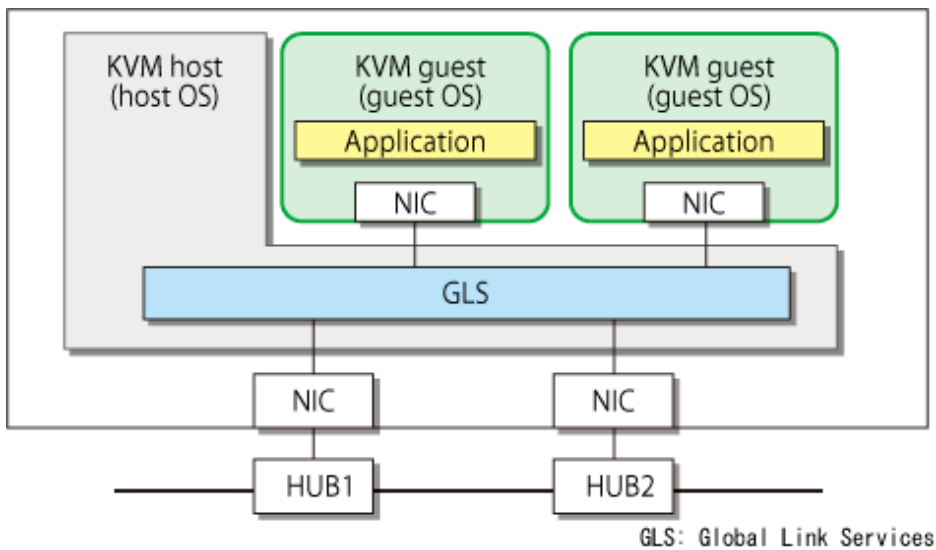
### C.3.4 Details on each configuration

---

#### 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.

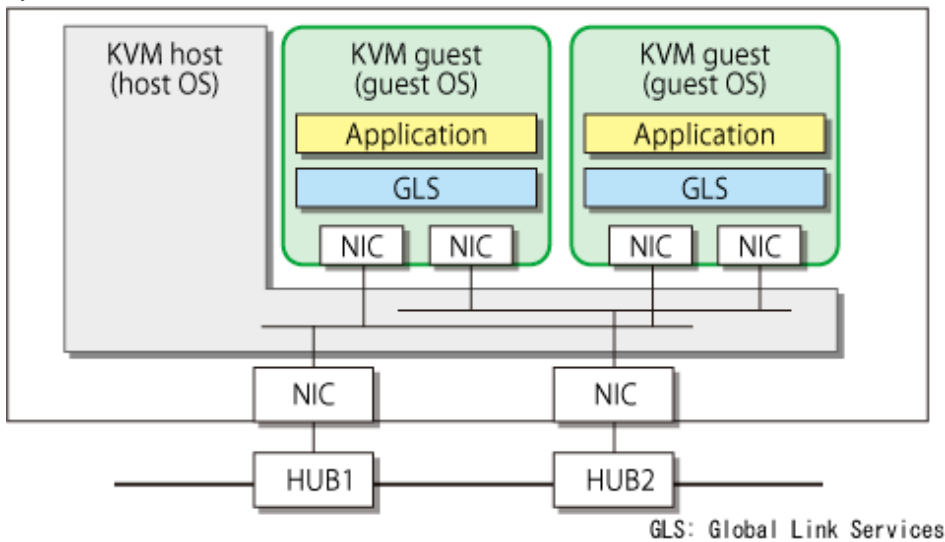
Figure C.1 Configuration 1: Configuration diagram for creating a highly reliable network of KVM guests on the KVM host



**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.

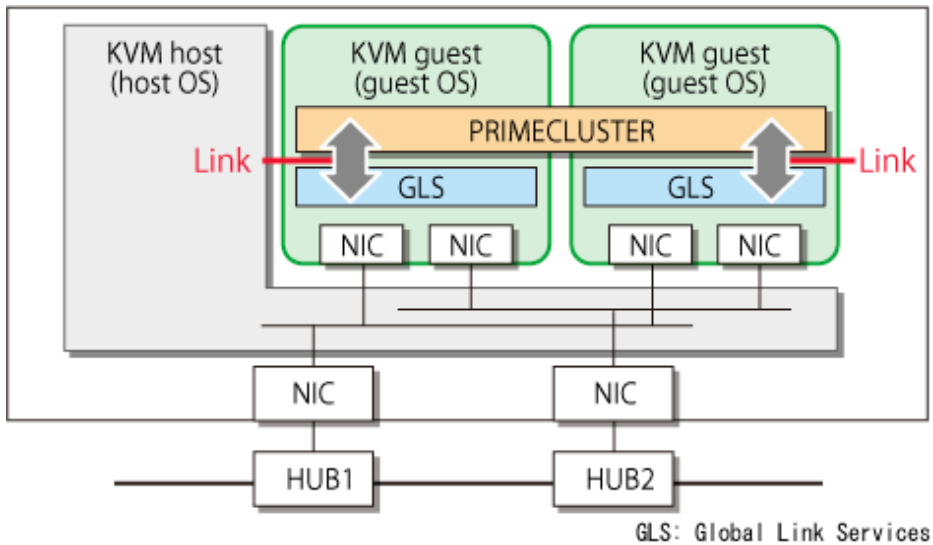
Figure C.2 Configuration 2: Configuration diagram for creating a highly reliable network on KVM guests in a single system



**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.

Figure C.3 Configuration 3: Configuration diagram for creating a highly reliable network on each KVM guest in a cluster system



## C.4 Operation of Redundant Line Switching Mode on the Virtual Machine Function

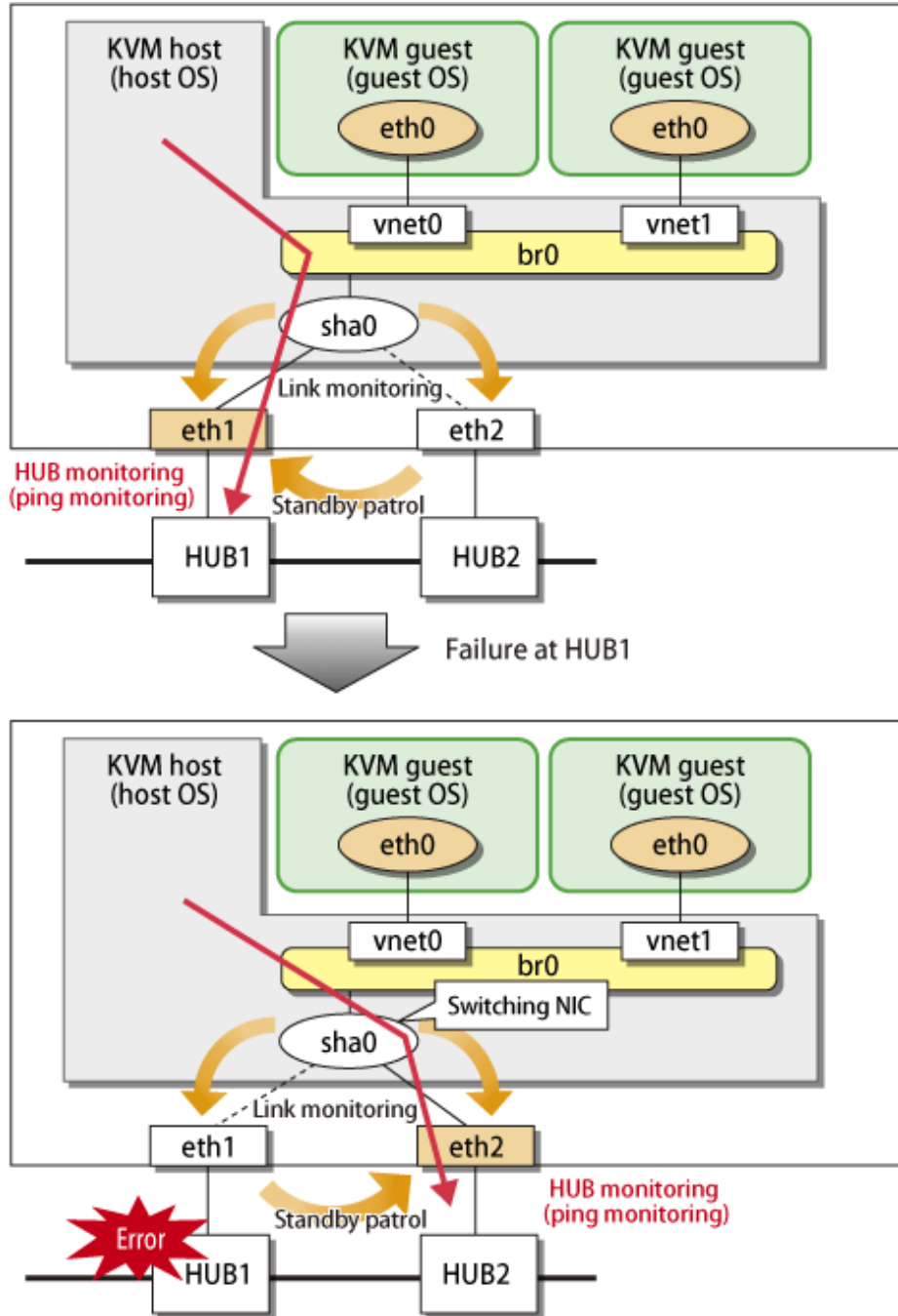
This section describes how to monitor the GLS network for each virtual network configuration and how to switch to a normal network when a network failure occurs.

### C.4.1 Configuration for creating a highly reliable network of 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 C.4 Configuration for creating a highly reliable network of KVM guests on the KVM host (Configuration 1)



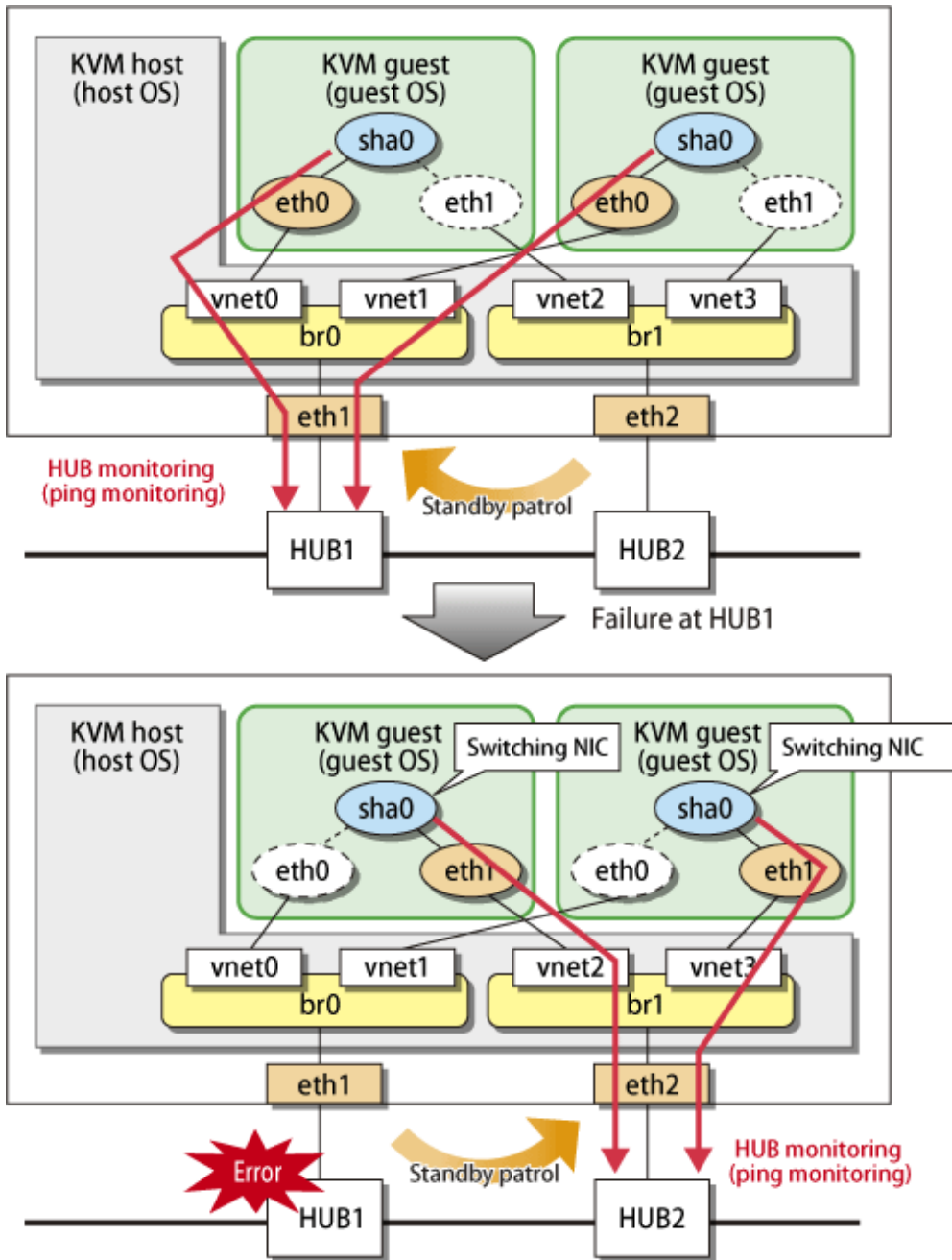
### C.4.2 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2)

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 C.5 Configuration for creating a highly reliable network on KVM guest a single system (Configuration 2)

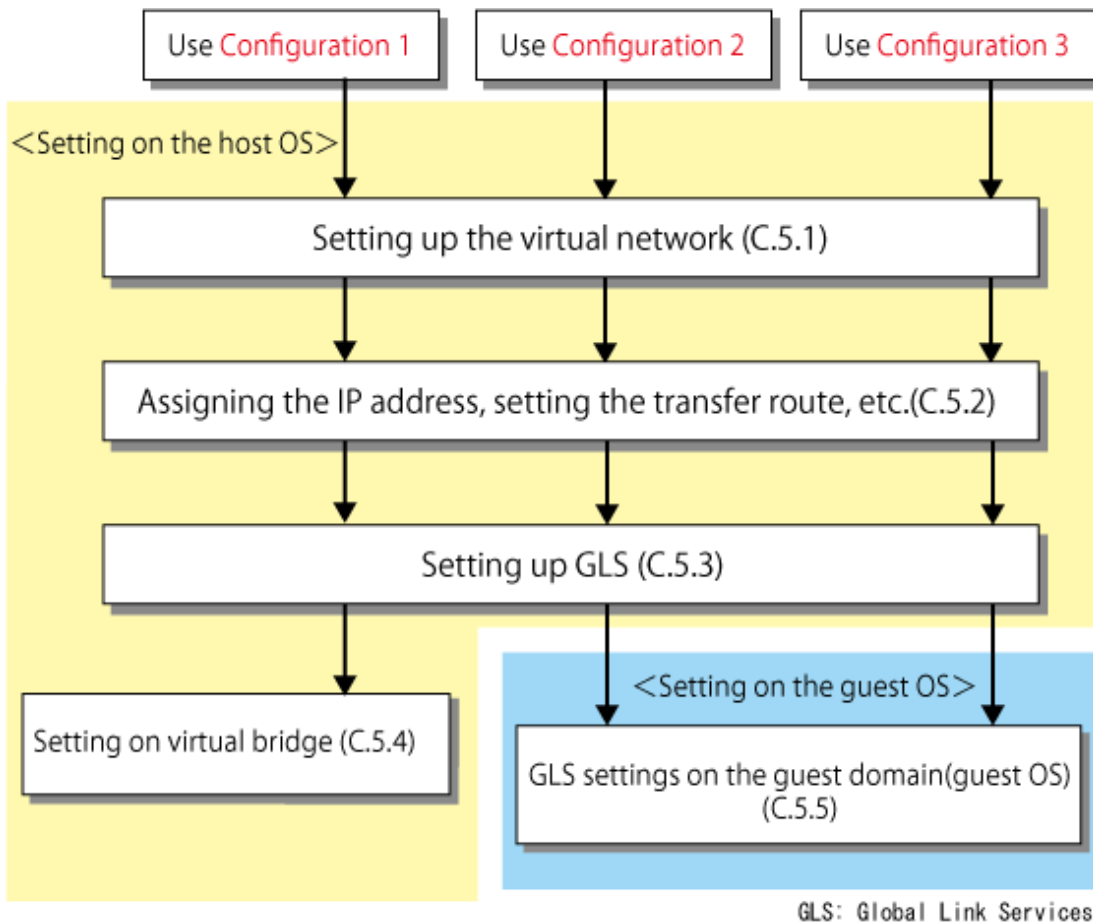


### C.4.3 Configuration for creating a highly reliable network on each KVM guest of a cluster system (Configuration 3)

This configuration is the same as the one described in "C.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.

## C.5 Setting up Redundant Line Switching Mode on the Virtual Machine Function

The setup procedure is as follows. For setup examples, see "C.6 Examples of Configuration Setup".



## C.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.

## 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](#)".

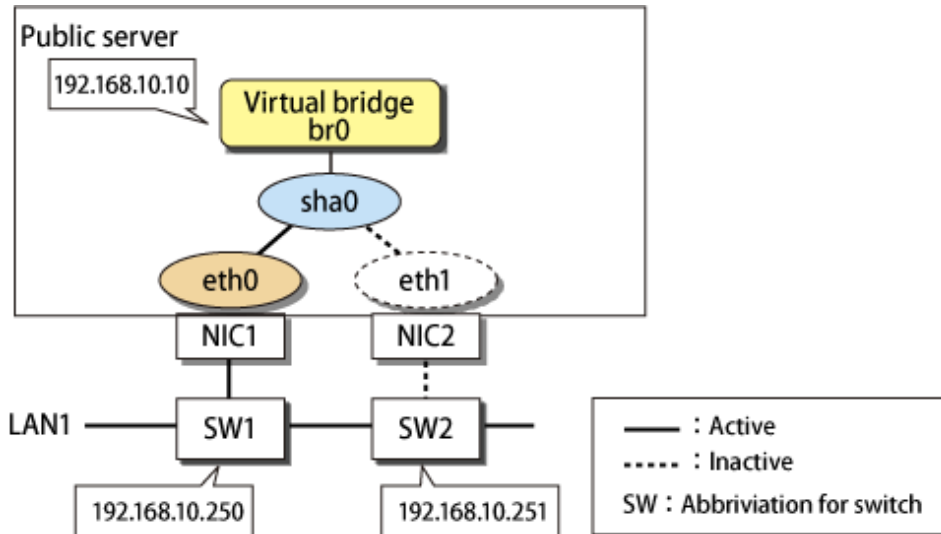
## C.5.3 Setting up GLS (for host OS)

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 Sample configurations for the virtual bridge

This section provides sample configurations for a virtual bridge based on the network configuration shown below.

Figure C.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/FJSSVhanet/usr/sbin/stphanet -n sha0
```

- 3) Create a new virtual interface.

- For RHEL8

```
# /bin/touch /etc/sysconfig/network-scripts/ifcfg-br0
```

- For RHEL9

Create br0 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "br0"
connection.interface-name: "br0"
connection.type: "bridge"
connection.autoconnect: "yes"
```

- 4) Define the IP address and other settings for the virtual bridge.

- For RHEL8

- Contents of /etc/sysconfig/network-scripts/ifcfg-br0

```
DEVICE=br0
TYPE=Bridge
BOOTPROTO=none
IPADDR=192.168.10.10
PREFIX=24
ONBOOT=yes
DELAY=0
```

- For RHEL9

Set the following parameters to br0 with the "nmcli connection modify" command.



```
ipv4.method: "manual"
ipv4.addresses: "192.168.10.10/24"
```

5) Edit the setting for the virtual interface.

- For RHEL8

Delete "IPADDR", "PREFIX", 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=none
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br0
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
connection.slave-type: "bridge"
connection.master: "br0"
ipv4.method: "disabled"
```

6) Activate the virtual interface.

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

7) Activate the virtual bridge.

- For RHEL8

```
# /usr/sbin/ifup br0
```

- For RHEL9

```
# /usr/bin/nmcli connection up br0
```

## Deleting the settings for the virtual bridge

1) Deactivate the virtual bridge.

- For RHEL8

```
# /usr/sbin/ifdown br0
```

- For RHEL9

```
# /usr/bin/nmcli connection down br0
```

2) Deactivate the virtual interface and dismantle the virtual bridge.

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



### Note

The following message may be output. This does not disrupt ongoing operation.

```
hanet: 78011: warning: nmcli failed. (connection down=2560 ifname=virtual interface name)
```

3) Delete the virtual bridge.

- For RHEL8

```
# /bin/rm /etc/sysconfig/network-scripts/ifcfg-br0
```

- For RHEL9

```
# nmcli connection delete br0
```

4) Edit the setting for the virtual interface.

- For RHEL8

Delete the statement of "BRIDGE=br0".

In addition, add statements of "IPADDR", "PREFIX", and similar statements related to the IP address as necessary.

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

```
DEVICE=sha0
IPADDR=192.168.10.10
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
connection.slave-type: ""
connection.master: ""
ipv4.method: "manual"
ipv4.addresses: "192.168.10.10/24"
```

5) Activate the virtual interface.

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

## 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](#)".

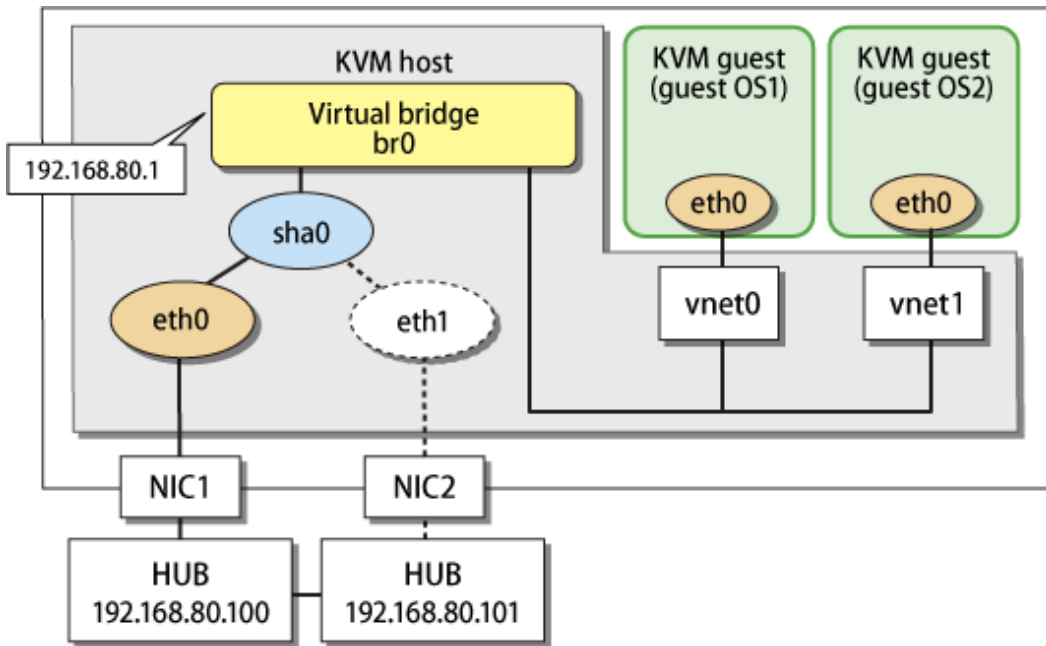


Set the same device model for the interface bundled by GLS on the guest OS.

## C.6 Examples of Configuration Setup

### C.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  swhub1   # IP address of the primary monitoring destination's HUB
192.168.80.101  swhub2   # IP address of the secondary monitoring destination's HUB
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) files as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting the virtual bridge

- For RHEL8

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=none
IPADDR=192.168.80.1
PREFIX=24
ONBOOT=yes
DELAY=0
```

- For RHEL9

Create br0 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "br0"
connection.interface-name: "br0"
connection.type: "bridge"
connection.autoconnect: "yes"
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
```

## 4) Setting a virtual interface

- For RHEL8

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 "PREFIX").

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

```
DEVICE=sha0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
BRIDGE=br0
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
connection.slave-type: "bridge"
connection.master: "br0"
ipv4.method: "disabled"
```

## 5) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

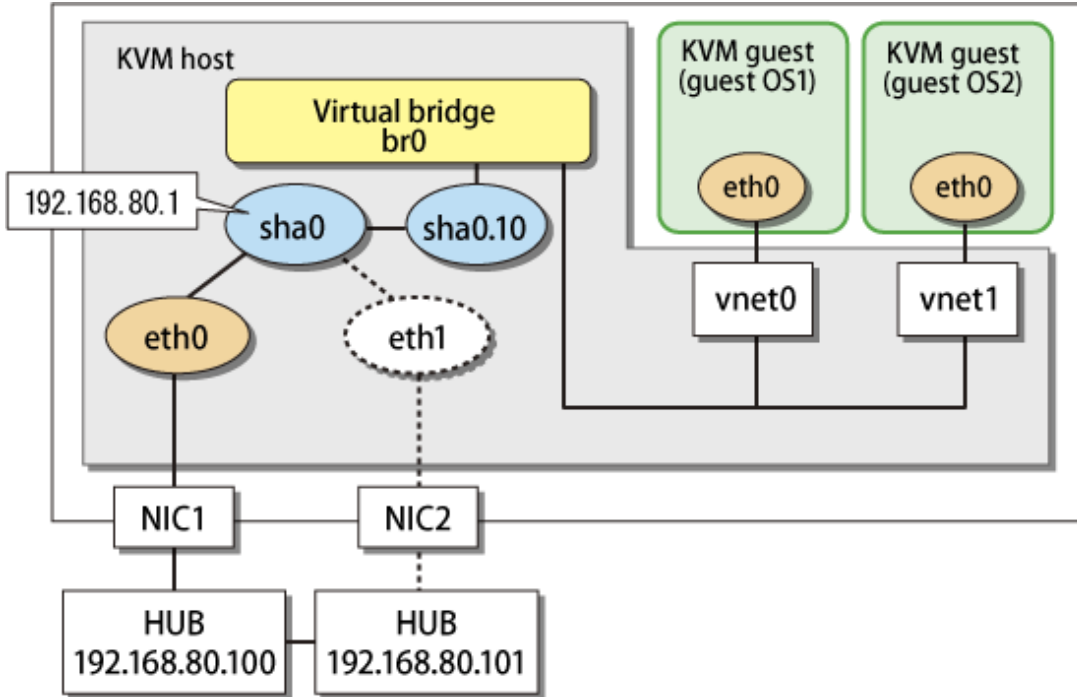
## 6) Reboot

Run the following command to reboot the system.

/sbin/shutdown -r now

## C.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 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 swhub1   # IP address of the primary monitoring destination's HUB
192.168.80.101 swhub2   # IP address of the secondary monitoring destination's HUB
```

- For RHEL8

1-2) Edit the /etc/sysconfig/network-scripts/ifcfg-ethX (X is 0, 1) files as follows.

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

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth0
ONBOOT=yes
```

- Contents of /etc/sysconfig/network-scripts/ifcfg-eth1

```
TYPE=Ethernet
BOOTPROTO=none
DEVICE=eth1
ONBOOT=yes
```

- For RHEL9

1-2) Set the following parameters to ethX (X is 0, 1) with the "nmcli connection modify" command.

```
ipv4.method: "disabled"
ipv6.method: "disabled"
connection.autoconnect: "yes"
```

After setting, verify that the following parameters are set for ethX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing ["3.2.2.1 Setup common to modes."](#)

```
connection.type: "802-3-ethernet"
connection.id: "ethX"
connection.interface-name: "ethX"
```

## 2) Creating a virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m v -t eth0,eth1
```

## 3) Setting the virtual bridge

- For RHEL8

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=none
ONBOOT=yes
DELAY=0
```

- For RHEL9

Create br0 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "br0"
connection.interface-name: "br0"
connection.type: "bridge"
connection.autoconnect: "yes"
ipv4.method: "disabled"
ipv6.method: "disabled"
```

## 4) Setting a virtual interface

- For RHEL8

Define an IP address or a prefix in the /etc/sysconfig/network-scripts/ifcfg-sha0 file.

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

```
DEVICE=sha0
IPADDR=192.168.80.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
connection.slave-type: "bridge"
connection.master: "br0"
ipv4.method: "manual"
ipv4.addresses: "192.168.80.1/24"
```

### 5) Adding a tagged VLAN interface

- For RHEL8

To add the tagged VLAN interface 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

```
VLAN=yes
TYPE=Vlan
PHYSDEV=sha0
VLAN_ID=10
BOOTPROTO=none
BRIDGE=br0
```

- For RHEL9

Create sha0.10 with the following parameters by using the "nmcli connection add" command.

```
connection.id: "sha0.10"
connection.interface-name: "sha0.10"
connection.type: "vlan"
connection.autoconnect: "yes"
connection.slave-type: "bridge"
connection.master: "br0"
vlan.parent: "sha0"
vlan.id: "10"
ipv4.method: "disabled"
ipv6.method: "disabled"
```

### 6) Setting the network monitoring function

```
/opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p 192.168.80.100,192.168.80.101
```

### 7) Setting /etc/NetworkManager/NetworkManager.conf

Describe the tagged VLAN interface, which is set in step 5), in /etc/NetworkManager/NetworkManager.conf.

- Contents of /etc/NetworkManager/NetworkManager.conf

```
[main]
...
ignore-carrier=sha0.10
```

### Note

The setting of /etc/NetworkManager/NetworkManager.conf is required to control the processing of NetworkManager for tagged VLAN interfaces and manage the processing in GLS. Make sure to set /etc/NetworkManager/NetworkManager.conf.

### 8) Reboot

Run the following command to reboot the system.

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

## C.6.3 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.

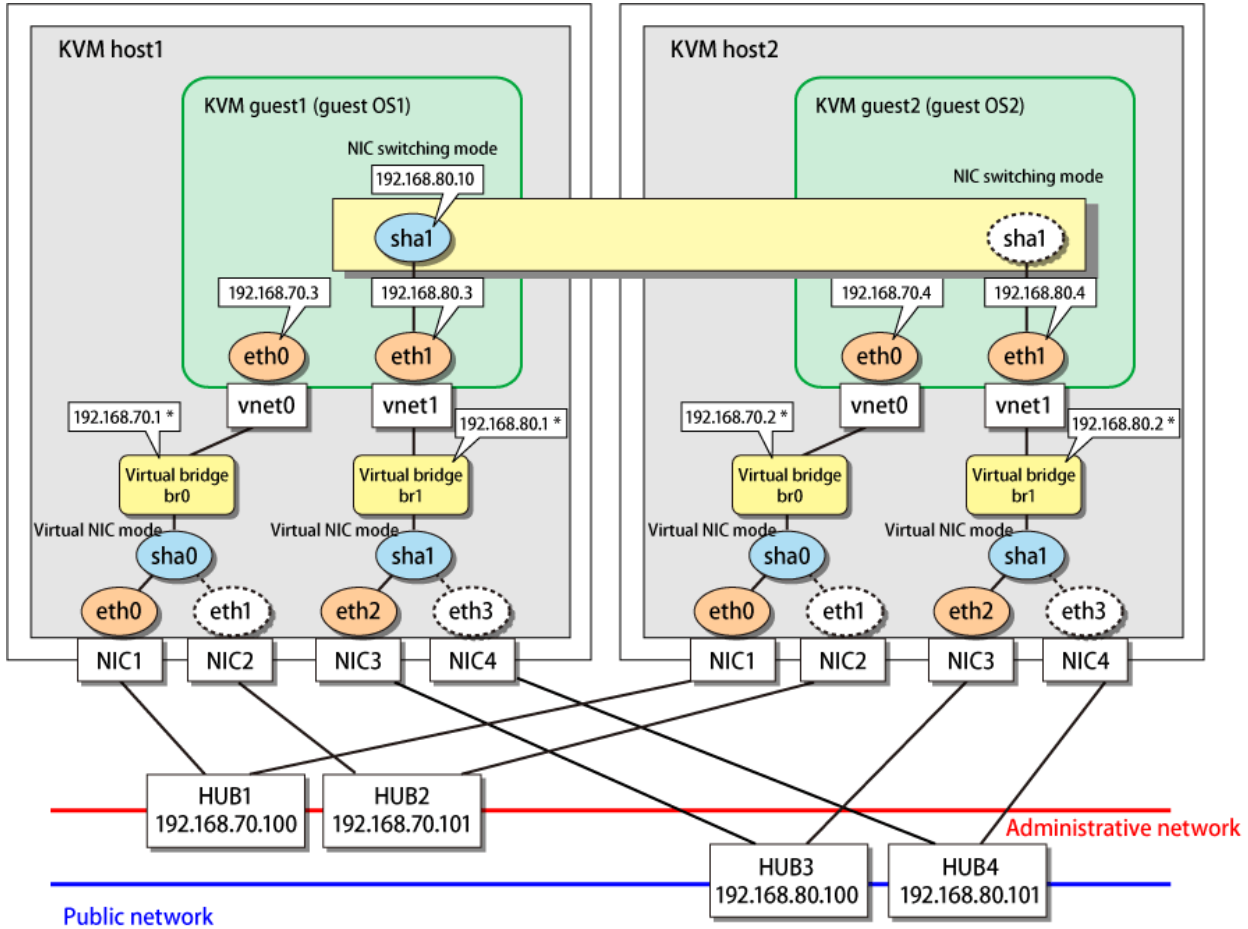
Make a redundant network on KVM hosts. To link up with the cluster system, install GLS on KVM guests. In addition to the cluster system, select this configuration when consolidating various servers to KVM guests.

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 "C.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 guest1 and KVM guest2]

Setting up GLS is the same as for "E.6.3 Setup example in a 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 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 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.

## Appendix D Operation on RHOSP

This chapter describes the operation of GLS on RHOSP. On RHOSP environment, GLS can be used on virtual machine instances. For details on RHOSP, refer to the RHOSP manual issued by Red Hat, Inc.

Note the following settings when using GLS on RHOSP environment.

- Only the single physical interface configuration of virtual NIC mode can be supported.
- Specify the DNS server to be used.

For RHEL8, add the following settings in the configuration file of the virtual interface (ifcfg-shaX).

- Add the setting "PEERDNS=yes".
- Add the settings "DNS1=<DNSServer1>" and "DNS2=<DNSServer2>".

For RHEL9, set the following parameters to the virtual interface (shaX) with the "nmcli connection modify" comand.

```
ipv4.ignore-auto-dns: "yes"
ipv4.dns: "<DNSServer1>, <DNSServer2>"
```

- For RHEL8, do not set SHAMACADDR in the configuration file of the virtual interface (ifcfg-shaX). For RHEL9, do not specify the "-s" option when creating the virtual interface with the "hanetconfig create" command.
- To use a virtual router as the monitoring destination, it is recommended to set the virtual router to be redundant. Also set the time to detect a network error in GLS to be longer than the time to switch the redundant virtual router.
- When not setting a virtual router used as a monitoring target to be redundant, set to avoid a failover of the cluster even when an error is detected in the transfer route.

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon param -n shaX -f no
```

- When configuring the static route information on the guest OS in the RHOSP environment when BOOTPROTO is set as dhcp, add and configure the static route information for the DHCP server of neutron in the subnet.

```
# neutron subnet-update --host-route destination=CIDR,nexthop=IPaddress
subnetname
```

# Appendix E Operation on VMware

This chapter describes the operation of GLS on VMware. For details on VMware, see the manuals for VMware.

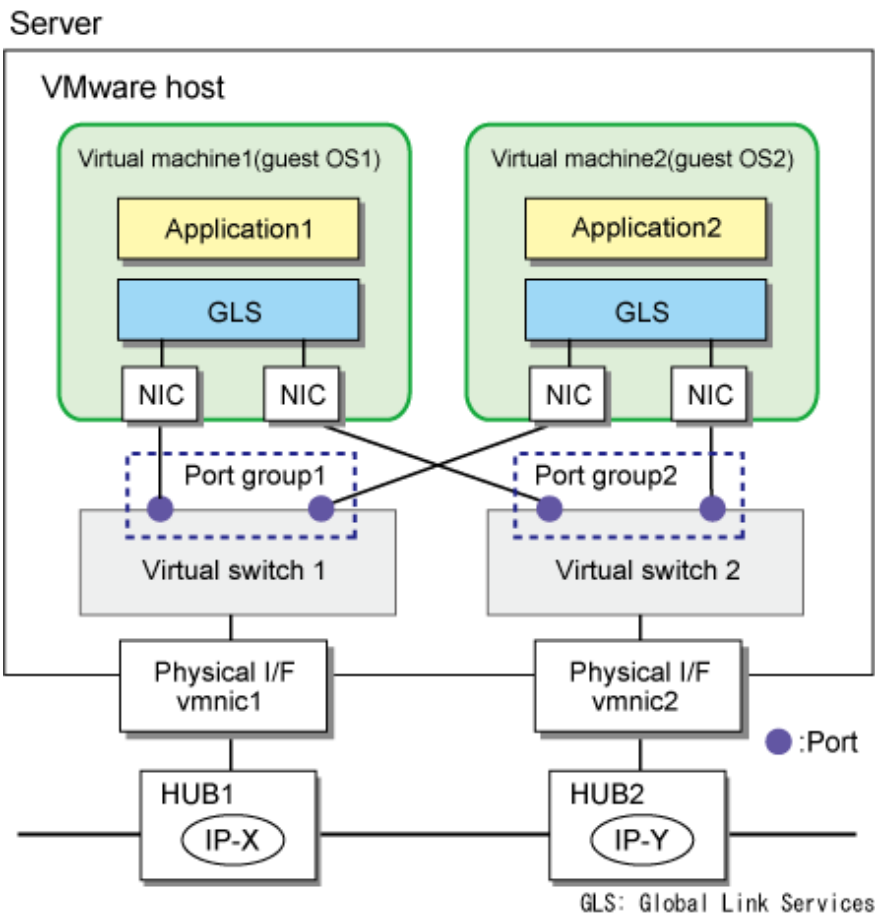
## E.1 VMware Overview

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 communicates 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 the following for the virtual switch in VMware:

- Set [Accept] for [Promiscuous Mode] under [Security].
- Set [Accept] for [Forged Transmits] under [Security].

## 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	Y
NIC switching mode	Y
Virtual NIC mode	Y
GS linkage mode	Y

Y: Supported N: 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.

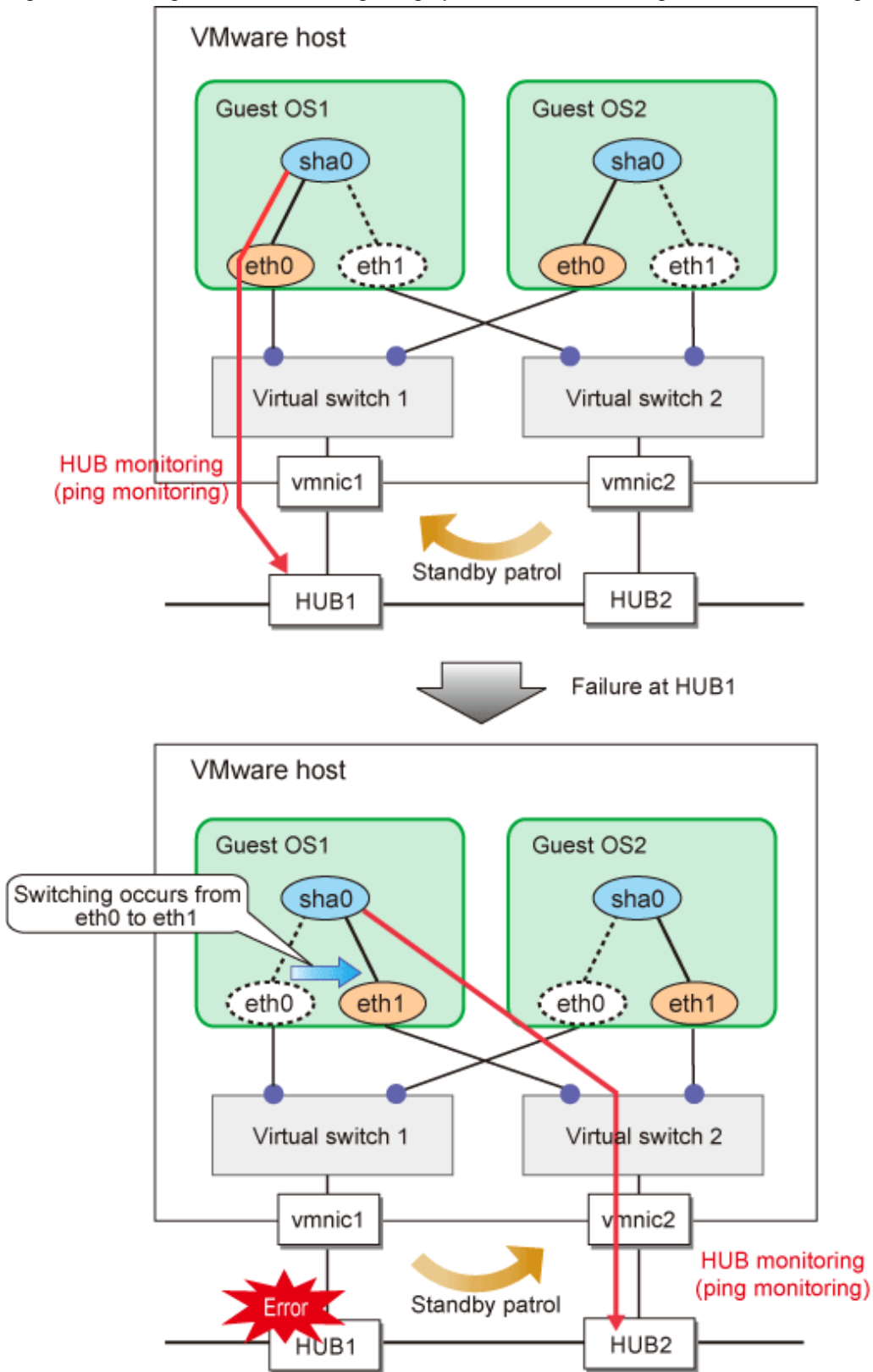
For the operation of GLS in VMware, there is no difference from the operation on a physical server.

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.

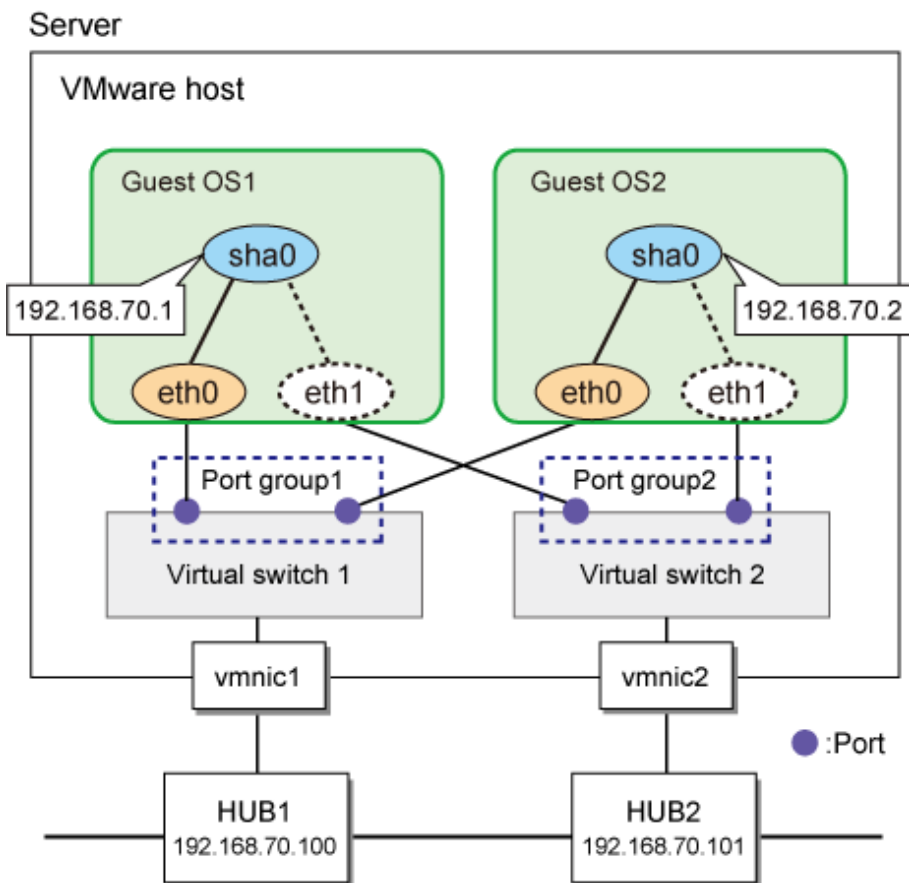
## E.5 Setting up Redundant Line Switching Mode on VMware

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.

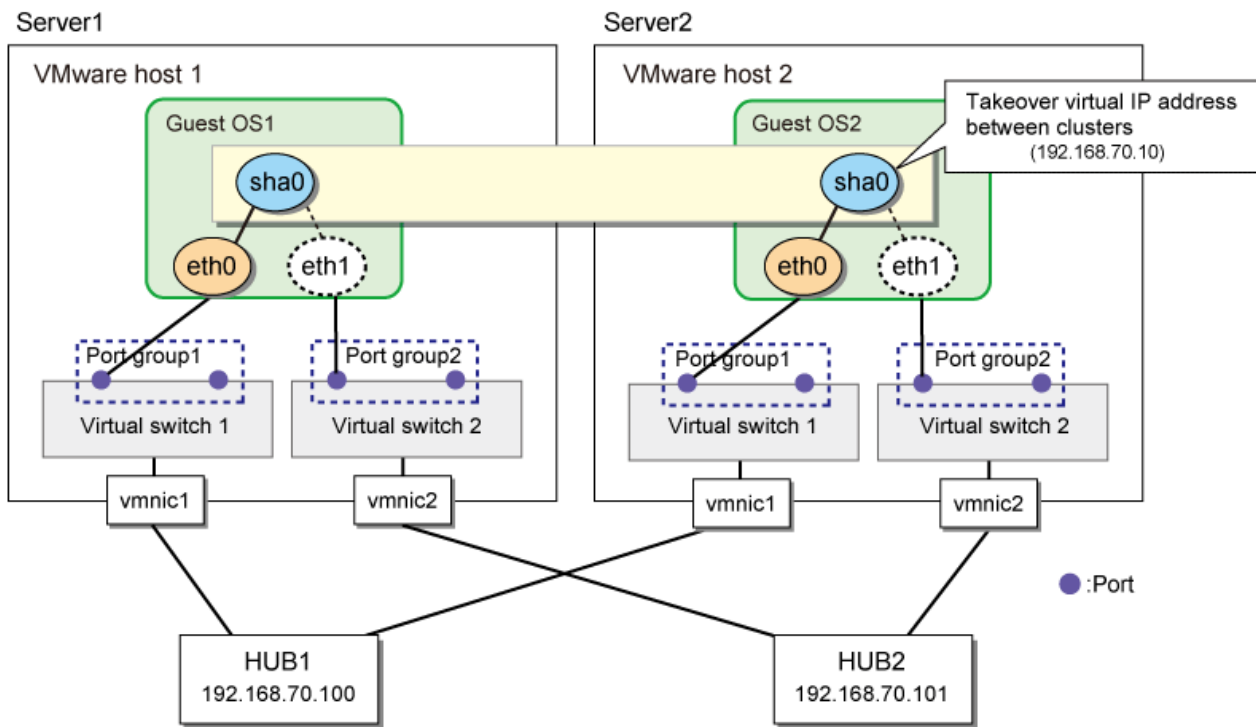
When using the virtual NIC mode, set [Accept] for [Promiscuous Mode] under [Security] for each virtual switch in VMware.

#### [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)]

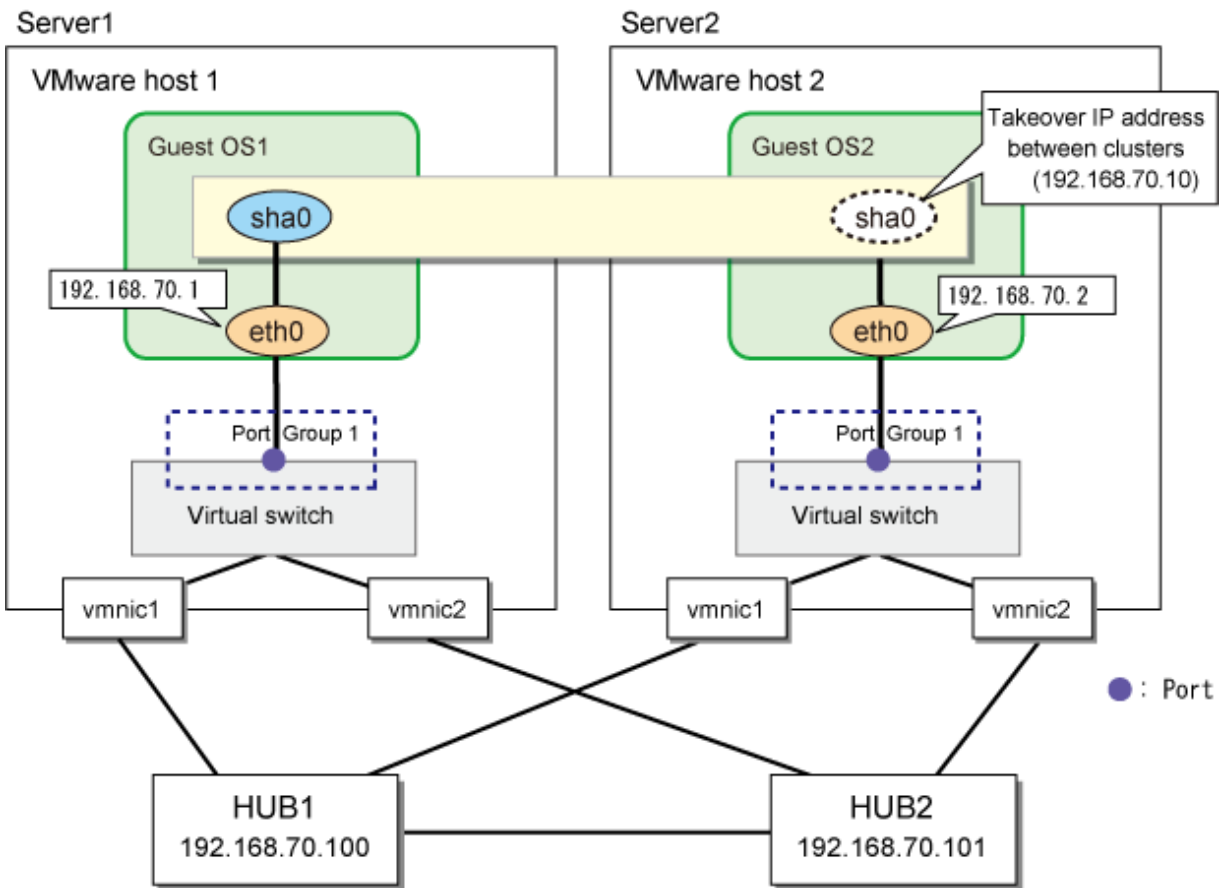
Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

### [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](#)".

## E.6.3 Setup example in a cluster system (NIC non-redundant)

This section describes a configuration setup example for the following network configuration.



### Note

Set so that the network error detection time of GLS on the guest OS becomes longer than the network error detection time by the redundant function on the VMware host.

### [Setting up the VMware host]

Connect the redundant interface to the guest machine on the VMware host machine.

### [Setting up the guest OS1]

#### 1) Setting up the system

1-1) Define the IP addresses and hostnames in /etc/hosts file.

```
192.168.70.10  hosta  # guest OS1/2 Virtual IP (Takeover IP address)
192.168.70.1  host11 # guest OS1 Physical IP
192.168.70.2  host21 # guest OS2 Physical IP
192.168.70.100 swhub1 # Primary HUB IP
192.168.70.101 swhub2 # Secondary HUB IP
```

1-2) Assign the defined IP address stated above in /etc/sysconfig/network-scripts/ifcfg-eth0 file.

- For RHEL8

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.1
PREFIX=24
```



```
DEVICE=eth0
ONBOOT=yes
```

- For RHEL9

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"
ipv4.addresses:"192.168.70.1/24"
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for eth0 with the nmcli connection show command.

- TYPE: "ethernet"
- DEVICE: "eth0"

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting up the subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.10 -e 192.168.70.1 -t 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
```

## 6) Creating the takeover virtual interface

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

## 7) Reboot

Run the following command to reboot the system.

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

## [Setting up the guest OS2]

### 1) Setting up the system

1-1) Define the IP address and host name to be used in /etc/hosts file. The defined content is the same with guest OS1.

1-2) Assign the defined IP address stated above to /etc/sysconfig/network-scripts/ifcfg-eth0 file.

- For RHEL8

```
TYPE=Ethernet
BOOTPROTO=none
IPADDR=192.168.70.2
PREFIX=24
DEVICE=eth0
ONBOOT=yes
```

- For RHEL9

- Configuration of eth0

Set the following parameters with the "nmcli connection modify" command.

```
ipv4.method:"manual"  
ipv4.addresses:"192.168.70.2/24"  
connection.autoconnect:"yes"
```

After setting, verify that the following parameters are set for eth0 with the nmcli connection show command.

- TYPE: "ethernet"
- DEVICE: "eth0"

## 2) Reflecting system setting

Run the following command and reload the connection profile. After reloading the profile, verify eth0 is enabled using the ip command.

```
/usr/bin/nmcli connection reload
```

## 3) Setting up the subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.70.0 -m 255.255.255.0
```

## 4) Creating the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig create -n sha0 -m d -i 192.168.70.10 -e 192.168.70.2 -t 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
```

## 6) Creating the takeover virtual interface

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

## 7) Reboot

Run the following command to reboot the system.

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

## [Setting up the RMS Wizard]

### 1) Setting up the cluster environment

After the setup of guest OS1 and guest OS2 is completed, register the created takeover virtual interface as a GIs resource to create cluster application. The setting up of cluster environment is performed using RMS Wizard. For details, see "PRIMECLUSTER Installation and Administration Guide."

### 2) Starting the cluster application

After the setup of cluster environment is completed, the takeover virtual interface is activated in the guest OS1 by starting the cluster application.

# Appendix F Operation on Hyper-V

This chapter describes the operation of GLS on Hyper-V. For details on Hyper-V, see the manuals for Hyper-V.

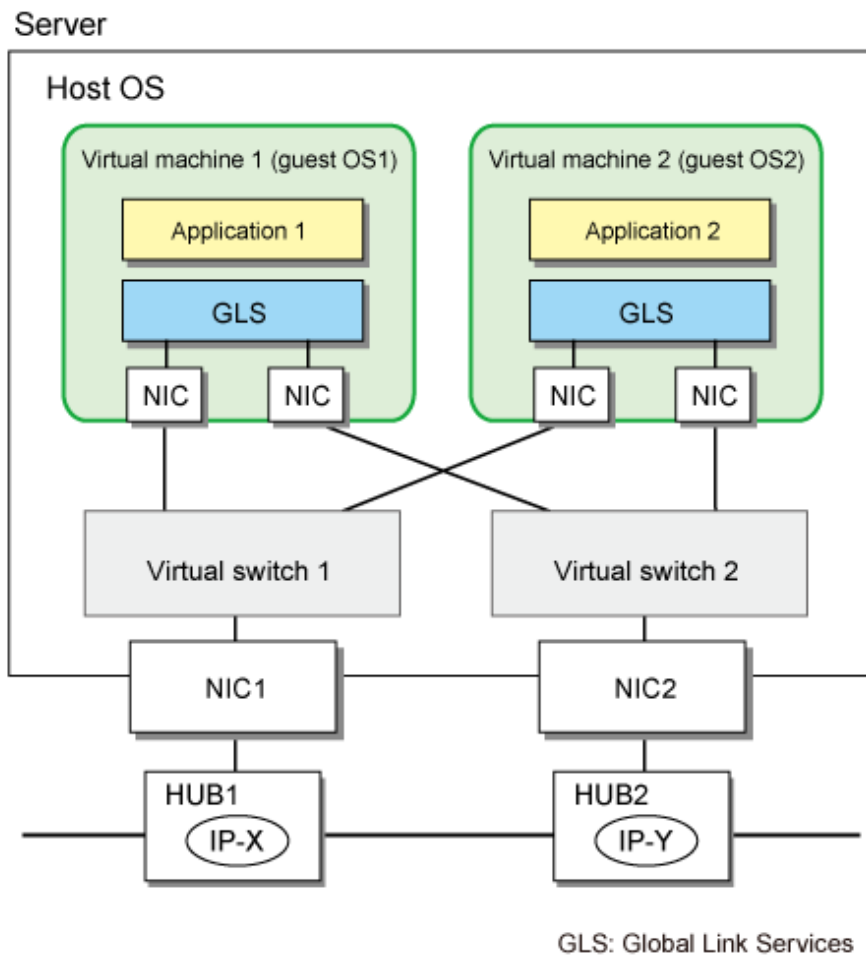
## F.1 Hyper-V Overview

Hyper-V is a product offered by Microsoft, which achieves server virtualization. Server virtualization enables you to consolidate multiple servers on one server.

## F.2 Configuration of Hyper-V

In a Hyper-V environment, servers on which applications operate are consolidated into a guest OS of Hyper-V as a virtual machine. NICs of a guest OS are connected to the virtual switch of Hyper-V. A guest OS communicates with external devices via this virtual switch.

GLS operates on a guest OS of Hyper-V. A redundant network can be provided by bundling NICs on the guest OS.



## F.3 Virtual Network Design in Hyper-V

### F.3.1 Concept of network configuration in Hyper-V

For a virtual network required for Hyper-V, see the manuals for Hyper-V.

To make a redundant network by using GLS on a guest OS of Hyper-V, network adapters bundled by GLS must be connected to different virtual switches.

## Note

- When creating network adapters bundled by GLS by using the Hyper-V Manager, set the MAC address to be [Static]. If the MAC address is set to be [Dynamic], the MAC address may be changed after the migration of a guest OS.
- To use the Virtual NIC mode, check [Enable MAC address spoofing] when creating network adapters bundled by GLS on the Hyper-V Manager.
- On a guest OS of Hyper-V, the link status cannot be monitored because the link status of the physical adapter cannot be notified. In this case, make sure to set the HUB monitoring (ping monitoring) for each guest OS.

## F.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.

Redundant Mode	Guest OS
Fast switching mode	Y
NIC switching mode	Y
Virtual NIC mode	Y
GS linkage mode	Y

Y: Supported, N: Not supported

## Note

- When the Fast switching mode provides the highly reliable guest OS network in the cluster system, and if the both nodes are in the same physical device, failover between clusters due to a network error cannot be executed. Configure each node in the different physical device.
- 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](#)."
- For a tagged VLAN connection, specify the VLAN ID when setting the network adapter of a guest OS. A tagged VLAN interface is not necessary to be created on a guest OS.
- When bundling the interface that was created by SR-IOV, use the NIC switching mode.

## F.4 Operation of Redundant Line Switching Mode on Hyper-V

This section describes how to monitor the GLS network for the virtual network configuration of Hyper-V and how to switch to a normal network when a network failure occurs.

### F.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 Hyper-V.

For the operation of GLS in Hyper-V, there is no difference from the operation on a physical server.

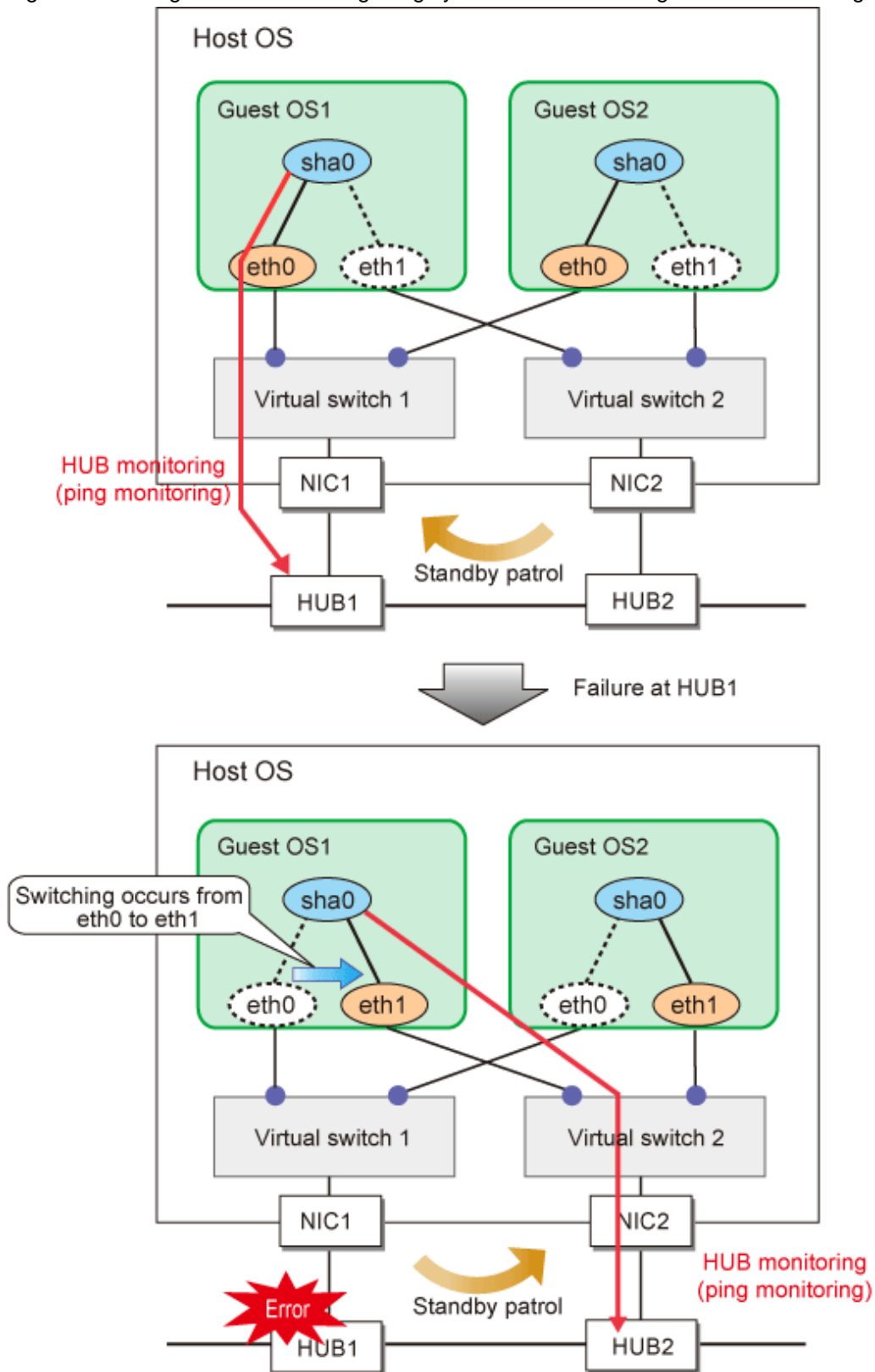
NIC switching mode is provided as an example in this section.

#### 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, the active NIC becomes

NIC2 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 (NIC2).

Figure F.1 Configuration for creating a highly reliable network on guest OSEs in a single system



## F.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 "[F.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.

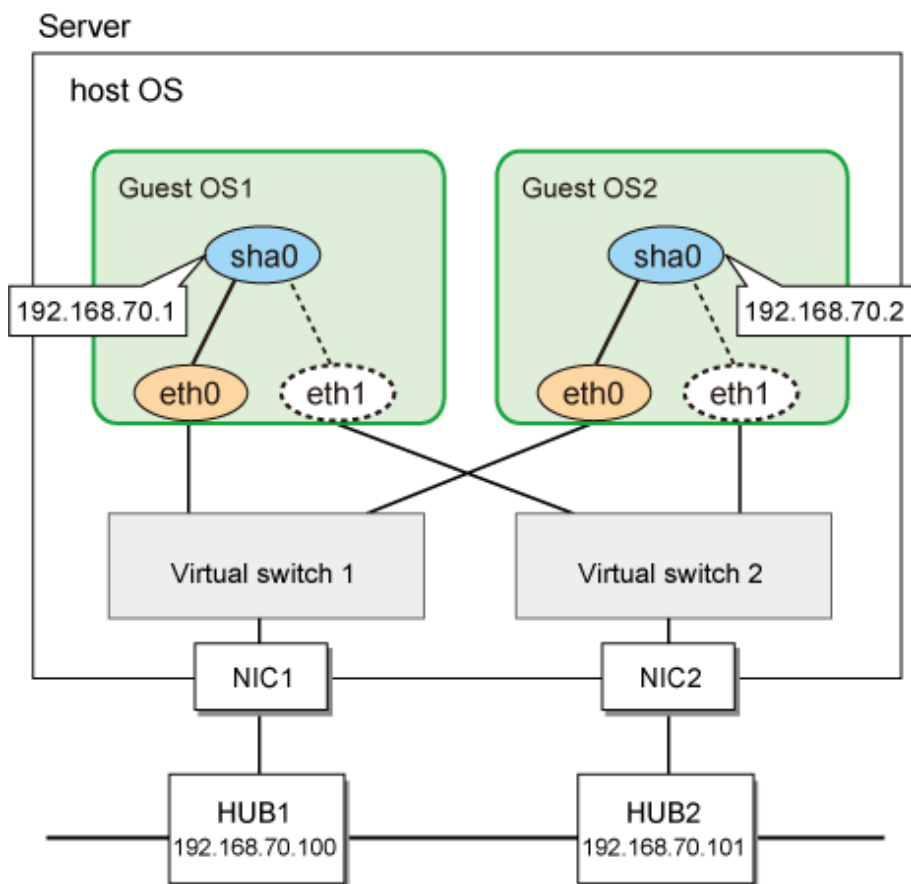
## F.5 Setting up Redundant Line Switching Mode on Hyper-V

According to the manuals for Hyper-V, configure guest OSes or virtual switches. After installing GLS on guest OSes, perform the same procedure as that of physical servers for configuration.

## F.6 Examples of Configuration Setup

### F.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 the host OS]

Create network adapters bundled by GLS by using the Hyper-V Manager.

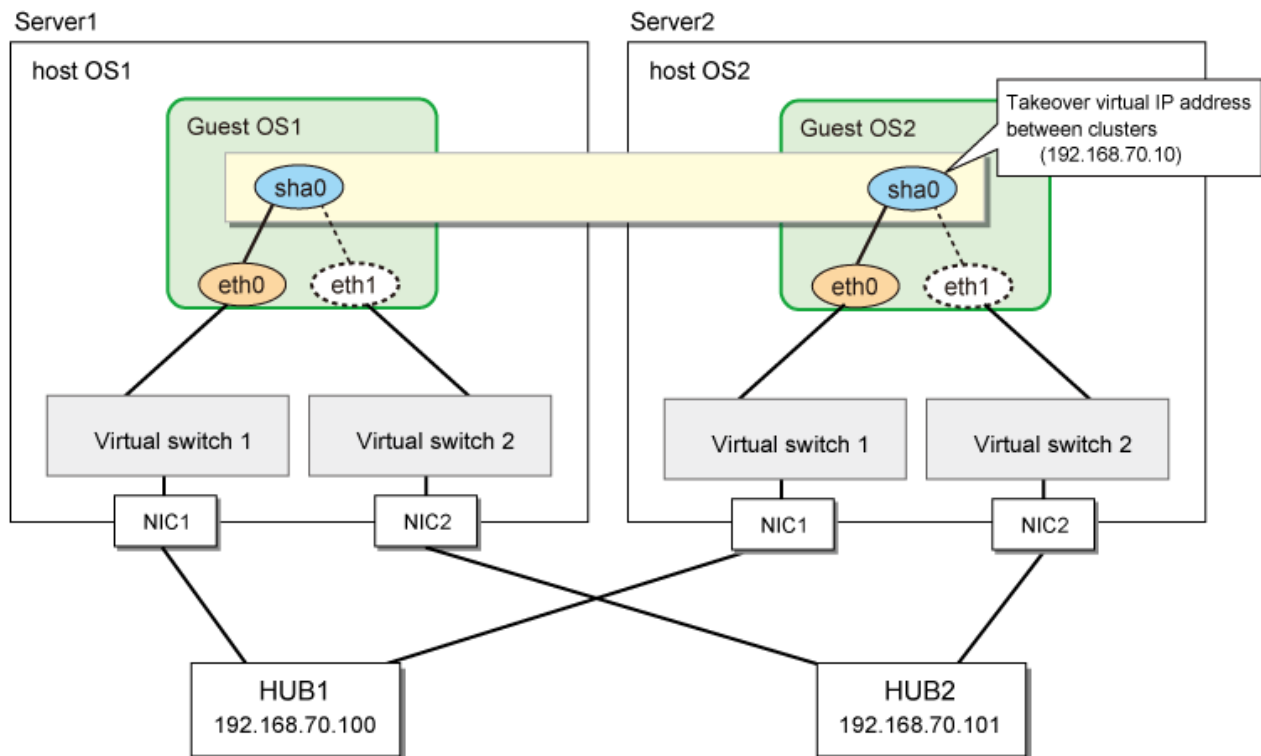
To use the Virtual NIC mode, check [Enable MAC address spoofing] when creating network adapters bundled by GLS.

#### [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](#)".

## F.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 the host OS]

Create network adapters bundled by GLS by using the Hyper-V Manager.

To use the Virtual NIC mode, check [Enable MAC address spoofing] when creating network adapters bundled by GLS.

### [Setting up the guest OS1 (active node)]

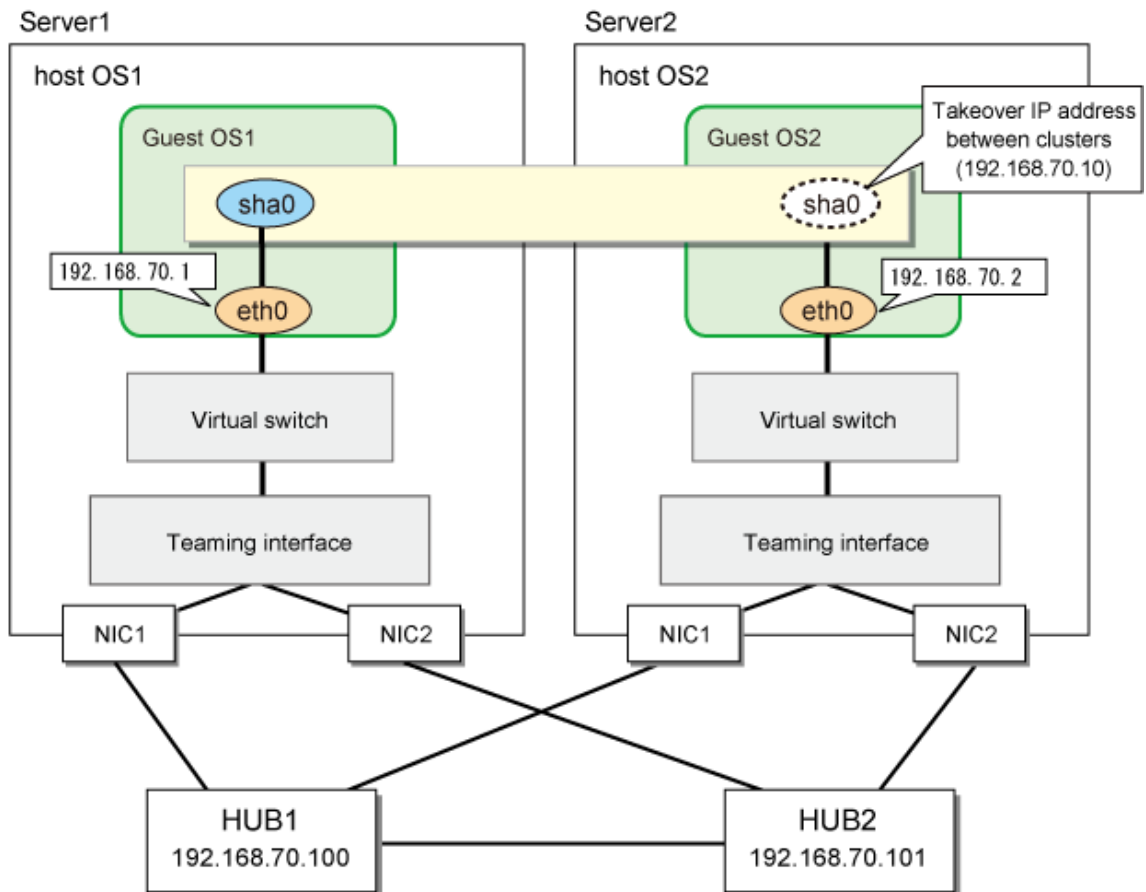
Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

### [Setting up the guest OS2 (standby node)]

Setting up GLS is the same as for physical servers. See "[Appendix B Examples of configuring system environments](#)".

## F.6.3 Setup example in a cluster system (NIC non-redundant)

This section describes a configuration setup example for the following network configuration.



### [Setting up the host OS]

Connect the redundant interface to the guest machine on the host OS using Hyper-V Manager.

### [Setting up the guest OS1/guest OS2]

Setting up GLS is the same with "E.6.3 Setup example in a cluster system (NIC non-redundant)."

#### Note

Set so that the network error detection time of GLS on the guest OS becomes longer than the network error detection time by the redundant function on the host OS.



# Appendix G Cloning environment

In GLS, the already configured cluster system can be cloned to configure the new cluster system by changing the IP address.

This chapter explains the procedure of cloning through the examples of the single system for each communication mode and the 1:1 active standby cluster system.

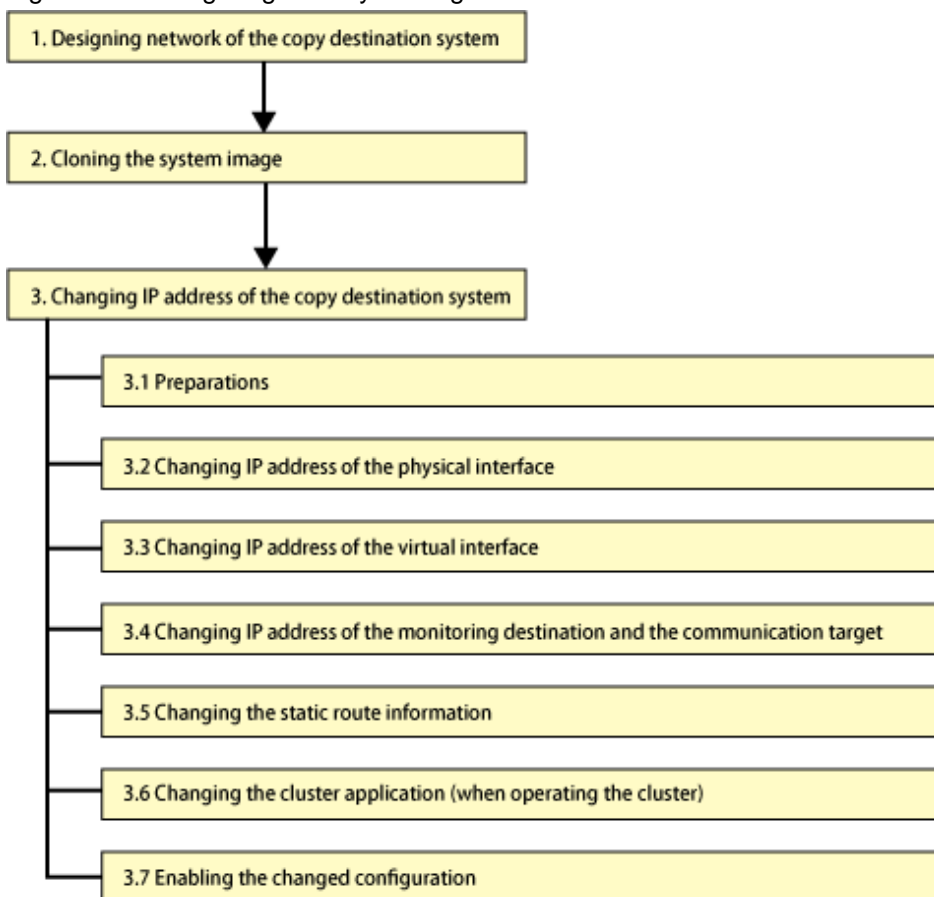
## Note

- The copy source and the copy destination including the hardware configurations (models and disk/NIC implemented locations) must be identical.
- Cloning follows the condition of the cloning software to be used and the cloning function.
- Before cloning the cluster system, see the manual "PRIMECLUSTER Installation and Administration Guide" to understand the procedure to change the whole cluster system.

## Configuring by cloning

The procedure to configure GLS by cloning is as follows.

Figure G.1 Configuring GLS by cloning



## G.1 Designing network of the copy destination system

On the TCP/IP network, the unique IP address is assigned to each node to identify the communication target node. If the same IP address is assigned to multiple nodes, normal communication is disabled.

When cloning the system, the setting of the IP address of the copy source system is transferred to the copy destination system without change. Therefore, the IP address must be changed to avoid the duplication of the IP address between the copy destination system and the copy source system. The IP address of the monitoring destination or the IP address of the communication target also must be changed when the copy destination system is connected to the network different from the network on the copy source system. In this case, before cloning the system, list all the IP addresses that should be changed on the copy destination system, and design how the value of these IP addresses should be changed.

Later sections describe the example of how to design the network for each communication mode.

## G.1.1 Designing the network of Fast switching mode

When cloning the system of Fast switching mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Physical interface
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system.

[Design example 1: Fast switching mode - Single system]

Below is the design example of how to clone HOST-A of "[B.1.1 Example of the Single system.](#)"

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual interface	sha0	192.168.80.1	192.168.180.1
	Physical interface	eth0	192.168.70.1	192.168.170.1
		eth1	192.168.71.1	192.168.171.1

[Design example 2: Fast switching mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "[B.1.4 Example of the Cluster system \(1:1 Standby\).](#)"

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual interface	sha0	192.168.80.1	192.168.180.1
	Physical interface	eth0	192.168.70.1	192.168.170.1
		eth1	192.168.71.1	192.168.171.1
HOST-B	Virtual interface	sha0	192.168.80.2	192.168.180.2
	Physical interface	eth0	192.168.70.2	192.168.170.2
		eth1	192.168.71.2	192.168.171.2
Takeover virtual interface		sha0:65	192.168.80.3	192.168.180.3

## G.1.2 Designing the network of NIC switching mode

When cloning the system of NIC switching mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Physical interface
- Monitoring destination IP of the HUB monitoring function (when the destination HUB is different)
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system. Check the IP address of the router on the destination network in advance as well when the copy destination system is connected to the network different from the network on the copy source system.

[Design example 3: NIC switching mode - Single system]

Below is the design example of how to clone HOST-A of "B.2.1 Example of the Single system without NIC sharing".

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Logical IP address	sha0/	192.168.70.1	192.168.170.1
	Physical IP address	eth0/ eth1	192.168.70.2	192.168.170.2
	HUB		192.168.70.100 192.168.70.101	192.168.170.100 192.168.170.101

[Design example 4: NIC switching mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "B.2.8 Example of the Cluster system (1:1 Standby)".

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Logical IP address	sha0/	192.168.70.1	192.168.170.1
	Physical IP address	eth0/ eth1	192.168.70.2	192.168.170.2
	HUB		192.168.70.100 192.168.70.101	192.168.170.100 192.168.170.101
HOST-B	Logical IP address	sha0/	192.168.70.1	192.168.170.1
	Physical IP address	eth0/ eth1	192.168.70.3	192.168.170.3
	HUB		192.168.70.100 192.168.70.101	192.168.170.100 192.168.170.101
Takeover virtual interface		sha0:65	192.168.70.1	192.168.170.1

### G.1.3 Designing the network of Virtual NIC mode

When cloning the system of Virtual NIC mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Monitoring destination IP of the network monitoring function (when the destination HUB is different)
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system. Check the IP address of the router on the destination network in advance as well when the copy destination system is connected to the network different from the network on the copy source system.

[Design example 5: Virtual NIC mode - Single system]

Below is the design example of how to clone HOST-A of "B.3.1 Example of the Single system."

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual IP address	sha0	192.168.80.1	192.168.180.1
	HUB		192.168.80.100 192.168.80.101	192.168.180.100 192.168.180.101

[Design example 6: Virtual NIC mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "B.3.3 Example of the Cluster system (1:1 Standby)."

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual IP address	sha0	192.168.80.1	192.168.180.1
	HUB		192.168.80.100	192.168.180.100
			192.168.80.101	192.168.180.101
HOST-B	Virtual IP address	sha0	192.168.80.2	192.168.180.2
	HUB		192.168.80.100	192.168.180.100
			192.168.80.101	192.168.180.101
Takeover virtual interface		sha0:65	192.168.80.3	192.168.180.3

## G.1.4 Designing the network of GS linkage mode

When cloning the system of GS linkage mode, the following IP addresses must be changed on the copy destination system.

- Virtual interface
- Physical interface
- Virtual gateway
- Remote host (when the destination host is different)
- IP address of the local router (for remote network communication)
- Takeover virtual interface (for cluster system)

Before cloning the system, see the following examples to decide the IP address to be assigned to the copy destination system.

[Design example 7: GS linkage mode - Single system]

Below is the design example of how to clone HOST-A of "[B.6.1 Example of the Single system.](#)"

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual interface	sha0	192.168.80.1	192.168.180.1
	Virtual gateway		192.168.80.254	192.168.180.254
	Physical interface	eth0	192.168.70.1	192.168.170.1
		eth1	192.168.71.1	192.168.171.1
GS-1	Virtual IP address	Virtual IP	192.168.81.2	192.168.181.2
	Real IP address	IP-1	192.168.70.2	192.168.170.2
		IP-2	192.168.71.2	192.168.171.2

[Design example 8: GS linkage mode - Cluster system (1:1 Active standby)]

Below is the design example of how to clone HOST-A and HOST-B of "[B.6.5 Example of the Cluster system \(1:1 Standby\).](#)"

IP address to be changed			Value in copy source	Value in copy destination
HOST-A	Virtual interface	sha0	192.168.80.1	192.168.180.1
	Virtual gateway		192.168.80.254	192.168.180.254
	Physical interface	eth0	192.168.70.1	192.168.170.1
		eth1	192.168.71.1	192.168.171.1
HOST-B	Virtual interface	sha0	192.168.80.1	192.168.180.1
	Virtual gateway		192.168.80.254	192.168.180.254
	Physical interface	eth0	192.168.70.2	192.168.170.2

IP address to be changed		Value in copy source	Value in copy destination
	eth1	192.168.71.2	192.168.171.2
Takeover virtual interface		sha0:65	192.168.80.1
GS-1	Virtual IP address	Virtual IP	192.168.81.3
	Real IP address	IP-1	192.168.70.3
		IP-2	192.168.71.3

## G.2 Copying the system image

Copy the system image to the copy destination system.

For the setting values of the OS and other middleware, see the manuals for each product and change them.

### Note

- Before starting the copy destination system, unplug the NIC cable, stop the copy source system, or connect the copy destination system with the network separated from the copy source system to prevent the duplicated IP address between the copy destination system and the copy source system.
- The MAC address of NIC differs between the copy source system and the copy destination system. Update the MAC address either by initializing the setting of NIC when cloning or by modifying the setting of NIC manually after cloning depending on the cloning software or the cloning function you are using.
- After cloning the cluster system, start the copy destination system in single user mode to configure the setting to stop the automatic start of RMS. After this setting, change the configuration of the copy destination system. For details, see "[G.3.1 Preparations](#)."

## G.3 Changing the setting of the copy destination system

This section explains how to change the setting of GLS in the copy destination system. When cloning the system operated by cluster, see the manual "PRIMECLUSTER Installation and Administration Guide."

### Information

- The procedure explained below is available when all the GLS setting is specified by the IP address (decimal dotted notation). When cloning the environment where the virtual interface or the monitoring destination is set by specifying the host name, the GLS setting can be changed by changing the IP address that is described in the /etc/hosts file in the copy destination environment, and then, by restarting OS.
- If the IP address is described in the script that is executed by the user command execution function, modify the script file according to the copy destination environment.

### Note

When starting OS in multi user mode before the setting of GLS is changed, unplug the NIC cable, stop the copy source system, or connect the network separated from the copy source system in advance to prevent the duplicated IP address between the copy destination system and the copy source system.

### G.3.1 Preparations

Before changing the setting of GLS in the copy destination system, configure the following setting.

## 1. Modifying the /etc/hosts file

Before changing the setting of GLS, start OS in single user mode. After that, change the IP address that is described in the /etc/hosts file to the IP address that is previously specified in "[G.1 Designing network of the copy destination system](#)." Change the host name if necessary.

Below is the example when changing the IP address of HOST-A in [Design example 1: Fast switching mode - Single system].

[Before change]

```
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
```

[After change]

```
192.168.170.1  host11    # HOST-A Physical IP
192.168.171.1  host12    # HOST-A Physical IP
192.168.180.1  hosta     # HOST-A Virtual IP
```

## 2. Deleting the setting of takeover virtual interface in GLS

When cloning the system where GLS is operated by the cluster, check that RMS is stopped. After that, delete all the setting of takeover virtual interface.

```
# /opt/FJSVhanet/usr/sbin/hanethvrsc delete -n all
```

## G.3.2 Changing the IP address of the physical interface

Change the IP address of the physical interface of Fast switching mode or GS linkage mode, and change the IP address of the primary physical interface of NIC switching mode to the IP address that is preliminary specified in "[G.1 Designing network of the copy destination system](#)." For Virtual NIC mode, this process is not necessary because the IP address is not assigned to the physical interface.

For RHEL8, edit the setting of the physical interface (etc/sysconfig/network-scripts/ifcfg-ethX file), and modify the IP address, netmask, network address, and broadcast address according to the copy destination environment. For RHEL9, edit the setting of the physical interface with the nmcli command. If the default gateway is described, also modify the gateway address according to the copy destination environment.

Below is the example when changing the setting of eth0 in [Design example 1: Fast switching mode - Single system].

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

[Before change]

```
DEVICE=eth0
BOOTPROTO=static
HOTPLUG=no
IPADDR=192.168.70.1
NETMASK=255.255.255.0
ONBOOT=yes
TYPE=Ethernet
```

[After change]

```
DEVICE=eth0
BOOTPROTO=static
HOTPLUG=no
IPADDR=192.168.170.1
NETMASK=255.255.255.0
ONBOOT=yes
TYPE=Ethernet
```

## G.3.3 Changing the IP address of the virtual interface

Change the IP address of the virtual interface according to "G.1 Designing network of the copy destination system." Below is the example for each communication mode.

### Fast switching mode

Take the following steps to change the IP address that is described in the design example in "G.1.1 Designing the network of Fast switching mode."

[How to change in design example 1: Fast switching mode - Single system]

1. Changing the subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.80.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.180.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

[How to change in design example 2: Fast switching mode - Cluster system (1:1 Active standby)]

1. Changing the subnet mask (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.80.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.180.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface (HOST-A)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

3. Changing the IP address of the virtual interface (HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.2
```

4. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.180.3
```

### NIC switching mode

Take the following steps to change the IP address that is described in the design example in "G.1.2 Designing the network of NIC switching mode"

[How to change in design example 3: NIC switching mode - Single system]

1. Changing the subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.70.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.170.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e
192.168.170.2
```

[How to change in design example 4: NIC switching mode - Cluster system (1:1 Active standby)]

1. Changing the subnet mask (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.70.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.170.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface (HOST-A)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e
192.168.170.2
```

3. Changing the IP address of the virtual interface (HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.170.1 -e
192.168.170.3
```

4. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

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

## Virtual NIC mode

Take the following steps to change the IP address that is described in the design example in "[G.1.3 Designing the network of Virtual NIC mode](#)."

[How to change in design example 5: Single system]

1. Changing the IP address of the virtual interface

Edit the setting of the virtual interface and modify the IP address or the prefix. If the default gateway is described, also modify the gateway address according to the copy destination environment.

- For RHEL8

Edit the setting of the virtual interface (/etc/sysconfig/network-scripts/ifcfg-sha0).

```
DEVICE=sha0
IPADDR=192.168.180.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

```
ipv4.method: "manual"
ipv4.addresses: "192.168.180.1/24"
```

[How to change in design example 6: Cluster system (HOST-A)]

1. Changing the IP address of the virtual interface

Edit the setting of the virtual interface and modify the IP address or the prefix. If the default gateway is described, also modify the gateway address according to the copy destination environment.

- For RHEL8

Edit the setting of the virtual interface (/etc/sysconfig/network-scripts/ifcfg-sha0).

[HOST-A]



```
DEVICE=sha0
IPADDR=192.168.180.1
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

[HOST-B]

```
DEVICE=sha0
IPADDR=192.168.180.2
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

- For RHEL9

Set the following parameters to sha0 with the "nmcli connection modify" command.

[HOST-A]

```
ipv4.method: "manual"
ipv4.addresses: "192.168.180.1/24"
```

[HOST-B]

```
ipv4.method: "manual"
ipv4.addresses: "192.168.180.2/24"
```

2. Changing the subnet mask (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.80.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.180.0 -m
255.255.255.0
```

3. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanethvrsc create -n sha0 -i 192.168.180.3
```

## GS linkage mode

Take the following steps to change the IP address that is described in the design example in "[G.1.4 Designing the network of GS linkage mode.](#)"

[How to change in design example 7: GS linkage mode - Single system]

1. Changing the subnet mask

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.80.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.180.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

3. Changing the IP address of the virtual gateway

```
/opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.180.254
```

4. Changing the static route information for the virtual IP address of the remote host in RHEL8

Edit the `/etc/sysconfig/network-scripts/route-sha0` file to modify the static route information of the virtual gateway for the virtual IP address of the remote host.

```
GATEWAY0=192.168.180.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.181.2 # Virtual IP of the remote host
```

[How to change in design example 8: GS linkage mode - Cluster system (1:1 Active standby)]

1. Changing the subnet mask (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetmask delete -i 192.168.80.0
/opt/FJSVhanet/usr/sbin/hanetmask create -i 192.168.180.0 -m
255.255.255.0
```

2. Changing the IP address of the virtual interface (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetconfig modify -n sha0 -i 192.168.180.1
```

3. Changing the IP address of the virtual gateway (both HOST-A and HOST-B)

```
/opt/FJSVhanet/usr/sbin/hanetgw delete -n sha0
/opt/FJSVhanet/usr/sbin/hanetgw create -n sha0 -g 192.168.180.254
```

4. Changing the static route information for the virtual IP address of the remote host (both HOST-A and HOST-B) in RHEL8

Edit the `/etc/sysconfig/network-scripts/route-sha0` file to modify the static route information of the virtual gateway for the virtual IP address of the remote host.

```
GATEWAY0=192.168.180.254 # Virtual gateway
NETMASK0=255.255.255.255 # Subnet mask
ADDRESS0=192.168.181.3 # Virtual IP of the remote host
```

5. Reconfiguring the takeover virtual interface (both HOST-A and HOST-B)

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

## G.3.4 Changing the IP address of the monitoring destination and the remote host

Change the IP address in the destination of the HUB monitoring and the IP address of the remote host according to "[G.1 Designing network of the copy destination system](#)." If the IP address is not necessary to be changed, move to the next step.

Below is the example for each communication mode.

### Fast switching mode

The IP address in the monitoring destination is not set. In this case, no IP address is necessary to be changed.

### NIC switching mode

Take the following procedure to change the IP address that is described in "[G.1.2 Designing the network of NIC switching mode](#)"

Execute the `hanetpoll modify` command to change the IP address in the monitoring destination in each copy destination system.

[Setting of design example 3 and design example 4 common for each HOST]

```
# /opt/FJSVhanet/usr/sbin/hanetpoll modify -n sha0 -p 192.168.170.100,192.168.170.101
```

#### Virtual NIC mode

Take the following procedure to change the IP address that is described in "[G.1.3 Designing the network of Virtual NIC mode.](#)"

Execute the hanetpathmon target command to change the IP address in the monitoring destination in each copy destination system.

[Setting of design example 5 and design example 6 common for each HOST]

```
# /opt/FJSVhanet/usr/sbin/hanetpathmon target -n sha0 -p
192.168.180.100,192.168.180.101
```

#### GS linkage mode

Take the following procedure to change the IP address that is described in "[G.1.4 Designing the network of GS linkage mode.](#)"

Execute the hanetobserv command to change the IP address of remote host in each copy destination system.

[Setting in design example 7]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n GS-1
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.181.2 -t
192.168.170.2,192.168.171.2
```

[Setting of design example 8 common for each HOST]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n GS-1
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS-1 -i 192.168.181.3 -t
192.168.170.3,192.168.171.3
```

When cloning the system where GLS is operated by the cluster, also change the monitoring setting between the active node and the standby node.

[HOST-A setting of design example 8]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n HOST-B
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-B -i 192.168.180.1 -t
192.168.170.2,192.168.171.2
```

[HOST-B setting of design example 8]

```
# /opt/FJSVhanet/usr/sbin/hanetobserv delete -n HOST-A
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n HOST-A -i 192.168.180.1 -t
192.168.170.1,192.168.171.1
```

## G.3.5 Changing the static route information

---

When connecting the copy destination system with the network different from the network in the copy source system, modify the static route information including the default gateway according to the environment of the destination environment.

For RHEL8, modify the gateway address that is described in the /etc/sysconfig/network file, in the /etc/sysconfig/network-scripts/route-interface name file, or in the /etc/sysconfig/network-scripts/ifcfg-interface name file if necessary.

For RHEL9, modify the gateway address by the "nmcli connection modify" command if necessary.

## G.3.6 Changing the setting of cluster application (in cluster operation)

---

If the takeover IP address of the cluster is changed in "[G.3.3 Changing the IP address of the virtual interface](#)", use the RMS Wizard to change the IP address of the GIs resource in the cluster environment configuration.

In the menu to configure the takeover IP address of the GIs resource, select the changed takeover IP address to change the IP address.

For details, see "PRIMECLUSTER Installation and Administration Guide".

## **G.3.7 Enabling the changed setting**

---

After the IP address is changed in the copy destination system, restart OS to check if the IP address is changed properly. Take the following step.

1. Starting OS in multi user mode

Restart OS in multi user mode.

2. Checking the IP address

After OS is restarted, check if the changed IP address is enabled. Check if the following procedure is complete.

- The changed IP address is set for each physical interface and for each virtual interface.
- The changed static route information including the default gateway for each routing table.
- The changed IP address is set for the monitoring target IP address and the monitoring works properly (in NIC switching mode and virtual NIC mode).
- The IP address of the communication target The changed IP address is set for the IP address of the communication target, and the monitoring works properly (in GS linkage mode).
- After RMS is started, the changed takeover IP address is set for the active node of the cluster. After that, when the node is switched, the changed takeover IP address is set for the standby node (in cluster system).

# Appendix H Troubleshooting

The cause of the frequently occurred trouble when using a Redundant Line Control Function and how to deal with it are explained in this section.

## H.1 Communication as expected cannot be performed (Common to IPv4 and IPv6)

### H.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](#)".

### H.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 fewer minutes interval.

### H.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

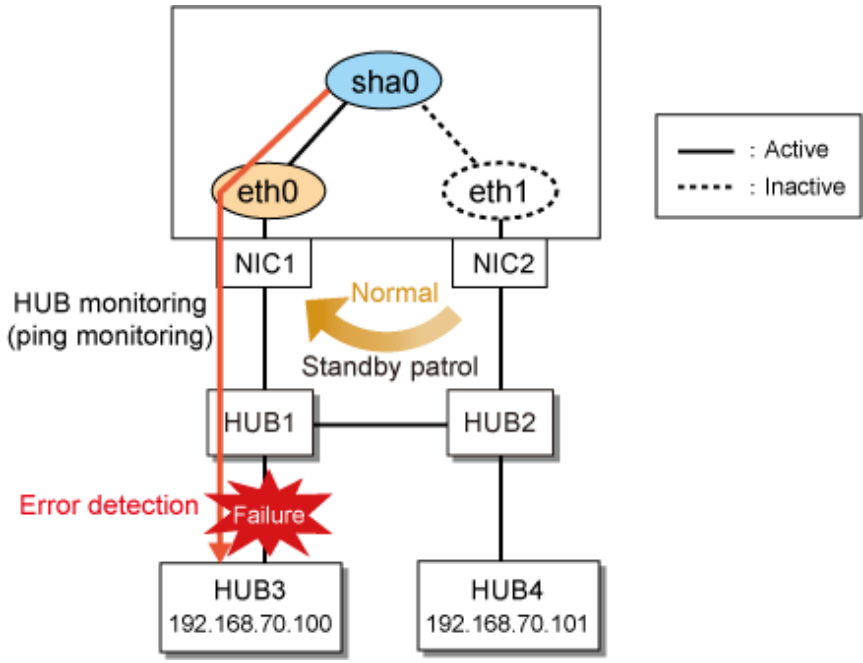
Examples for "when the communication is not switched" and "when the communication is switched" are shown below.

 **Example**

**When the communication is not switched**

In the case of [Figure H.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 H.1 When the communication is not switched



 **Example**

**When the communication is switched**

In the case of [Figure H.2 When the communication is switched \(1\)](#) and [Figure H.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 H.2 When the communication is switched (1)

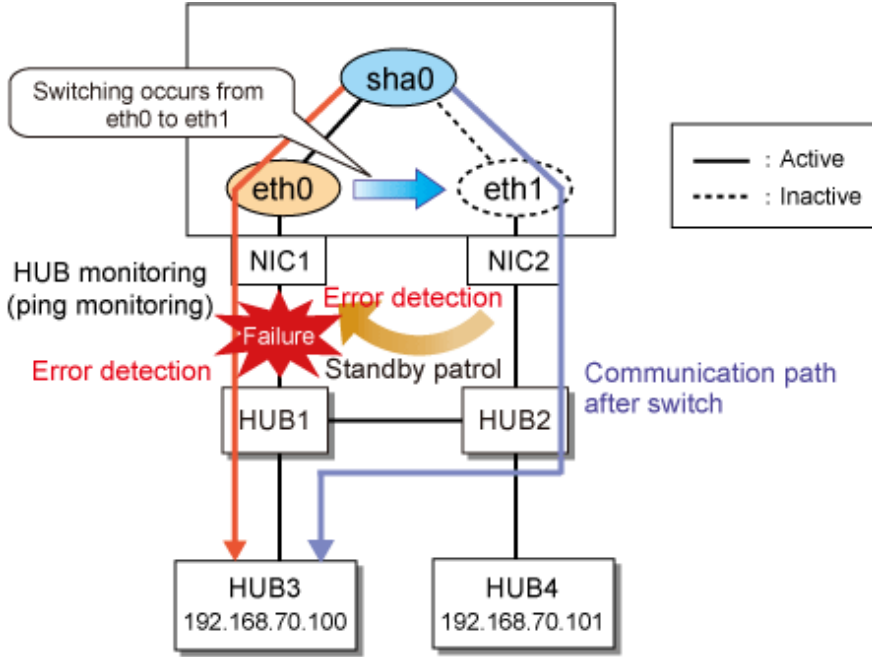
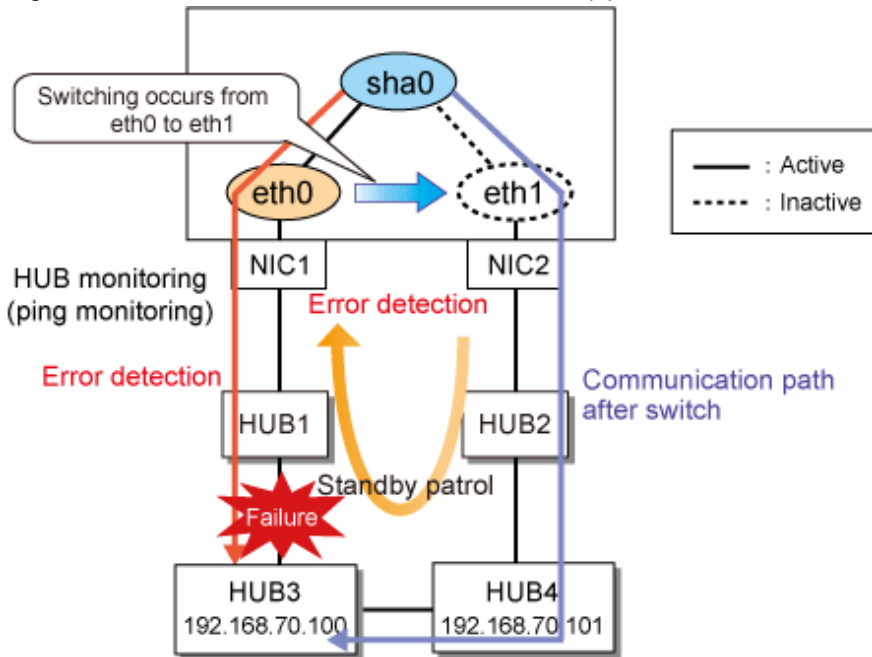


Figure H.3 When the communication is switched (2)




---

## H.2 Virtual interface or the various functions of Redundant Line Control Function cannot be used

---

### H.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 userApplication fails on cluster system.

When using a logical IP 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 monitor-to information that defined initially using a hanetpoll copy command.

## H.2.2 The immediate automatic fail-back is not executed when the standby patrol is recovered in NIC switching mode

---

### Symptom:

The following message is displayed when the standby patrol is recovered in NIC switching mode, and the immediate automatic fail-back is not executed 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.

## H.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.



## H.3 Failure occurs during operation (Common to both Single and Cluster system)

### H.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.

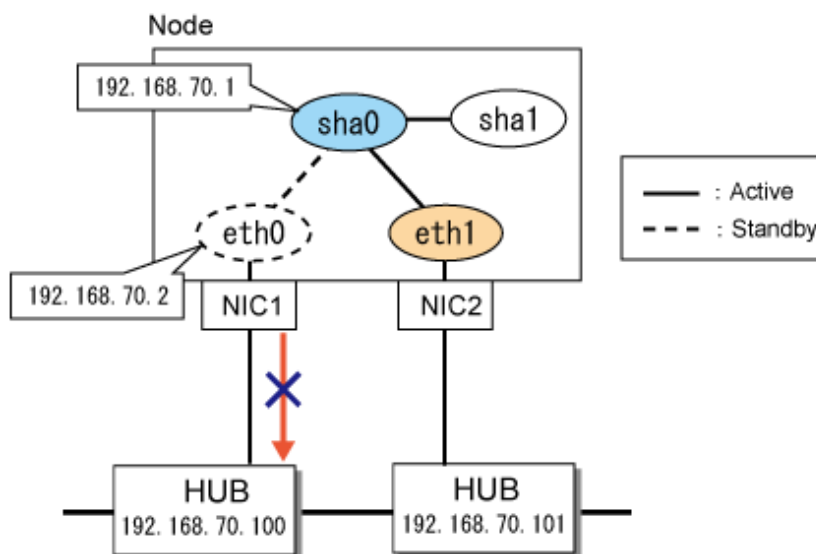
```
hanet: ERROR: 87000: polling status changed: Primary polling failed.
(eth0,target=192.168.70.100)
```

```
# /opt/FJSVhanet/usr/sbin/dsppoll

Polling Status      = ON
interval(idle)     = 5( 60)
times               = 5
link detection      = YES
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

GLS: Global Link Services

- 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

GLS: Global Link Services

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.

Confirmation item		Contents
	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>
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. Confirm that the Netmask is set by the ip 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)
	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	<p>Errors may occur in VLAN-ID settings. Confirm whether the following VLAN-IDs are in accordance.</p> <p>1) VLAN-ID of the port connected with the cable of primary NIC</p> <p>2) VLAN-ID of the port connected with the cable of secondary NIC</p> <p>3) VLAN-ID that is set as a monitored target by the management IP address of HUB</p>
	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

Confirmation item		Contents
		sent packets etc. by a command such as the sar command in Linux environment. In addition, in the environment where the network with different types of speed 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 a command such as the ss 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	Run a command such as the ip route command to confirm that there is no transmission path on the same network as the virtual IP address of GLS. 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.

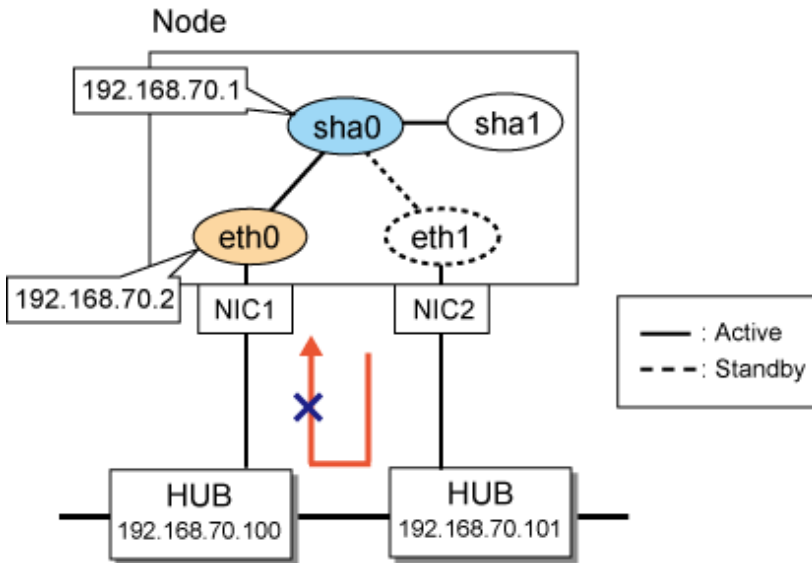
GLS: Global Link Services

### **H.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

Message output patterns	Confirmation items	
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	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)
	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.

Confirmation item		Contents
	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 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 a command such as the sar command in Linux. In addition, in the environment where the network with a different speed 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.

### H.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.

### H.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 userApplication or to switch nodes on cluster system.

**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.

### H.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 the NIC switching mode.

**Corrective action:**

When using the logical IP address takeover function in the 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. 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.

 **Point**

.....  
When using the physical interface ethX, the takeover virtual interface and the logical interface are displayed as the secondary addresses of ethX by the ip command.  
.....

Figure H.4 The remote host is the transmitting side.

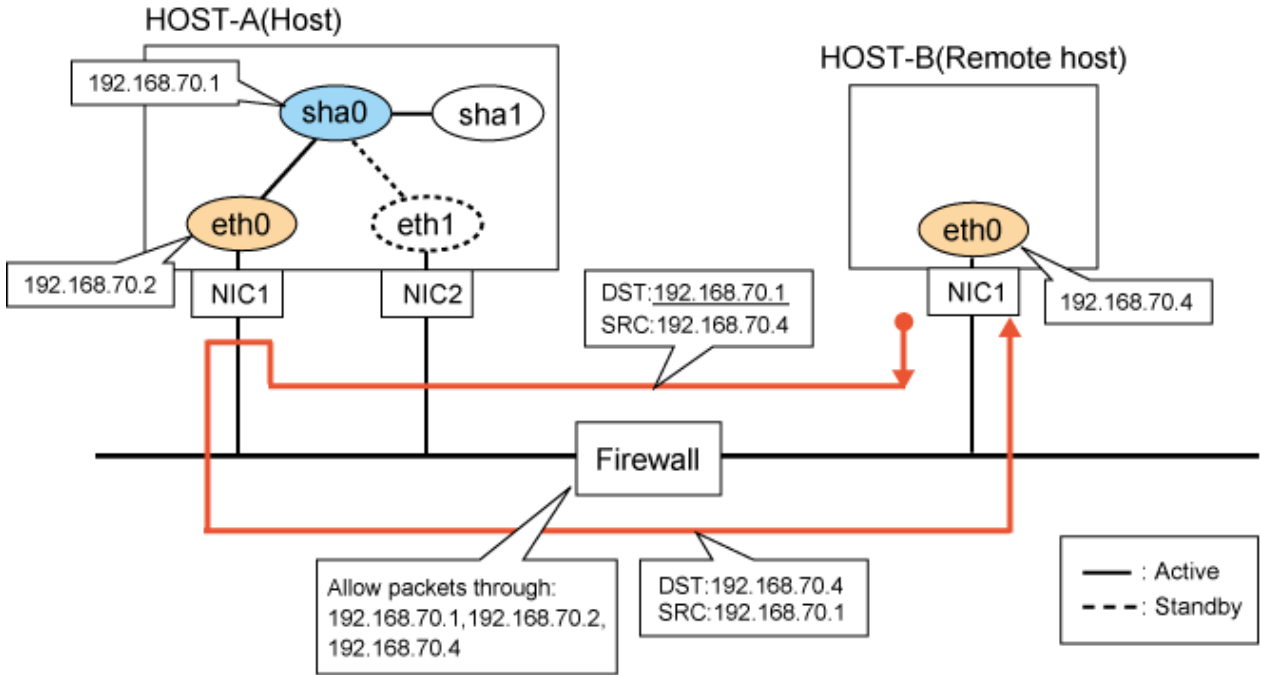
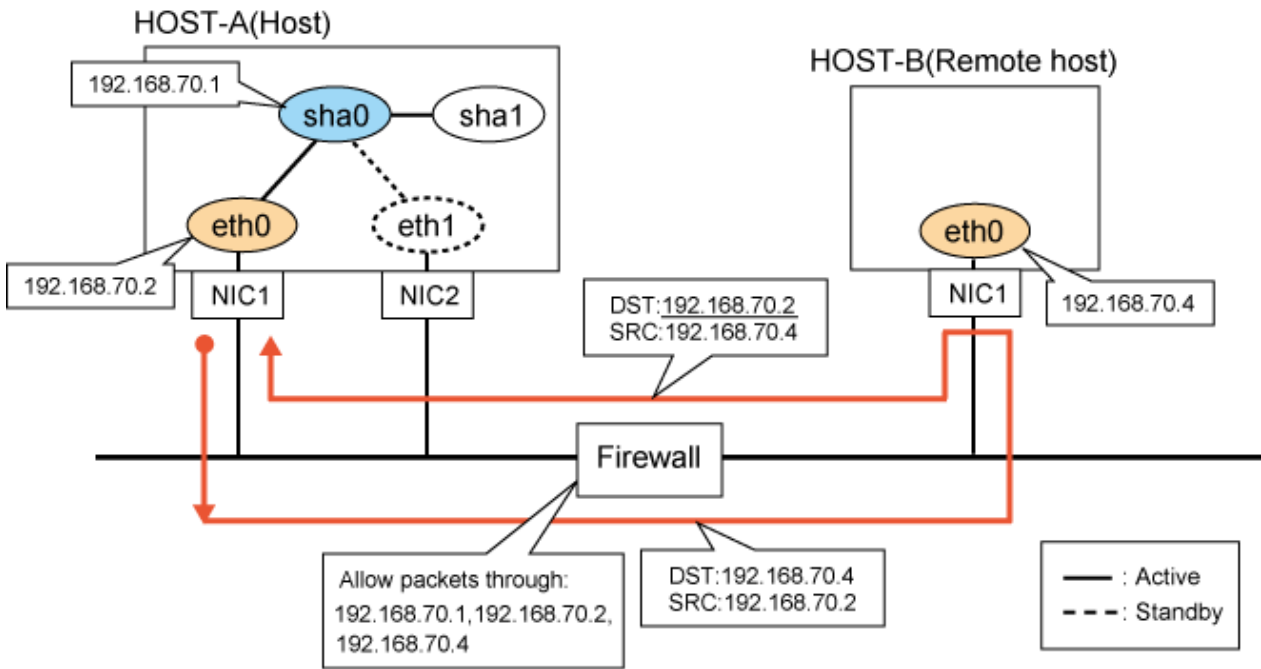


Figure H.5 The local host is the transmitting side.



### H.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 60 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 120  <- Set time for detecting a virtual driver hang in seconds
```

2. Restart the operating system.

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



If the configuration file is backed up in 4.3A40 or earlier environment, the above settings cannot be restored by the restoration function. Set the file again depending on the environment.

## H.4 Failure occurs during operation (In the case of a Cluster system)

### H.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
```

## H.5 Resuming connection lags after switching (Common to both Single and Cluster system)

---

### H.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.

## H.6 Incorrect operation by the user

---

### H.6.1 Accidentally deleted the virtual interface

---

#### Symptom:

Unable to recover the virtual interface (sha) deleted with the ifconfig command or the ip command by accident.

#### Corrective action:

After the virtual interface (sha) is disabled by the ifconfig command or the ip command in Fast switching mode, the behavior of the strhanet/stphanet command cannot be guaranteed. Follow the procedure below to recover the virtual interface if it is disabled by mistake.

#### [Example 1]

Accidentally executing "ifconfig sha0 down" against the 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
```

#### [Example 2]

Accidentally executing "ip link set sha0 down" against the virtual interface sha0 for Fast switching mode.

```
If IPv4 address is being used:  
# ip link set sha0 up
```

#### [Example 3]

Accidentally deleting the IP address against the virtual interface sha0 for Fast switching mode.

```
If IPv4 address is being used:  
# ip -f inet addr add IPv6 address/prefixlen dev sha0
```



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.

## H.6.2 Cluster applications are switched or stopped during maintenance work of network devices

---

### Symptom:

A Gls resource failure occurs, and then cluster applications are switched or stopped.

### Corrective action:

During operation, due to the effect of maintenance work such as replacing or restarting a HUB, changing a cable connection, and shutting down a network to take security measures, the GLS monitoring function detects a failure, and then cluster applications may be switched or stopped. In this case, perform the following procedure to recover all the failed nodes.

#### 1. Recovering the transfer path where a failure has occurred

Restore the failed transfer path to the normal status (perform necessary work such as reconnecting the cable, powering on the switch/HUB again, and replacing the failed switch/HUB).

#### 2. Checking the GLS status

##### - Fast switching mode

Make sure that the status of the communication target is Active by using the dsphanet command with the -o option.

##### - GS linkage mode

Make sure that the status of the communication target is Active by using the dspobserv command.

##### - NIC switching mode

Make sure that the status of HUB monitoring is ON by using the dspool command.

Also, make sure that the status of the standby patrol is ON by using the dsphanet command.

##### - Virtual NIC mode

Make sure that the status of HUB monitoring is ON and the status of the standby patrol is Active by using the dspathmon command.

#### 3. Clearing the Gls resource failure status

Clear the Gls resource failure status by using "Cluster Admin" in Web-Based Admin View.

#### 4. Restoring the original operation status

Restore the original operation status by restarting the cluster applications or performing fail-back operation for the cluster applications, from "Cluster Admin" in Web-Based Admin View.

# Appendix I Check list

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

## I.1 Checkpoint list

Table I.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="#">Hostname settings</a>	If GLS is set using the hostname rather than an IP address, enable the "hostname translation function".	OK/NG
8	<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
9	<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
10	<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
11	<a href="#">Application</a>	Check that the application to be used is the TCP/IP application using TCP and UDP.	OK/NG

GLS: Global Link Services

Table I.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 I.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
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 I.4 Virtual NIC mode

NO	Checkpoint	Description	Check field
1	<a href="#">Interface setting file</a>	Check that the IP addresses, subnet masks, or prefixes 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

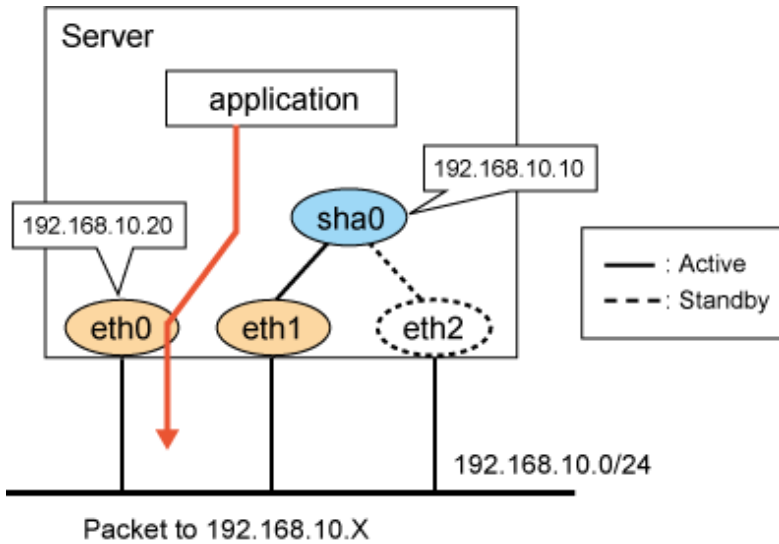
Table I.5 GS linkage mode

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

## I.2 Setup common to modes

### I.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

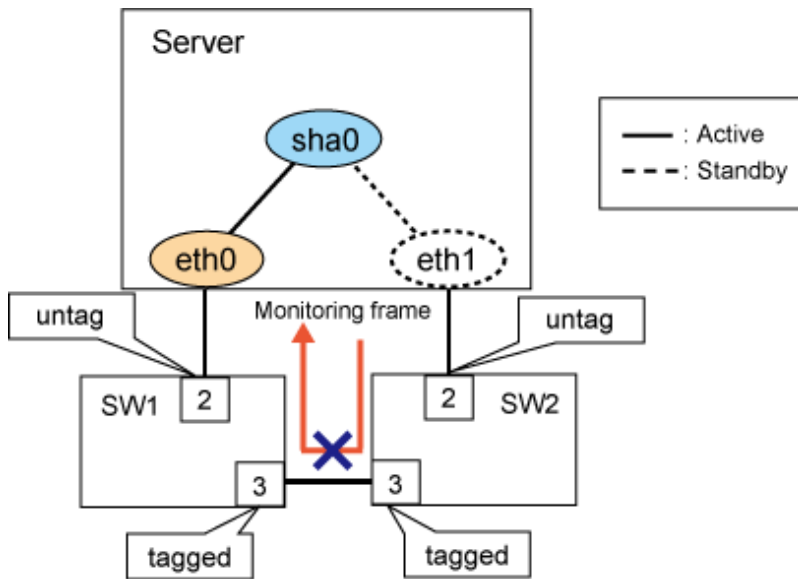
- Use a command such as the ip route command to check that the same network address is not set for a different device. In the following execution example, different devices have been set to the same network. Therefore, you need to change the network address of the either of the two.

```
# ip route
192.168.10.0/24 dev eth0 proto kernel scope link src 192.168.10.20
192.168.10.0/24 dev sha0 proto kernel scope link src 192.168.10.10
```

### I.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).





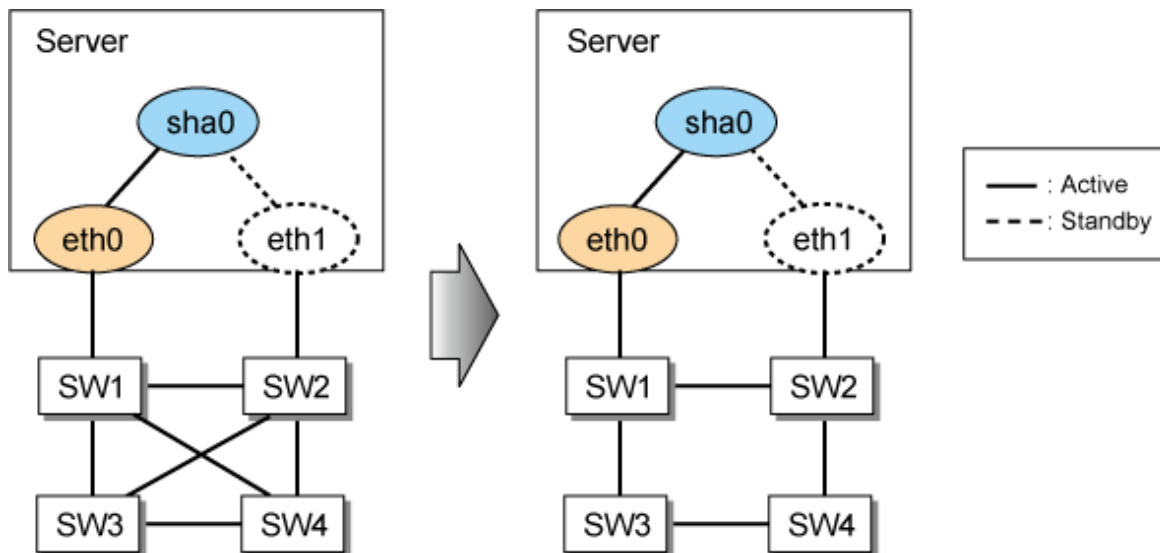
### Confirmation method

Check the VLAN settings of network devices

## I.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.

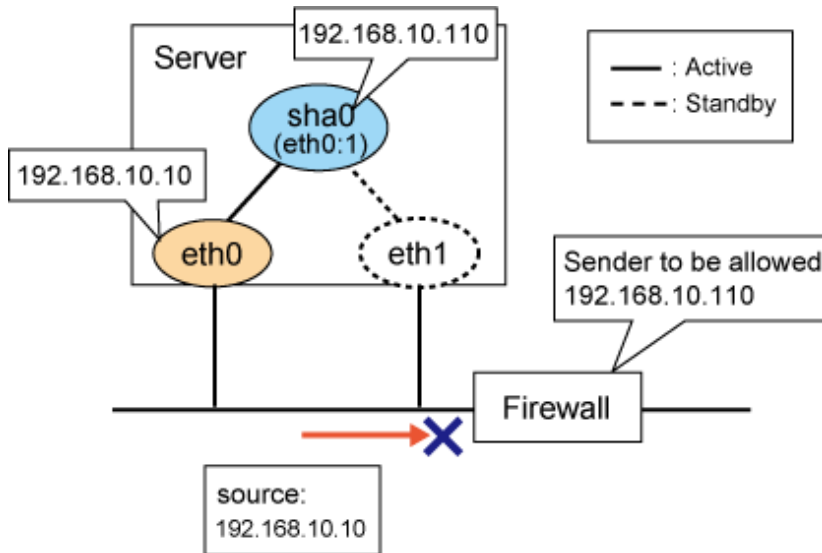


### Confirmation method

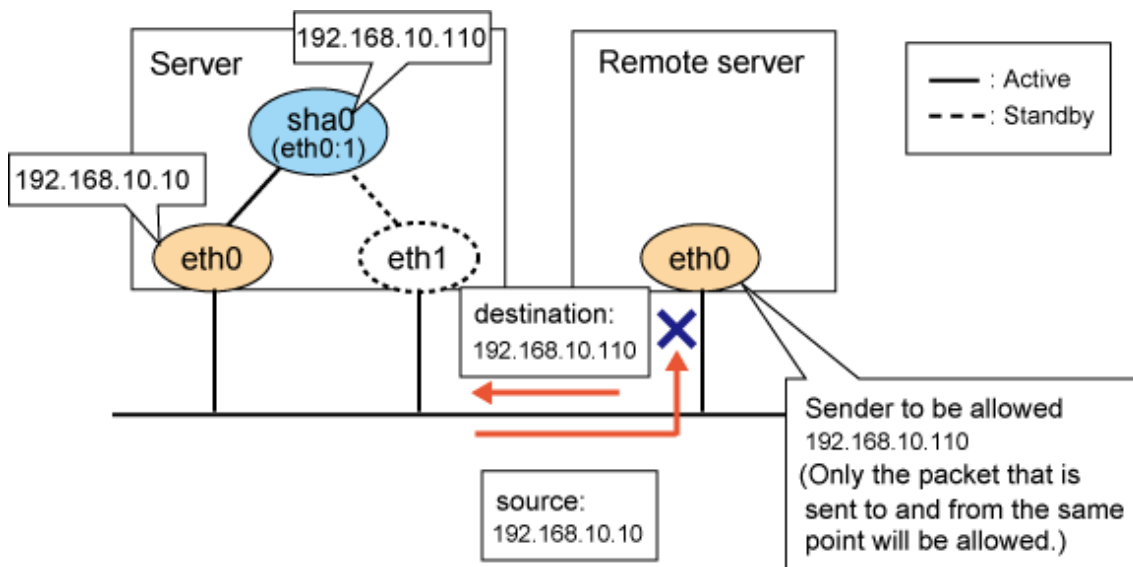
Check the connection of the network configuration diagram.

## I.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 "[H.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.



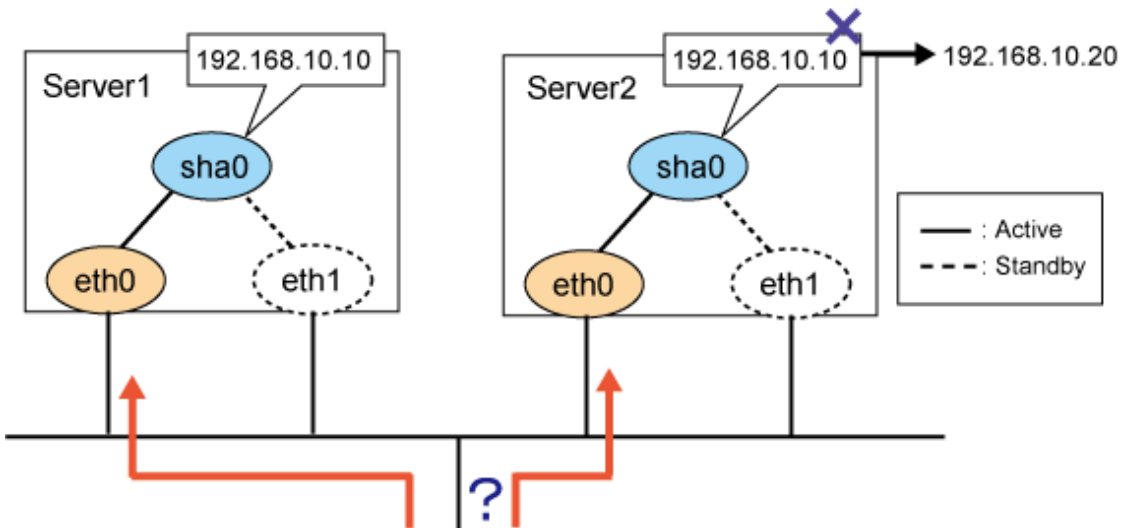
### Confirmation method

Check the filtering settings for the firewall and the communication target.

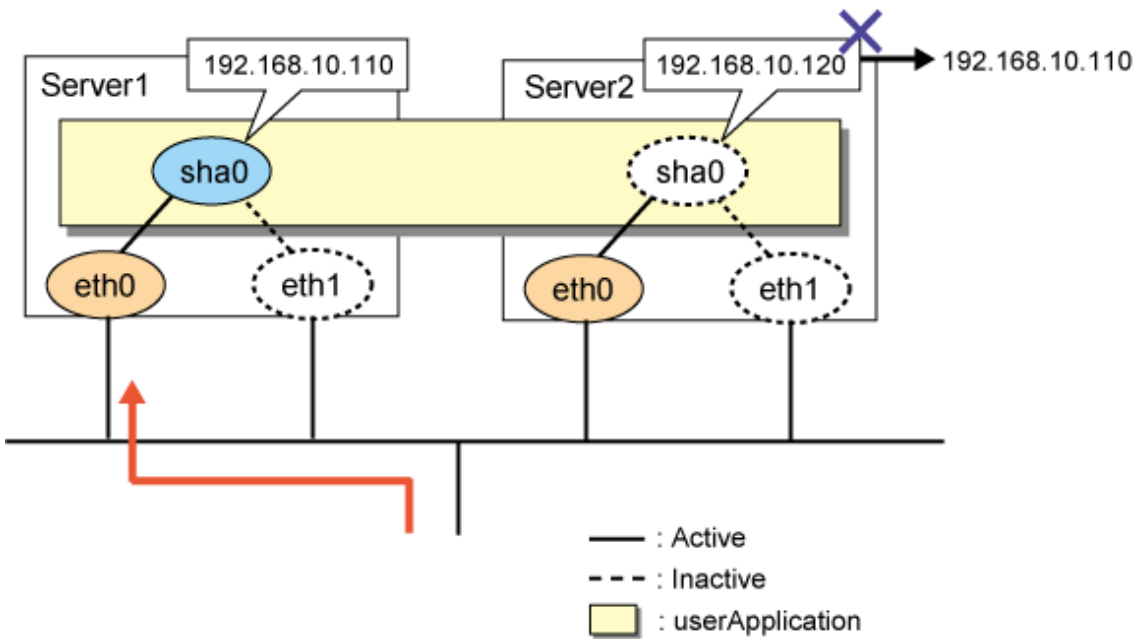
## I.2.5 IP address settings

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  -              -

```

## I.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 netmask 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          192.168.11.110  d                192.168.11.110  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  -                 -
sha1:65       192.168.11.110  -                 -
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"

## I.2.7 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

```

### I.2.8 Distribution procedure after settings change

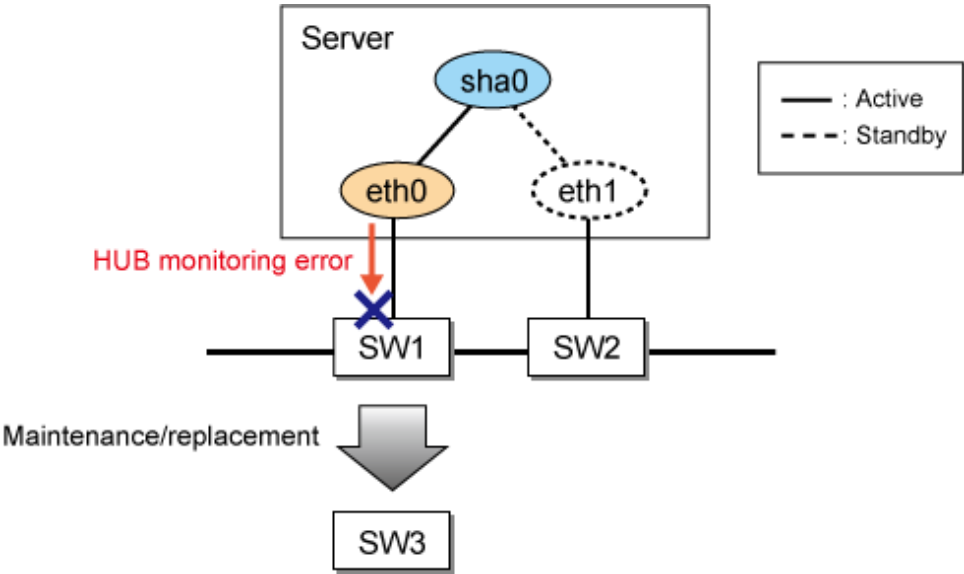
If you have changed the GLS settings, you need to distribute the reboot and other settings for operations. Check that the distribution procedure has been performed. For details, see "3.4 Changing system setup"

**Confirmation method**

Check the procedure manual for settings changes.

### I.2.9 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.

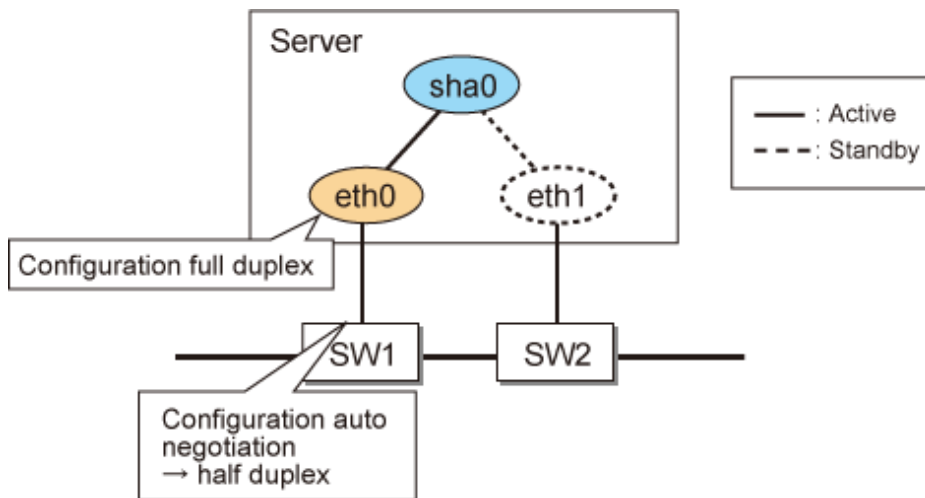
```

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

```

## I.2.10 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
```

## I.2.11 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.



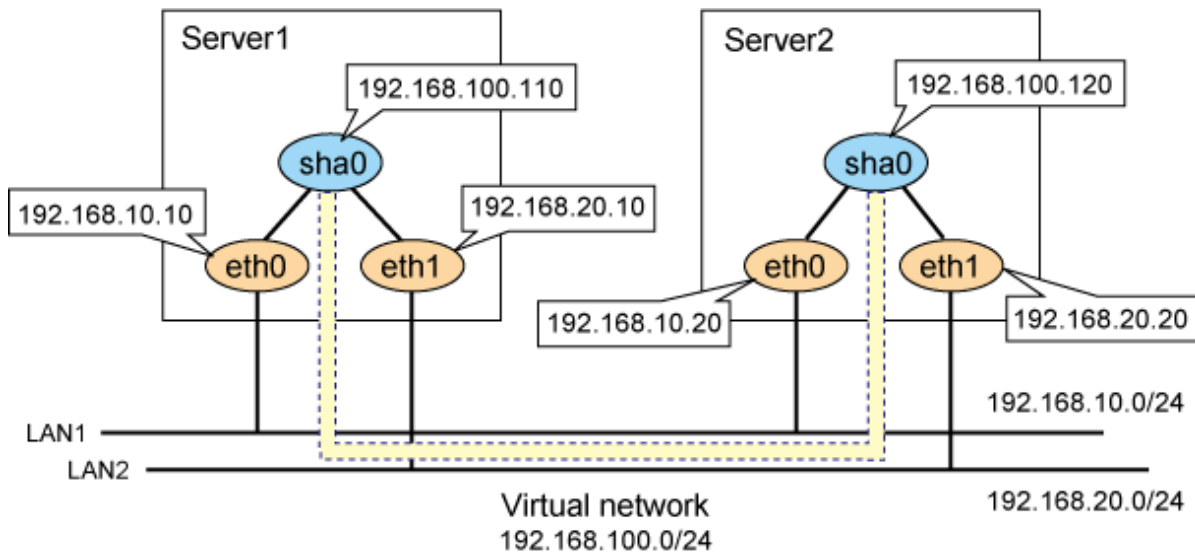
See

- "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"

## I.3 Fast switching mode

### I.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 a command such as the ip route command to check that the network address has been assigned correctly. The following is an example of display when the command is run on the server 1.

```
# ip route
192.168.10.0/24 dev eth0 proto kernel scope link src 192.168.10.10
192.168.20.0/24 dev eth1 proto kernel scope link src 192.168.20.10
192.168.100.0/24 dev sha0 proto kernel scope link src 192.168.100.110
```

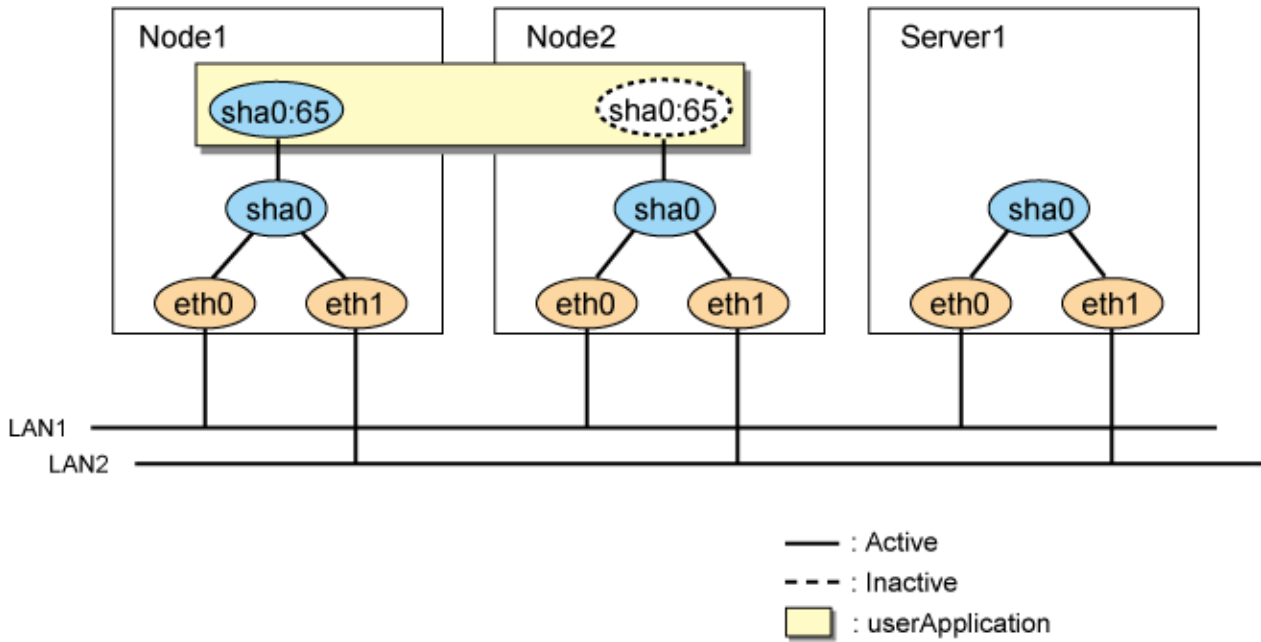


See

"2.1.1 Fast switching mode"

### I.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.



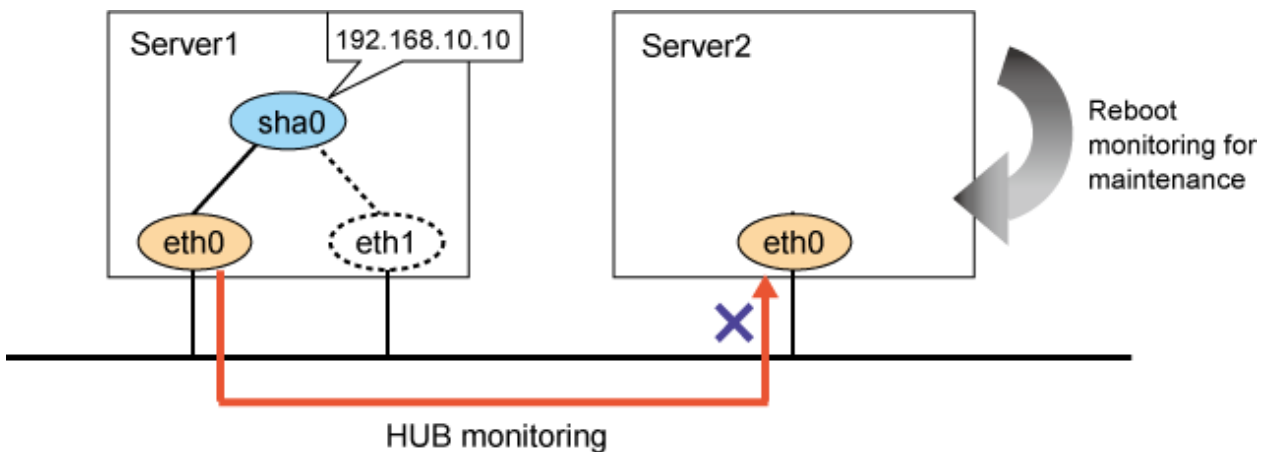
See

"5.1 Outline of Cluster System Support"

## I.4 NIC switching mode

### I.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.



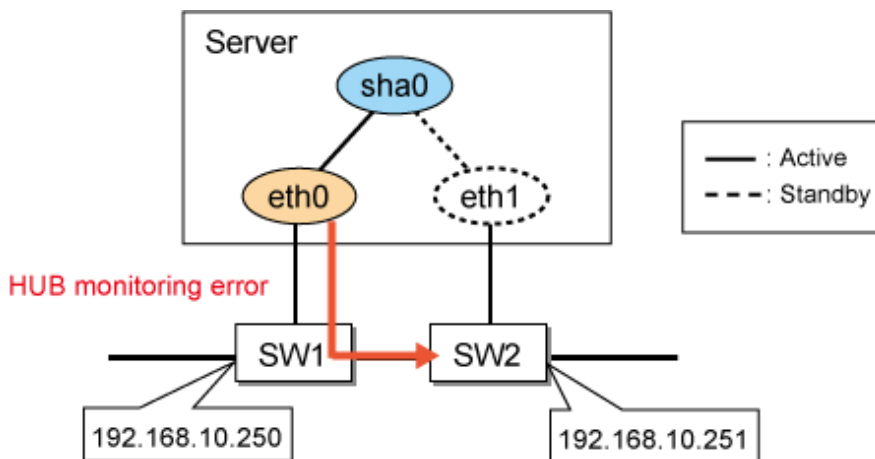
## I.4.2 Monitoring time adjustment

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 address to be taken over to another router in the event of a router failure.

## I.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
```

## I.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"

## I.5 Virtual NIC mode

### I.5.1 Interface setting file

Virtual interfaces in the 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

- For RHEL8

Check that the IP addresses, subnet masks, or prefixes 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
PREFIX=24
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
```

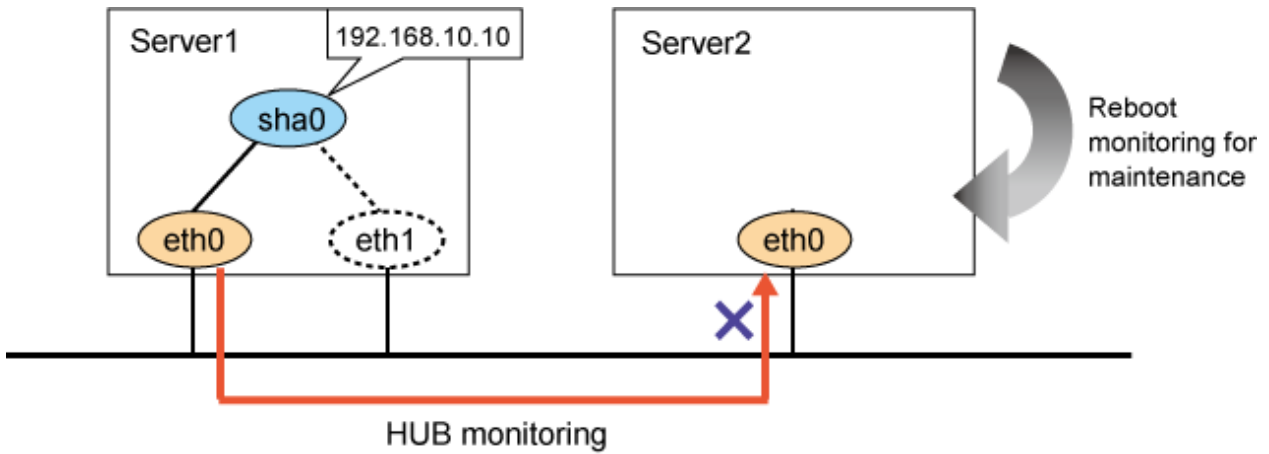
- For RHEL9

Verify that the following parameters are set for shaX with the "nmcli connection show" command. If the parameters are different, fix the settings seeing "3.2.2.1 Setup common to modes."

```
connection.type: "802-3-ethernet"
connection.id: "shaX"
connection.interface-name: "shaX"
connection.autoconnect: "yes"
ipv4.method: "manual"
ipv4.addresses: "192.168.1.1/24"
```

## I.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.

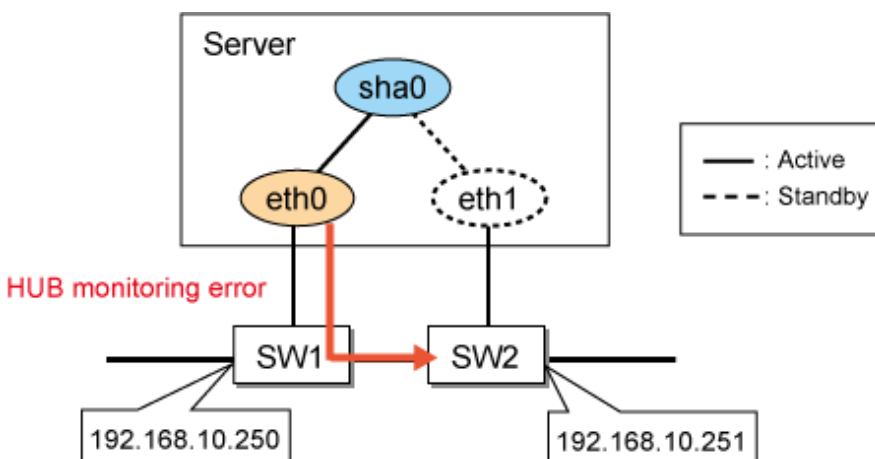
## I.5.3 Monitoring time adjustment

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.

## I.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]

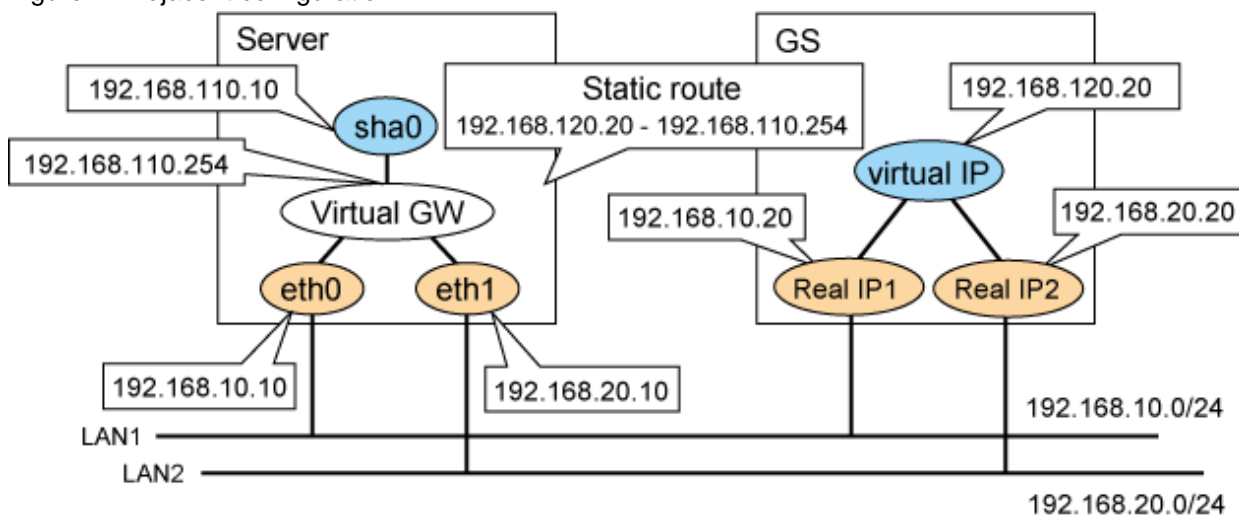
Name      Hostname/prefix  Mode Interface List
+-----+-----+-----+-----+
# hanetpathmon target
[Target List]
Name      VID Target
+-----+-----+-----+
sha0      -    192.168.10.250,192.168.10.251
```

## I.6 GS linkage mode

### I.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 I.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

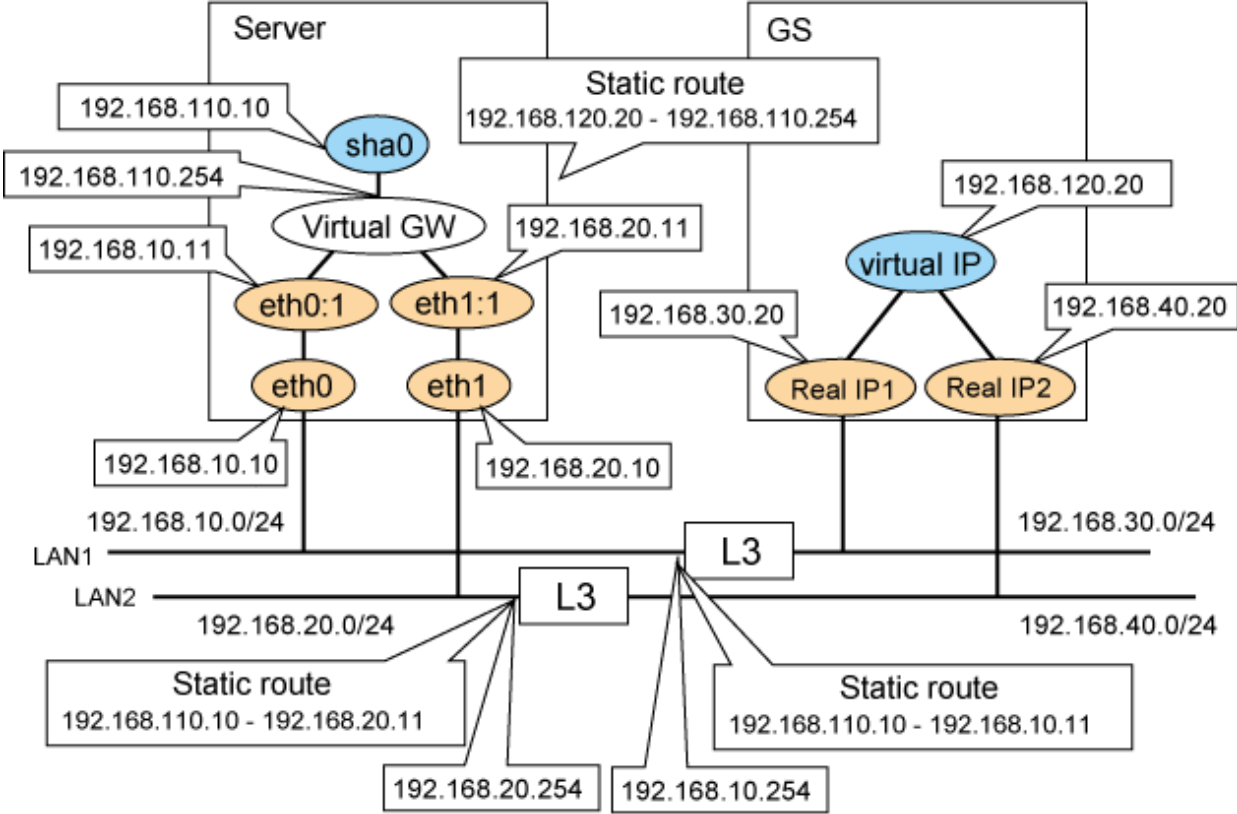
# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
-----+-----+
192.168.110.0   255.255.255.0

# /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 I.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

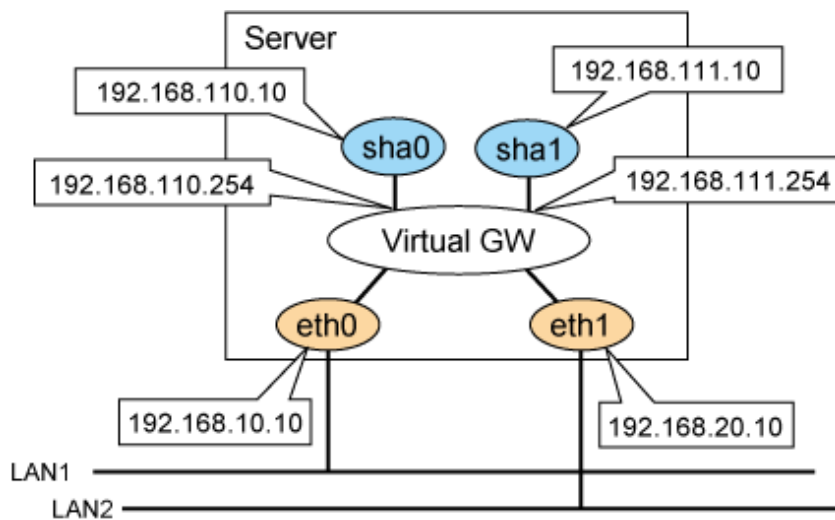
# /opt/FJSVhanet/usr/sbin/hanetmask print
network-address netmask
+-----+-----+
192.168.110.0   255.255.255.0
192.168.10.0    255.255.255.0
192.168.20.0    255.255.255.0

# /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

```



"2.2.2.3 Using GS linkage mode"

## I.6.2 Communication target setting

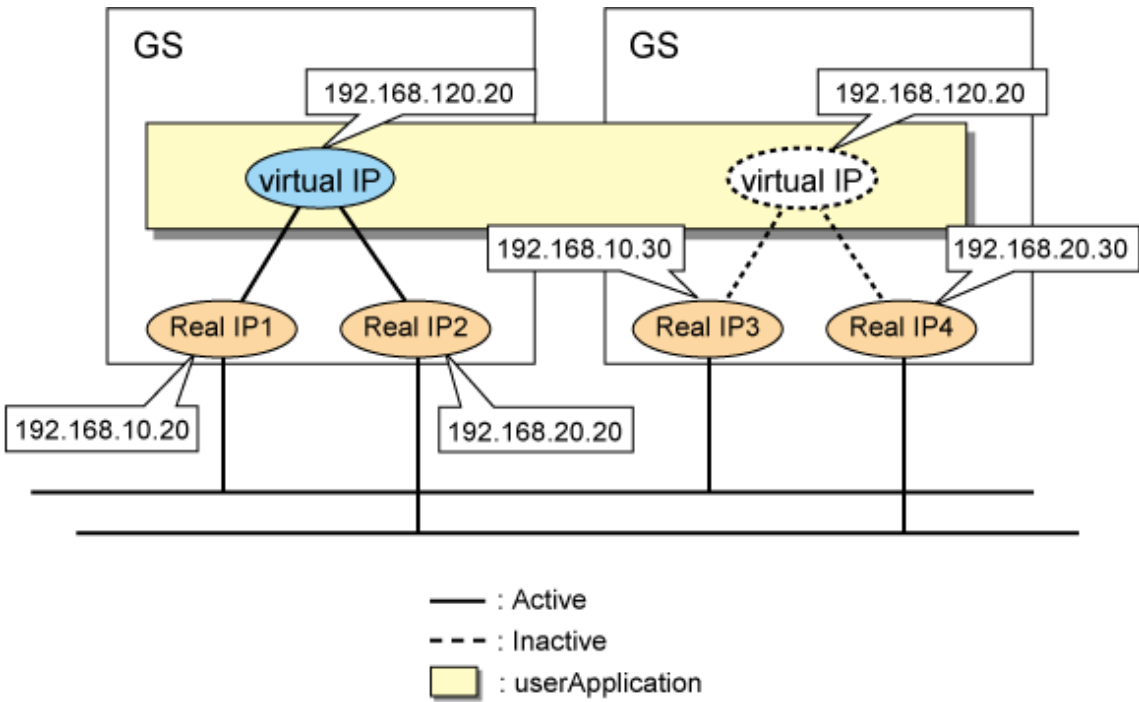
Check whether the "hanetobserv" command has been set correctly.

If GS's IP address moves between nodes as follows, execute the "hanetobserv create" command for each GS node.

```

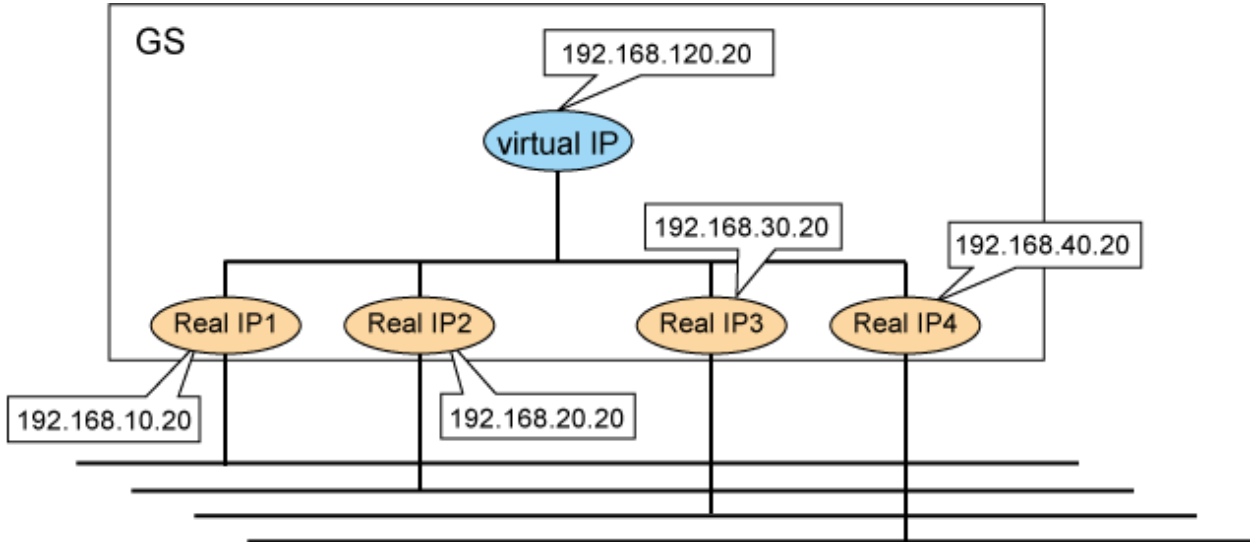
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.20,192.168.20.20
# /opt/FJSVhanet/usr/sbin/hanetobserv create -n GS -i 192.168.120.20 -t
192.168.10.30,192.168.20.30
# /opt/FJSVhanet/usr/sbin/hanetobserv print
Destination Host Virtual Address (Router Address+)NIC Address
+-----+-----+-----+-----+
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
```



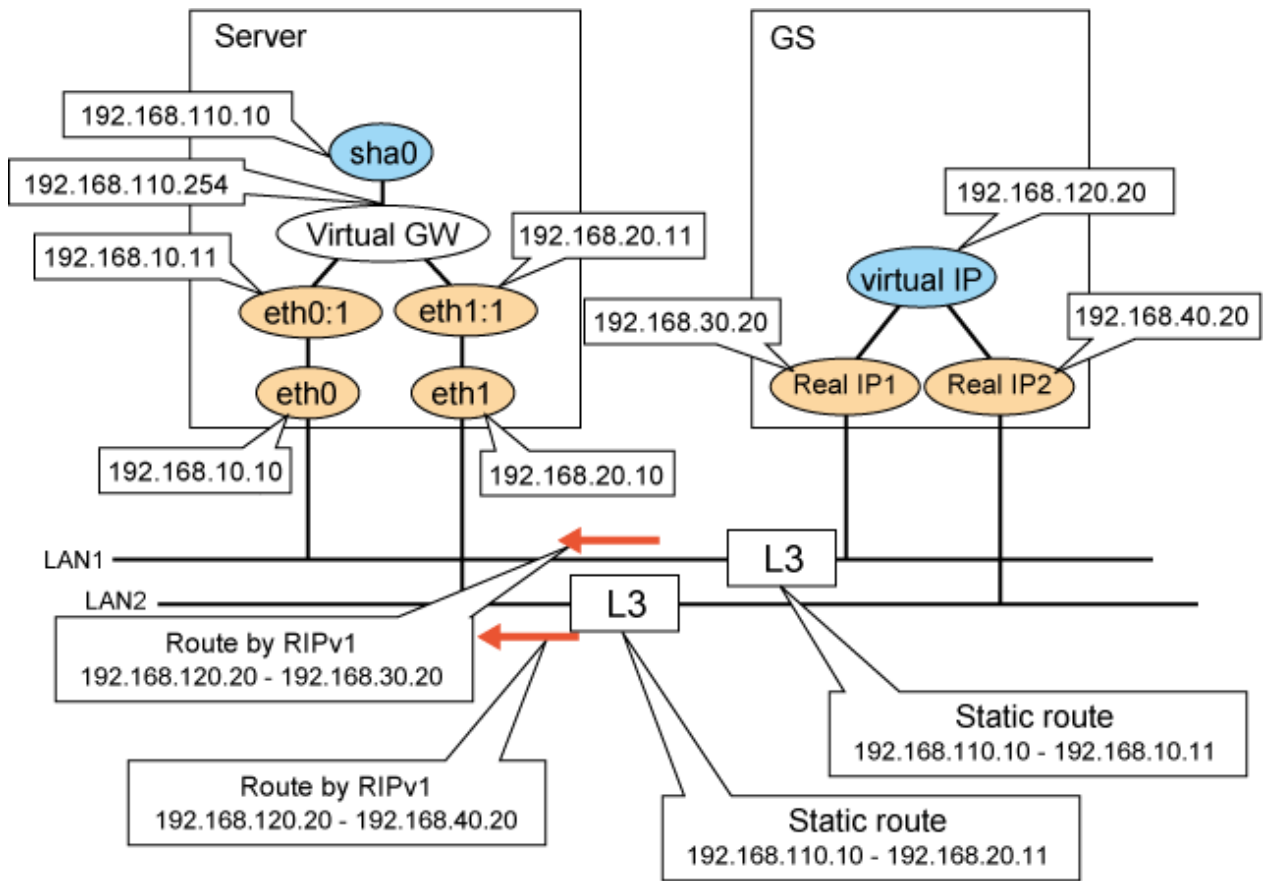
 See

.....  
 "3.10.1.1 Setting the monitoring destination information"  
 .....

### I.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 routing daemon (quagga(ripd)) which obtains RIP in the server.

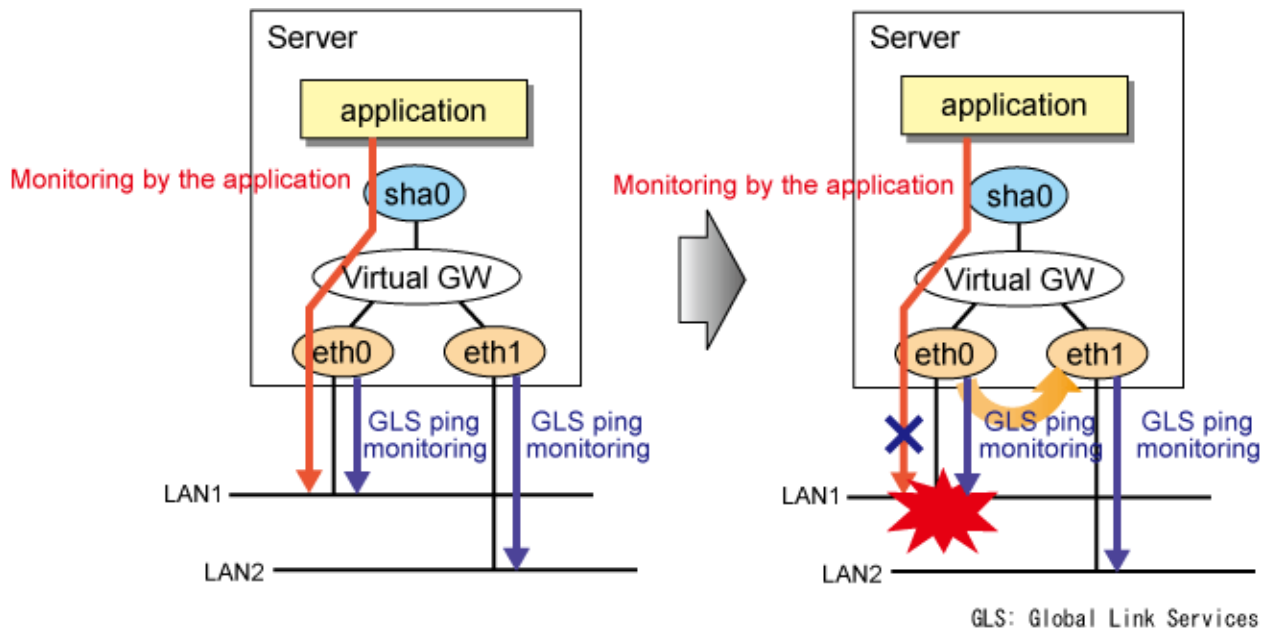


See

- "2.1.4.5 Notes"
- "2.10.5 Duplicated operation via GS linkage mode"

## I.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
```

## I.6.5 Maintenance procedure performed when the communication target stopped

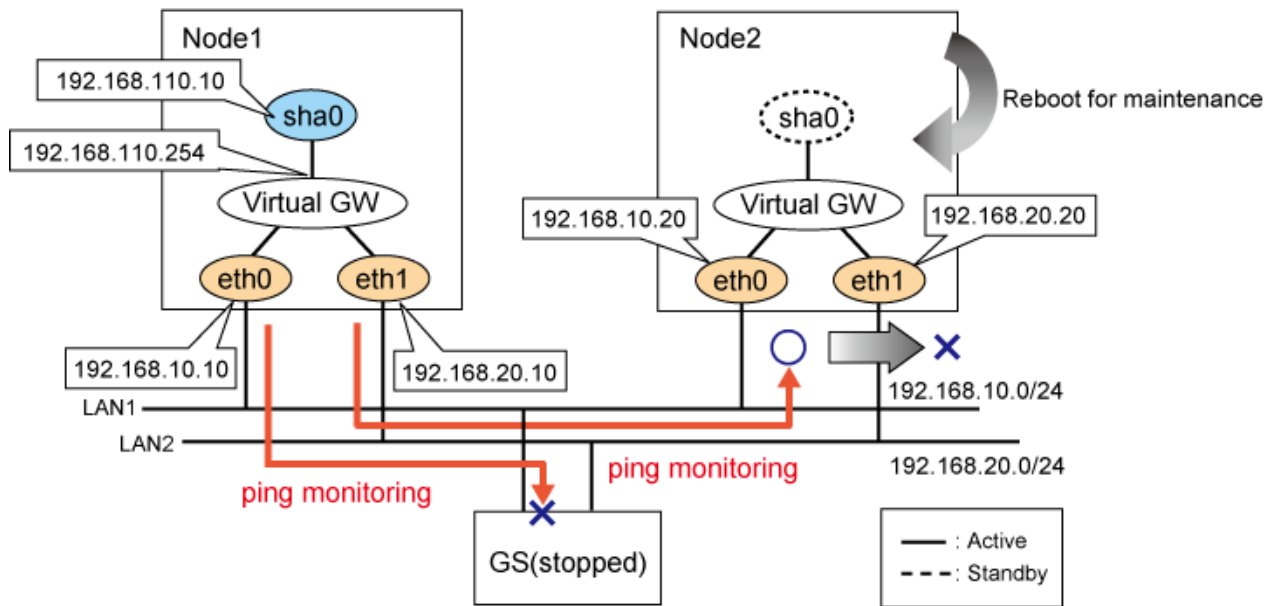
Actions to be taken will differ depending on whether the IP addresses of neighboring switches are set or not in the destination cluster node monitoring information.

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"  
.....

## I.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 J Resident Process in GLS and Monitoring Target

This appendix explains the resident process in GLS and the monitoring target.

## - Resident Process in GLS

Table J.1 Processes in GLS

Process name	Function	Resident
/opt/FJSVhanet/etc/sbin/hanetctld	GLS control daemon	Resident
/opt/FJSVhanet/etc/sbin/hanetmond	Monitors the status of the GLS control daemon and the sha driver.	Non-resident
/opt/FJSVhanet/etc/sbin/hanetpathmd	Monitors the network in the Virtual NIC mode.	Non-resident
/opt/FJSVhanet/etc/sbin/hanetselect	Monitors the transfer path in the NIC switching mode and the GS linkage mode.	Non-resident

GLS: Global Link Services

### Note

The following are not resident processes because the processes stop if an error is detected when a virtual interface is stopped.

- hanetmond
- hanetpathmd
- hanetselect

## - Monitoring Target

Table J.2 Process that can be set as a monitoring target

Process name	Function	Number of processes
/opt/FJSVhanet/etc/sbin/hanetctld	GLS control daemon	1 to 3

GLS: Global Link Services

### Note

- In the following cases, the GLS control daemon is restarted, so the process may not temporarily exist.
  - Restarting GLS by using the resethanet -s command
  - Restarting GLS service (fjsvhanet.service)
- The number of processes of the GLS control daemon is usually one. However, it may be temporarily two or three when a child process is started.

# Appendix K Changes from previous versions

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

## K.1 Changes from Redundant Line Control function 4.0A20 to version 4.1A20

Table K.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 K.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

### K.1.1 New command

There are no new commands for Redundant Line Control function 4.1A20.

### K.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/FJShanet/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/FJShanet/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.

## K.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 "StandbyTransition" attribute will not be set as the default value. If this configuration is used without any modification, it does not monitor the GLS resource status in standby node. In such case, temporary stop the cluster application and use 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](#)".



## K.2 Changes from Redundant Line Control function 4.1A20 to version 4.1A30

---

Table K.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 K.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 or later
	resethanet command	Redundant Line Control function 4.1A30 or later
Incompatible function	Verifying the Network address	Redundant Line Control function 4.1A30 or later
	HUB monitoring function	Redundant Line Control function 4.1A30 or later

### K.2.1 New command

---

There are no new commands for Redundant Line Control function 4.1A30.

### K.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.

### K.2.3 Incompatible function

---

## (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 netmask value configured on the physical and virtual interfaces. It is possible that IP address or netmask value is invalid. Note that, command process continues execution regardless of the warning messages.
  - /opt/FJShanet/usr/sbin/hanetconfig create
  - /opt/FJShanet/usr/sbin/hanetconfig modify
  - /opt/FJShanet/usr/sbin/hanetconfig copy
  - /opt/FJShanet/usr/sbin/strhanet
  - /opt/FJShanet/usr/sbin/hanetnic add
  - /opt/FJShanet/usr/sbin/hanethvrsc create
- When the definition error of a network address is detected at the time of system starting or RMS starting, a warning message may be output to the system log instead of a standard error (stderr).

## (2) HUB monitoring function

### [Contents]

The time to detect ping errors in the HUB-to-HUB monitoring of HUB monitoring function is reduced. With this modification, the "recovery monitoring period" parameter is integrated with the "monitoring period" parameter, and the "recovery monitoring period" is no longer used.

**[Changes]**

- Before modification

The default detection time of HUB-to-HUB monitoring is about 52 seconds.  
The "recovery monitoring period" parameter is used in HUB monitoring.

- After modification

The default detection time of HUB-to-HUB monitoring is about 27 seconds.  
The "recovery monitoring period" parameter is not used in HUB monitoring.

### K.3 Changes from Redundant Line Control function 4.1A30 to version 4.1A40

---

There is no difference of the function.

### K.4 Changes from Redundant Line Control function 4.1A40 to version 4.2A00

---

[Table K.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 K.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

#### K.4.1 New command

---

There are no new commands for Redundant Line Control function 4.2A00.

#### K.4.2 Incompatible command

---

No commands in the Redundant Line Control function 4.2A00 are incompatible from the previous versions.

#### K.4.3 Incompatible function

---

##### (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.

## K.5 Changes from Redundant Line Control function 4.2A00 to version 4.2A30

Table K.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 K.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
	dsobserv command	Redundant Line Control function 4.2A30
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

### K.5.1 New commands

Redundant Line Control function 4.2A30 provides the following commands.

- hanetgw Command
- hanetobserv Command
- dsobserv Command

For details on each command, see "[Chapter 7 Command references](#)".

### K.5.2 Incompatible command

No commands in the Redundant Line Control function 4.2A30 are incompatible from the previous versions.

### K.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.

## K.6 Changes from Redundant Line Control function 4.2A30 to version 4.3A00

[Table K.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 K.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

Category	Item	Version
	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

## K.6.1 New command

---

There are no new commands for Redundant Line Control function 4.3A00.

## K.6.2 Incompatible command

---

### (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.

## K.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.

## K.7 Functional Improvements in Redundant Line Control function 4.3A00

[Table K.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 K.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

## K.7.1 New command

---

There are no new commands for functional improvements in Redundant Line Control function 4.3A00.

## K.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 "hanetobserv" 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.

**K.7.3 Incompatible function**

## (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:

<code>Recovery detection time = recovery monitoring interval (in seconds) x retry count (times) + (0 to recovery monitoring interval (in seconds))</code>
---

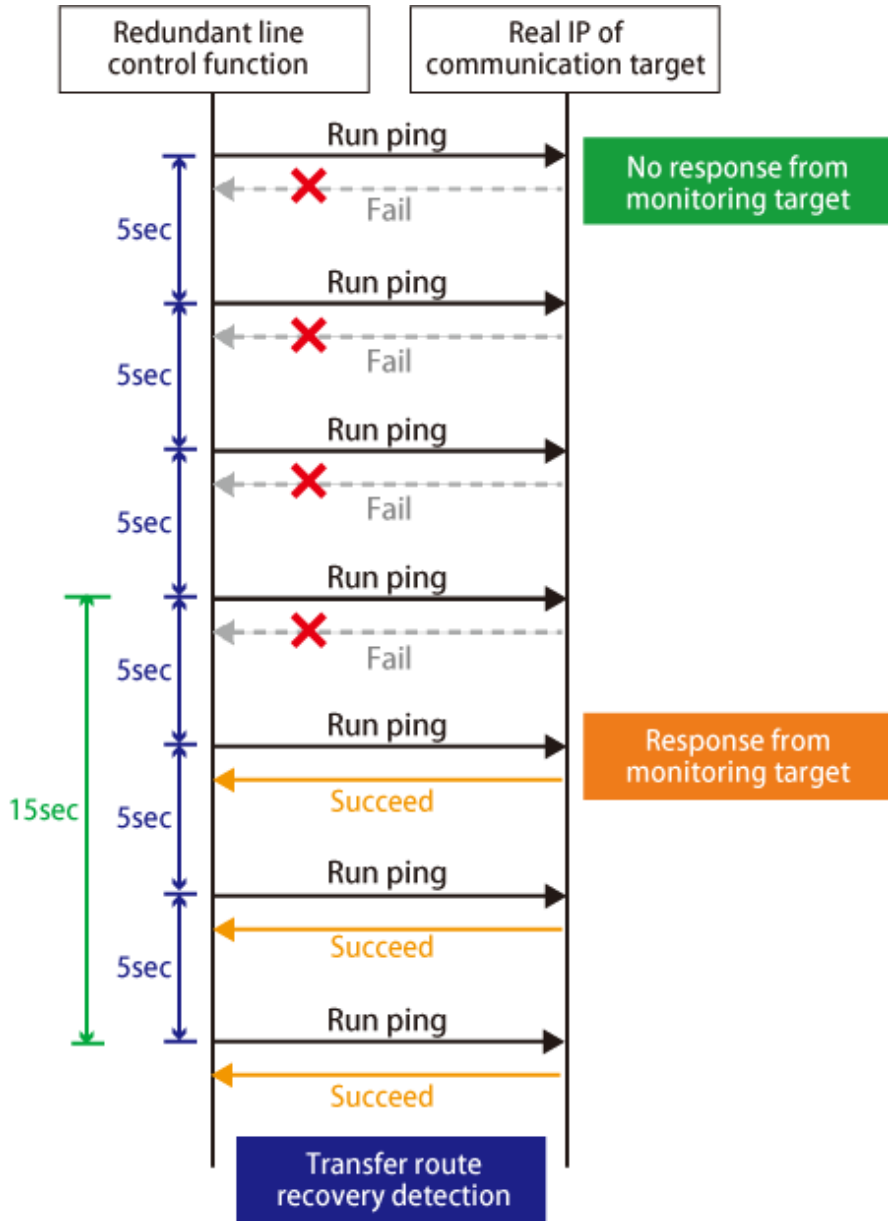
The default value would look like the following.

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 times + 0 to 5 sec = 10 to 15 sec

Figure K.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.

## K.8 Changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10

Table K.7 List of changes from Functional Improvements in Redundant Line Control function 4.3A00 to 4.3A10 is a list of changes.

Table K.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

GLS: Global Link Services

## K.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.

## K.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.

## K.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/FJShanet/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)
```

# K.9 Changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20

Table K.8 List of changes from Functional Improvements in Redundant Line Control function 4.3A10 to 4.3A20 is a list of changes.

Table K.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
	Conditions to output the message for the GLS virtual interface	Redundant Line Control function 4.3A20 or later

GLS: Global Link Services

## K.9.1 New command

---

There are no new commands for Redundant Line Control function 4.3A20.

## K.9.2 Incompatible command

---

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.

## K.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

## K.10 Changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30

Table K.9 List of changes from Functional Improvements in Redundant Line Control function 4.3A20 to 4.3A30 is a list of changes.

Table K.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 address 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

### K.10.1 New command

There are no new commands for Redundant Line Control function 4.3A30.

### K.10.2 Incompatible command

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.

## K.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 address 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.

## K.11 Changes from Functional Improvements in Redundant Line Control function 4.3A30 to 4.3A40

Table K.10 List of changes from Functional Improvements in Redundant Line Control function 4.3A30 to 4.3A40 is a list of changes.

Table K.10 List of changes from Functional Improvements in Redundant Line Control function 4.3A30 to 4.3A40

Category	Item	Version
New command	None	-
Incompatible commands	hanetparam command	Redundant Line Control Function 4.3A40 or later
	hanetconfig command	Redundant Line Control Function 4.3A40 or later
	hanetpoll command	Redundant Line Control Function 4.3A40 or later
	hanetobserv command	Redundant Line Control Function 4.3A40 or later
Incompatible function	RHEL5-Xen Virtual Machine Function	Redundant Line Control Function 4.3A40 or later

### K.11.1 New command

There are no new commands for Redundant Line Control function 4.3A40.

### K.11.2 Incompatible commands

The following are the incompatible commands of Redundant Line Control function from the previous version.

#### (1) hanetparam command

##### [Contents]

"The default value of the -h option is changed from NO to YES. For details, see "[7.6 hanetparam Command](#)."

##### [Changes]

- Before modification

The default value of the -h option is set to NO (changed based on the OS setting).

- After modification

The default value of the -h option is set to YES (only the /etc/hosts file is used to change the host name).

#### (2) hanetconfig command/hanetpoll command/hanetobserv command

##### [Contents]

A numeric string cannot be specified as a host name.

##### [Changes]

- Before modification

A numeric string can be specified as a host name.

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.)

- After modification

A numeric string cannot be specified as a host name. If a numeric string is specified, the following error message is output.

```
hanet: 10500: operation error: invalid ip_address. ip=xxxxx
```

## K.11.3 Incompatible function

### (1) RHEL5-Xen Virtual Machine Function

#### [Contents]

RHEL5-Xen Virtual Machine Function is not supported.

#### [Changes]

- Before modification

RHEL5-Xen Virtual Machine Function can be used.

- After modification

RHEL5-Xen Virtual Machine Function cannot be used.

## K.12 Changes from Functional Improvements in Redundant Line Control function 4.3A40 to 4.4A00

Table K.11 List of changes from Functional Improvements in Redundant Line Control function 4.3A40 to 4.4A00 is a list of changes.

Table K.11 List of changes from Functional Improvements in Redundant Line Control function 4.3A40 to 4.4A00

Category	Item	Version
New command	None	-
Incompatible commands	strhanet command	Redundant Line Control Function 4.4A00 or later
	hanetnic add command	Redundant Line Control Function 4.4A00 or later
	hanetconfig command	Redundant Line Control Function 4.4A00 or later
	hanetpoll command	Redundant Line Control Function 4.4A00 or later
	hanetparam command	Redundant Line Control Function 4.4A00 or later
Incompatible functions	Secure Boot	Redundant Line Control Function 4.4A00 or later
	Detecting wrong settings of the monitoring destination	Redundant Line Control Function 4.4A00 or later
	Detecting hang-up of the ping command	Redundant Line Control Function 4.4A00 or later
	Adding execution timing of the user command	Redundant Line Control Function 4.4A00 or later
	Setting file of the self-checking function	Redundant Line Control Function 4.4A00 or later
	Outputting a message to the console	Redundant Line Control Function 4.4A00 or later
	Network setting file of the physical interface	Redundant Line Control Function 4.4A00 or later
	Fujitsu Hot Standby Protocol	Redundant Line Control Function 4.4A00 or later
	Changing the location of ifcfg-shaX file	Redundant Line Control Function 4.4A00 or later

### K.12.1 New command

There are no new commands for Redundant Line Control function 4.4A00.

## K.12.2 Incompatible commands

---

The following are the incompatible commands of Redundant Line Control function from the previous version.

### (1) strhanet command/hanetnic add command

#### [Contents]

Under the following conditions, these commands end with an error when GLS bundles the physical interfaces that are already used by other interfaces except GLS.

- Redundant line switching mode is Virtual NIC mode, and
- OS is RHEL7, and
- Target physical interfaces are already used by other virtual interfaces (bonding, virtual bridge, for example) except GLS.

The configurations described above have not been supported from previous versions. Therefore, the supported configurations are unchanged in this version.

#### [Changes]

- Before modification

The command ends successfully. However, the target physical interfaces cannot be used for communication.

- After modification

The following error message is output and the physical interfaces cannot be bundled.

```
ERROR: 923XX: physical interface is already linked by another network device.  
(shaX:ethY)
```

### (2) hanetconfig command/hanetpoll command

#### [Contents]

In single user mode, the configuration definition of NIC switching mode can be added, changed, and deleted.

#### [Changes]

- Before modification

When the system is started in single user mode, the configuration definition of NIC switching mode cannot be added, changed, and deleted.

- After modification

If the system is started in single user mode, the configuration definition of NIC switching mode can be added, changed, and deleted.

### (3) hanetparam command

#### [Contents]

The default value of "-e" option is changed from "NO" to "YES". For details, see "[7.6 hanetparam Command](#)."

#### [Changes]

- Before modification

For the default value of "-e" option, "NO" (self-checking function is disabled) is set.

- After modification

For the default value of "-e" option, "YES" (self-checking function is enabled) is set.

#### [Notes]

When the product version is upgraded, this setting is taken over.

## K.12.3 Incompatible functions

---

The following are the incompatible functions of Redundant Line Control function from the previous version.

### (1) Secure Boot

#### [Contents]

Secure Boot function of RHEL7 is supported.

#### [Changes]

- Before modification  
In the environment where Secure Boot function is enabled, GLS cannot be used.
- After modification  
In the environment where Secure Boot function is enabled, GLS can be used.

### (2) Detecting wrong settings of the monitoring destination

#### [Contents]

If the settings are incorrect as follows, the HUB monitoring function detects a route error.

- Redundant line switching mode is NIC switching mode or Virtual NIC mode.
- The network segment is not consistent between the IP address of the monitoring target and the IP address of the virtual interface.
- Communication with the IP address of the monitoring target is enabled by other interfaces except the virtual interface of GLS.

An error in the settings can be found earlier when a route error is detected.

#### [Changes]

- Before modification  
An error in the communication route cannot be detected.
- After modification  
An error in the communication route can be detected, and the error message number 870 is output to the system log.

#### [Notes]

- The incorrect settings described above cannot be detected in the following environments:
  - OS is RHEL7.
  - IPv6 is used as the monitoring destination IP address.

### (3) Detecting hang-up of the ping command

#### [Contents]

In the following monitoring functions, a hang-up of the ping command can be detected.

- HUB monitoring function in NIC switching mode
- Remote host monitoring function in GS linkage mode

#### [Changes]

- Before modification  
When the ping command hangs, an error in the route cannot be detected.
- After modification  
When the ping command hangs, an error in the route is detected. The operation after the route error is detected is the same as the operation after an error is detected in each communication mode.  
With this functional change, parameters are newly added to the interfaces of the following user command.



- When an error is detected in a transfer route in NIC switching mode

For details, see "(2) When detected an error in a transfer route" in "[3.12.2.1 Settings for NIC switching mode.](#)"

#### **(4) Adding execution timing of the user command**

##### **[Contents]**

Under the following conditions, the user command is executed.

- In the following redundant line switching mode, an error or a recovery of the virtual interface is detected:
  - Virtual NIC mode
- In the following redundant line switching mode, the takeover virtual interface is activated or inactivated:
  - Fast switching mode
  - Virtual NIC mode
  - GS linkage mode

For details, see "[2.8.2 User command execution function.](#)"

##### **[Changes]**

- Before modification  
The user command is not executed under the conditions described above.
- After modification  
The user command is executed under the conditions described above.

#### **(5) Setting file of the self-checking function**

##### **[Contents]**

When GLS is installed, the setting file for the self-checking function is deployed. For details, see "[H.3.6 Virtual driver hang detected by Self-checking function.](#)"

##### **[Changes]**

- Before modification  
The setting file for the self-checking function is newly created by a user if necessary.
- After modification  
When GLS is installed, the setting file for the self-checking function with the standard setting is deployed.

#### **(6) Outputting a message to the console**

##### **[Contents]**

From this new version, the following messages are not output to the console. However, you can change the settings so that these messages are output to the console as in the settings of previous versions.

- Messages output when the virtual interface in NIC switching mode is activated or inactivated
- Messages output when the takeover virtual interface is activated or inactivated in all the Redundant line switching modes

##### **[Changes]**

- Before modification  
The messages are output to both the system log and the console.
- After modification  
The messages are output only to the system log.

To output the messages to the console as in previous versions, add "disable\_console" parameter and set it to "0" in the following setting file.

/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
disable_console 0 < = Add the parameter and set "0" to it.
```

## (7) Network setting file of the physical interface

### [Contents]

For RHEL 7 or later, the naming conventions for NIC names are changed to generate device names based on the hardware locations of NICs (Predictable Network Interface Names).

In an environment where Predictable Network Interface Names are enabled, the setting of "HWADDR" can be skipped in the network setting file (/etc/sysconfig/network-scripts/ifcfg-ethX) of the physical interfaces bundled by the virtual interface of GLS.

### [Changes]

- Before modification

In the network setting file of the physical interfaces, "HWADDR" must be set.

- After modification

In the network setting file of the physical interfaces, the setting of "HWADDR" can be skipped.

## (8) Fujitsu Hot Standby Protocol

### [Contents]

In GS linkage mode, the operation when the message of Fujitsu Hot Standby Protocol failed to be sent is changed.

### [Changes]

- Before modification

The following error message is output:

```
ERROR: 80590: internal error.(*) [sock.c(***)]
```

- After modification

The following error message is output:

```
WARNING: 93200: cannot send fhsp message. (dest=hostip, code)
```

For details of this message, see ["A.1.3 Console output messages \(numbers 800 to 900\)."](#)

## (9) Changing the location of ifcfg-shaX file

### [Contents]

Change the interface configuration file (ifcfg-shaX) location of virtual interface in Virtual NIC mode.

### [Changes]

- Before modification

The interface configuration file (ifcfg-shaX) is stored in the following directory during the configuration of virtual interface in Virtual NIC mode.

/etc/opt/FJSVhanet/config/ifcfg-shaX

The symbolic link of the above file is also created in the following directory.

/etc/sysconfig/network-scripts/

- After modification

The interface configuration file (ifcfg-shaX) is stored in the following directory during the configuration of virtual interface in Virtual NIC mode.

/etc/sysconfig/network-scripts/ifcfg-shaX

However, the symbolic link of the above file is not created.

## K.13 Changes from Functional Improvements in Redundant Line Control function 4.4A00 to 4.5A00

Table K.12 List of changes from Functional Improvements in Redundant Line Control function 4.4A00 to 4.5A00 is a list of changes.

Table K.12 List of changes from Functional Improvements in Redundant Line Control function 4.4A00 to 4.5A00

Category	Item	Version
New command	None	-
Incompatible commands	hanetpoll command	Redundant Line Control Function 4.5A00 or later
	dspoll command	Redundant Line Control Function 4.5A00 or later
Incompatible functions	Ping response monitoring in HUB monitoring function	Redundant Line Control Function 4.5A00 or later
	Link status monitoring in HUB monitoring function	Redundant Line Control Function 4.5A00 or later
	MAC address broadcast of IPv6 address	Redundant Line Control Function 4.5A00 or later
	Detection time of driver hang in self-checking function	Redundant Line Control Function 4.5A00 or later

### K.13.1 New command

There are no new commands for Redundant Line Control function 4.5A00.

### K.13.2 Incompatible commands

The following are the incompatible commands of Redundant Line Control function from the previous version.

#### (1) hanetpoll command

- create/modify sub-command

[Contents1]

By specifying "\_none\_" with the -p option, it is possible to set a not used ping response monitoring of the HUB monitoring.

[Changes 1]

- Before modification  
"\_none\_" cannot be specified for -p option.
- After modification  
"\_none\_" can be specified for -p option.

[Contents 2]

Two monitoring destinations can be specified using -p option for the virtual interface of single physical interface configuration.

[Changes 2]

- Before modification  
Only one monitoring destination can be specified using -p option for the virtual interface of single physical interface configuration.
- After modification  
Up to two monitoring destinations can be specified using -p option for the virtual interface of single physical interface configuration.

- modify sub-command

[Contents]

The monitoring destination settings can be changed while the virtual interface remains active.

[Changes]

- Before modification  
For changing the monitoring destination settings, the virtual interface state must be inactive.
- After modification  
Monitoring destination settings can be changed while the virtual interface state is active.

- print sub-command

[Contents 1]

When ping response monitoring is not used, "\_none\_" is displayed in the Hostname parameter.

[Changes 1]

- Before modification  
Only the host name or IP address is indicated in the Hostname parameter.
- After modification  
Host name, IP address or "\_none\_" is displayed in the Hostname parameter.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = OFF
    interval(idle) =  5( 60) sec
    time           =  5 times
    link detection = YES
FAILOVER Status     = YES
Name  HUB Poll Hostname
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
sha0      OFF  _none_
```

[Contents 2]

The repair\_time parameter will no longer be displayed.

[Changes 2]

- Before modification

The repair\_time parameter is displayed.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = OFF
      interval(idle) = 5( 60) sec
      time           = 5 times
      repair_time    = 5 sec
      link detection = YES
FAILOVER Status     = YES
Name   HUB Poll Hostname
+-----+-----+-----+
sha0   OFF   192.168.70.100,192.168.70.101
```

- After modification

The repair\_time parameter is not displayed.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll print
Polling Status      = OFF
      interval(idle) = 5( 60) sec
      time           = 5 times
      link detection = YES
FAILOVER Status     = YES
Name   HUB Poll Hostname
+-----+-----+-----+
sha0   OFF   192.168.70.100,192.168.70.101
```

- on sub-command

[Contents 1]

When disabling all the monitoring of the HUB monitoring function, message is indicated when the HUB monitoring function is started.

[Changes 1]

- Before modification

All the monitoring of the HUB monitoring function cannot be disabled.

- After modification

When disabling all the monitoring of the HUB monitoring function, the message below is displayed during the startup of HUB monitoring function.

```
hanet: 00100: The virtual interface is excluded from HUB monitoring.
```

[Contents 2]

It is not necessary to stop monitoring by hanetpoll off command when applying the changes of monitoring parameter.

[Changes 2]

- Before modification

It is necessary to stop monitoring by hanetpoll off command when applying the changes of monitoring parameter.

- After modification

It is not necessary to stop monitoring by hanetpoll off command when applying the changes of monitoring parameter.

[Contents 3]

The -b option (recovery monitoring period settings of HUB monitoring) is obsoleted.

[Changes 3]

- Before modification  
The not used -b option existed.
- After modification  
The -b option is obsoleted.

- devparam sub-command

[Contents]

The repair\_time parameter will no longer be displayed.

[Changes]

- Before modification  
The repair\_time parameter is displayed.

```
# /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 = YES
FAILOVER Status     = YES

[ Polling Parameter of each interface ]
Name  intvl idle  time  repar link  Fover
+-----+-----+-----+-----+-----+-----+
sha0      2    60    5    5  YES  YES
```

- After modification  
The repair\_time parameter is not displayed.

```
# /opt/FJSVhanet/usr/sbin/hanetpoll devparam
[ Standard Polling Parameter ]
Polling Status      = ON
    interval(idle) = 5( 60) sec
    time           = 5 times
    link detection = YES
FAILOVER Status     = YES

[ Polling Parameter of each interface ]
Name  intvl idle  time  -    link  Fover
+-----+-----+-----+-----+-----+-----+
sha0      2    60    5  ---  YES  YES
```

**(2) dsppoll command**

[Contents 1]

When not setting the ping response monitoring, "----" will be displayed in the Primary Target/Secondary Target parameter.

[Changes 1]

- Before modification  
Host name or IP address is displayed in the Primary Target/Secondary Target parameter.
- After modification  
Host name, IP address or "----" is displayed in the Primary Target/Secondary Target parameter.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
Polling Status = ON
interval(idle) = 5( 60)
times = 5
link detection = YES
FAILOVER Status = YES

Status Name Mode Primary Target/Secondary Target HUB-HUB
+-----+-----+-----+-----+-----+
ON sha0 d ----(ON)/----(WAIT) OFF
```

**[Contents 2]**

The repair\_time parameter will no longer be displayed.

**[Changes 2]**

- Before modification

The repair\_time parameter is displayed.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
Polling Status = ON
interval(idle) = 5( 60)
times = 5
repair_time = 5
link detection = YES
FAILOVER Status = YES

Status Name Mode Primary Target/Secondary Target HUB-HUB
+-----+-----+-----+-----+-----+
ON sha0 d 192.168.70.100(ON)/192.168.70.101(WAIT) ACTIVE
```

- After modification

The repair\_time parameter is not displayed.

```
# /opt/FJSVhanet/usr/sbin/dsppoll
Polling Status = ON
interval(idle) = 5( 60)
times = 5
link detection = YES
FAILOVER Status = YES

Status Name Mode Primary Target/Secondary Target HUB-HUB
+-----+-----+-----+-----+-----+
ON sha0 d 192.168.70.100(ON)/192.168.70.101(WAIT) ACTIVE
```

### K.13.3 Incompatible functions

The following are the incompatible functions of Redundant Line Control function from the previous version.

**(1) Ping response monitoring in HUB monitoring function**

**[Contents 1]**

The setting to disable ping response monitoring is possible.

**[Changes 1]**

- Before modification

Ping response monitoring is always used.

- After modification

The setting to disable ping response monitoring is possible.

#### **[Contents 2]**

It is possible to use ping response monitoring to multiple monitoring destinations from virtual interface of a single physical interface configuration.

#### **[Changes 2]**

- Before modification

It is impossible to use ping response monitoring to multiple monitoring destinations from virtual interface of a single physical interface configuration.

- After modification

It is possible to use ping response monitoring to multiple monitoring destinations from virtual interface of a single physical interface configuration.

### **(2) Link status monitoring in HUB monitoring function**

#### **[Contents]**

Default of link status monitoring in the HUB monitoring function has been enabled.

#### **[Changes]**

- Before modification

The link status monitoring function is disabled by default and link down of the NIC is not detected.

- After modification

The link status monitoring function is enabled by default and link down of the NIC is detected.

### **(3) MAC address broadcast of IPv6 address**

#### **[Contents]**

MAC address of the interface that activated the IPv6 address is informed in the following switching:

- Route switching of NIC switching mode
- Node switching of cluster configuration

Switching of transfer route is informed by MAC address broadcast.

#### **[Changes]**

- Before modification

MAC address is not informed in switching.

- After modification

MAC address is informed in switching.

### **(4) Detection time of driver hang in self-checking function**

#### **[Contents]**

The driver hang up detection time for the self-checking function is set to 60 seconds.

#### **[Changes]**

- Before modification

The initial value for the driver hang up time for the self-checking function is 15 seconds.

- After modification

The initial value for the driver hang up time for the self-checking function is 60 seconds.



## K.14 Changes from Functional Improvements in Redundant Line Control function 4.5A00 to 4.5A10

---

Table K.13 List of changes from Functional Improvements in Redundant Line Control function 4.5A00 to 4.5A10 is a list of changes.

Table K.13 List of changes from Functional Improvements in Redundant Line Control function 4.5A00 to 4.5A10

Category	Item	Version
New command	None	-
Incompatible commands	hanetconfig command	Redundant Line Control Function 4.5A10 or later
	hanethvrsc command	Redundant Line Control Function 4.5A10 or later
Incompatible function	None	-

### K.14.1 New command

---

There are no new commands for Redundant Line Control function 4.5A10.

### K.14.2 Incompatible commands

---

The following are the incompatible commands of Redundant Line Control function from the previous version in Redundant Line Control function 4.5A10.

#### (1) hanetconfig command

- create/copy/modify sub-commands

[Contents]

When -i option or -e option is specified, if the setting of hanetmask command corresponding to the IP address specified for the option does not exist, a warning message is displayed.

[Changes]

- Before modification  
Warning messages are not displayed.
- After modification  
Warning messages are displayed.

#### (2) hanethvrsc command

- create sub-command

[Contents]

When -i option or -e option is specified, if the setting of hanetmask command corresponding to the IP address specified for the option does not exist, a warning message is displayed.

[Changes]

- Before modification  
Warning messages are not displayed.
- After modification  
Warning messages are displayed.

### K.14.3 Incompatible function

---

There are no functions incompatible with the previous version in Redundant Line Control function 4.5A10.

## K.15 Changes from Functional Improvements in Redundant Line Control function 4.5A10 to 4.6A00

---

Table K.14 List of changes from Functional Improvements in Redundant Line Control function 4.5A10 to 4.6A00 is a list of changes.

Table K.14 List of changes from Functional Improvements in Redundant Line Control function 4.5A10 to 4.6A00

Category	Item	Version
New command	None	-
Incompatible command	None	-
Incompatible function	None	-

### K.15.1 New command

---

There are no new commands for Redundant Line Control function 4.6A00.

### K.15.2 Incompatible command

---

No commands in the Redundant Line Control function 4.6A00 are incompatible from the previous versions.

### K.15.3 Incompatible function

---

There are no functions incompatible with the previous version in Redundant Line Control function 4.6A00.

### K.15.4 Specification changes for RHEL8

---

In the Redundant Line Control function 4.6A00, specification changes from RHEL7 when using the Redundant Line Control function in RHEL8 or later are as follows.

#### (1) Environment settings

##### [Description 1]

The handling of the operating system configuration file (ifcfg-ethX file) in GLS has been changed.

##### [Changes 1]

- RHEL7

GLS does not update the operating system configuration file (ifcfg-ethX file).

- RHEL8 or later

GLS updates the operating system configuration file (ifcfg-ethX file).

##### [Description 2]

The operation if there is a difference between the system settings by a user and the settings by GLS when installing GLS has been changed.

##### [Changes 2]

- RHEL7

Before starting GLS, the IP address is set according to the system definition and after starting GLS, the IP address is set according to the GLS definition.

- RHEL8 or later

The IP address is always set according to the GLS definition.

##### [Description 3]

The configuration for using the tagged VLAN interface in a Virtual NIC mode has changed.

**[Changes 3]**

- RHEL7

OS configuration changes for link state are not required when configuring tagged VLAN interfaces on virtual interfaces.

- RHEL8 or later

OS configuration changes for link state are required in/etc/NetworkManager/NetworkManager.conf when configuring tagged VLAN interfaces on virtual interfaces.

For more information, see Section "[3.3.3 Virtual NIC mode.](#)"

**[Description 4]**

The procedure for executing OS commands and editing files has been changed when setting the environment.

**[Changes 4]**

- RHEL7

RHEL 7 does not support NetworkManager.

- RHEL8 or later

Since RHEL 8 and later supports NetworkManager, the procedure for executing OS commands and editing files differs from RHEL 7 and earlier.

**(2) Settings of the physical interface (ifcfg-ethX file)****[Description]**

The settings of the physical interface (ifcfg-ethX file) when installing GLS has been changed.

**[Changes]**

For details, refer to "[3.2.2 Network configuration.](#)"

**(3) Change the scope of support****[Description 1]**

Redundant network methods available on the KVM host (host OS) has been changed.

**[Changes 1]**

- RHEL7

Supports a KVM host (host OS) configuration that uses NIC switching mode to bundle virtual bridges on the virtual interfaces.

- RHEL8 or later

Configuring a KVM host (host OS) to bundle virtual bridges on the virtual interfaces using a NIC switching mode is not supported. For RHEL 8 or later, if you want to make the guest domain network more reliable on KVM hosts in a cluster system, use the "[C.6.3 Setup example for creating a highly reliable network of guest domains on KVM hosts in a cluster system](#)" configuration.

**[Description 2]**

The interfaces that can be bundled in the GLS virtual interface has been changed.

**[Changes 2]**

- RHEL7

The Virtual NIC mode allows bundling of non-GLS virtual interfaces (bonding).

- RHEL8 or later

Non-GLS virtual interfaces (bonding) cannot be bundled.

## K.16 Changes from Functional Improvements in Redundant Line Control function 4.6A00 to 4.6A10

---

There is no difference of the function.

## K.17 Changes from Functional Improvements in Redundant Line Control function 4.6A10 to 4.6A20

---

There is no difference of the function.

## K.18 Changes from Functional Improvements in Redundant Line Control function 4.6A20 to 4.7A00

---

### K.18.1 Incompatible function

---

The features that are incompatible with the previous version are as follows in Redundant Line Control function 4.7A00.

#### (1) Use of IPv6 addresses in NIC switching mode

##### [Description 1]

IPv6 addresses cannot be used in the NIC switching mode.

##### [Changes 1]

- before modification  
IPv6 addresses can be used in the NIC switching mode.
- after modification  
IPv6 addresses cannot be used in the NIC switching mode.

#### (2) Use of IPv6 addresses in Fast switching mode

##### [Description 1]

IPv6 addresses cannot be used in the Fast switching mode.

##### [Changes 1]

- before modification  
IPv6 addresses can be used in the Fast switching mode.
- after modification  
IPv6 addresses cannot be used in the Fast switching mode.

#### (3) Physical interface settings

##### [Description 1]

The physical interface settings for GLS installation have been changed.

##### [Changes 1]

For details, refer to "[3.2.2 Network configuration](#)."

#### (4) hanetconfig command

##### [Description 1]

For the Virtual NIC mode in RHEL9, SHAMACADDR can be configured by using "hanetconfig" command.

**[Changes 1]**

- before modification

"hanetconfig" command does not support -s option.

- after modification

For RHEL9, "create", "print", and "modify" subcommands of "hanetconfig" command support -s option.

## **K.18.2 Specification changes for RHEL9**

---

### **(1) Environment settings**

**[Description 1]**

The handling of the operating system configuration file in GLS has been changed.

**[Changes 1]**

- RHEL8

GLS updates the operating system configuration file (ifcfg-ethX file).

- RHEL9

GLS updates the operating system configuration file (ethX.nmconnection file).

# 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.

---

## 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 assigned to one physical interface as the secondary address. For instance, a logical interface to a physical interface eth0 is displayed as the secondary address of eth0.

[Related article] Logical IP address (logical IP)

---

## 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

---

## 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 "OS IV VTAM-G TISP Handbook (V10)".

\*: The virtual IP address as the communication target of GLS

---

## 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

	[A]		
Active interface.....		640	
Active Standby.....		188,191	
Automatic fail-back function.....		44,640	
	[C]		
Cascade.....		213,216,226	
Cloning environment.....		547	
Cluster failover function (failover function).....		640	
Cluster system			
.....		184,185,373,377,381,386,428,431,437,441,445,448,453	
Configuration of GS load sharing.....		617	
Configuring Tagged VLAN interface.....		34	
	[D]		
dsphanet Command.....		274	
dsobserv Command.....		313	
dsobserv command.....		610,615	
dspathmon Command.....		304	
dspathmon command.....		614	
dspoll Command.....		293,632	
Duplicated operation via Virtual NIC mode.....		69	
Dynamic switching function.....		640	
	[E]		
Example of configuring Virtual NIC mode.....		457	
	[F]		
Fast switching mode			
.....		1,8,11,30,68,73,93,96,102,125,128,180,362,487,640	
Fast switching mode, Virtual NIC mode, GS linkage mode..		171	
Fault monitoring function.....		12,16,23,27	
	[G]		
GS linkage mode			
.....		2,9,24,32,61,70,77,95,102,122,126,205,606,608,640	
GS linkage mode.....		169	
GS Load Sharing.....		495	
	[H]		
hanetbackup Command.....		319	
hanetconfig Command.....		260,600,620	
hanetconfig command.....		615	
hanetconfig command.....		623,625,635	
hanetgw Command.....		305	
hanethvrsc Command.....		315	
hanethvrsc command.....		615,635	
hanetmask Command.....		276	
hanetnic add command.....		625	
hanetnic Command.....		294	
hanetnic command.....		621	
hanetobserv Command.....		307	
hanetobserv command.....		610,617,623	
hanetparam Command.....		279	
hanetparam command.....		616,623	
hanetparam command.....		625	
hanetpathmon Command.....		299	
hanetpathmon command.....		614	
hanetpoll Command.....		284,601,603,629	
hanetpoll command.....		608,623,625	
hanetrestore Command.....		320	
Hostname resolution.....		607,609	
Hot-standby.....		149	
HUB-to-HUB monitoring function.....		640	
HUB monitoring.....		133	
HUB monitoring function.....		39,133,604,640	
	[I]		
Interface status monitoring feature.....		49,602	
	[K]		
KVM.....		640	
KVM guest.....		640	
KVM host.....		640	
	[L]		
LAN card.....		641	
Line monitoring.....		641	
link monitoring.....		607,608	
Link status monitoring function.....		46,641	
Load sharing configuration.....		151,641	
Logical interface.....		641	
Logical IP address.....		641	
Logical IP address takeover function.....		641	
Logical virtual interface.....		365,641	
	[M]		
Monitoring frame.....		641	
Monitoring the remote host.....		147	
Mutual standby.....		208,209,211,212	
	[N]		
Network monitoring function.....		46,641	
NIC sharing.....		395,437,641	
NIC switching mode			
.....		1,8,15,31,55,68,74,94,96,105,125,129,135,162,180,230,391,642	
	[O]		
Operation on Hyper-V.....		541	
Operation on RHOSP.....		532	
Operation on the Virtual Machine Function (for RHEL6).....		514	
Operation on VMware.....		533	
	[P]		
Physical interface.....		34,642	
Physical IP address.....		642	
Physical IP address takeover function.....		642	
Physical IP address takeover function I.....		642	
Physical IP address takeover function II.....		642	
Primary interface.....		642	
	[R]		
Real interface.....		642	

Redundant Line Control Function.....	178,236,323,642
resethanet Command.....	321,603
Resource state monitoring function for standby node.....	602
RMS Wizard.....	642

[S]

Secondary interface.....	642
Self-checking function.....	173
Sharing physical interface.....	30,127
Sharing transfer route monitoring.....	643
Single configuration.....	148
Standby interface.....	643
Standby patrol function.....	43,140,643
Standby patrol function (automatic fail-back if a failure occurs) .....	643
Standby patrol function (immediate automatic fail-back).....	643
stphanet Command.....	272
stphanet command.....	601
stpptl Command.....	298
strhanet Command.....	270,601
strhanet command.....	625
strptl Command.....	297
Switching function.....	13,19,23

[T]

Tagged VLAN.....	605,643
Tagged VLAN interface.....	35,643
Takeover physical IP address.....	398,441,445
Takeover virtual interface.....	185,186,643
TNOTIFY command.....	643

[U]

userApplication.....	185
User command execution function.....	54,160

[V]

Verifying the Network address.....	604
Virtual bridge.....	643
Virtual interface.....	644
Virtual IP address (virtual IP).....	644
Virtual Machine Function.....	607,609
Virtual NIC mode .....	2,9,21,76,94,96,111,125,132,168,180,231,233,234,476,481, 559,617,644

[W]

Web-Based Admin View.....	644
---------------------------	-----